ICEcore™

Discover Cool Collaboration

Installation and Configuration Guide

ICEcore Version 1.0

SiteScape™
MAKES TEAMS WORK

www.icecore.com

Legal Notices

SiteScape, Inc., makes no representations or warranties with respect to the contents or use of this documentation, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, SiteScape, Inc., reserves the right to revise this publication and to make changes to its content, at any time, without obligation to notify any person or entity of such revisions or changes.

Further, SiteScape, Inc., makes no representations or warranties with respect to any software, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, SiteScape, Inc., reserves the right to make changes to any and all parts of SiteScape software, at any time, without any obligation to notify any person or entity of such changes.

Any products or technical information provided under this Agreement may be subject to U.S. export controls and the trade laws of other countries. You agree to comply with all export control regulations and to obtain any required licenses or classification to export, re-export or import deliverables. You agree not to export or re-export to entities on the current U.S. export exclusion lists or to any embargoed or terrorist countries as specified in the U.S. export laws. You agree to not use deliverables for prohibited nuclear, missile, or chemical biological weaponry end uses.

SiteScape, Inc., has intellectual property rights relating to technology embodied in the product that is described in this document.

SiteScape, Inc.
12 Clock Tower Place, Suite 210
Maynard, MA 021754
U.S.A.
www.SiteScape.com

Third-Party Materials

All third-party trademarks are the property of their respective owners.

Contents

About This Guide

This guide covers the installation and initial configuration of ICEcore. In this manual, the term "ICEcore" applies to all versions of ICEcore unless otherwise noted.

Audience

This guide is intended for ICEcore administrators.

Contents of this Manual

This manual provides information about the following:

 ◆ Installing ICEcore
 ◆ Configuring ICEcore
 ◆ Controlling Access

Conventions

This manual uses the following conventions:

A greater-than symbol (>) is used to separate actions within a step and items in a cross-reference path.

A trademark symbol ($^®$, ™, etc.) denotes a Novell trademark. An asterisk (*) denotes a third-party trademark.

When a single pathname can be written with a backslash for some platforms or a forward slash for other platforms, the pathname is presented with a backslash. Users of platforms that require a forward slash, such as Linux or UNIX, should use forward slashes as required by your software.

What you see	What it means
Click the *Add toolbar* item.	References to toolbar items, links, menu items, and buttons are presented in *italic* font.
Click the *Getting Started* link.	
Click the *Add Document* menu item.	
Click *Close*.	
Type `status`, then press Enter.	Text that you must type and file names are presented in `Courier` font.
Open the `ManagerGuide.pdf` file.	

Additional Documentation

You may find more information in the ICEcore documentation, which is accessible from links within ICEcore:

- ICEcore Help system
- ICEcore Quick Start Guide
- ICEcore User Guide
- ICEcore Admin Guide

The ICEcore online documents may be found from within the ICEcore Help system. To access the ICEcore Help system, after logging in (described later in this manual), click the *Help* link.

In the ICEcore Help system, click the *Getting Started Manuals* link to access copies of the online documents listed above.

Installing ICEcore

1

This chapter describes how to initially install and configure ICEcore:

1.1 Prerequisites

You need a few things before you install ICEcore:

1. Computer:
   - Linux systems need to have a minimum open file limit of 4096.
     For SLES, check `/etc/security/limits.conf`:
     ```
     hard nofile 65535
     soft nofile 4096
     ```
   - Minimum 2Ghz processor
   - Multi-CPU systems preferred
   - Minimum 2GB RAM

     NOTE: You may potentially run with less RAM for specific development and testing configurations without simultaneous users, lots of database traffic, etc.

   See "Memory Guidelines" on page 11 for details.

2. Sun JDK 1.5.0_011 or higher installed (Java 1.6 is not yet supported).

3. A Database Server:
   - MySQL 5.0.37 (or higher) Server and Client for Linux or MySQL 5.0.26 (or higher) Server and Client for Windows

     ---
     NOTE: MySQL 5.1 is not yet supported.

   - SQL Server for Windows (2000 or 2005)

   See "Database Planning" on page 3 for details.

How much disk do you need?

This depends on how much data you plan to put into the system. See sections "Database Planning" on page 3 and "File System Planning" on page 5.

The software takes about 250 MB.

1.2 Steps for Installing ICEcore

The following sequence shows the steps you want to follow to install ICEcore:

1 Install JDK (Sun JDK 1.5.0_011 or higher).

2 Set `JAVA_HOME` environment variable.

   For example:

   - On Linux: `export JAVA_HOME=/usr/java/jdk_1.5.0_11`
   - On Windows: `JAVA_HOME=C:\Program Files\Java\jdk1.5.0_11`

3 Install and Configure the Database Server.

4 Download the appropriate ICEcore kit.

5 Edit the `installer.xml` file (see Editing the Installer (.xml) File).

NOTE: If you are doing an upgrade, use your existing `license-key.xml` and `installer.xml` files by placing them in the same directory as the installer program. If you are doing a new installation, copy the `sample-installer.xml` file to `installer.xml` and edit that file. The `license-key.xml` file required to install the product is provided with the software kit (but is not included in kit).

---

6 If you want to run the indexing service in ICEcore on a different machine from ICEcore, you have to Install the Lucene Index Server on the other machine.

7 Run the installer (on Linux, do a `chmod +x installer-(liferay|jboss).linux` to make the installer executable).

   The installer is named one of the following according to your operating system and portal server:

   - `installer-liferay.exe`
   - `installer-liferay.linux`
   - `installer-jboss.exe`
   - `installer-jboss.linux`

8 Start and Stop ICEcore.
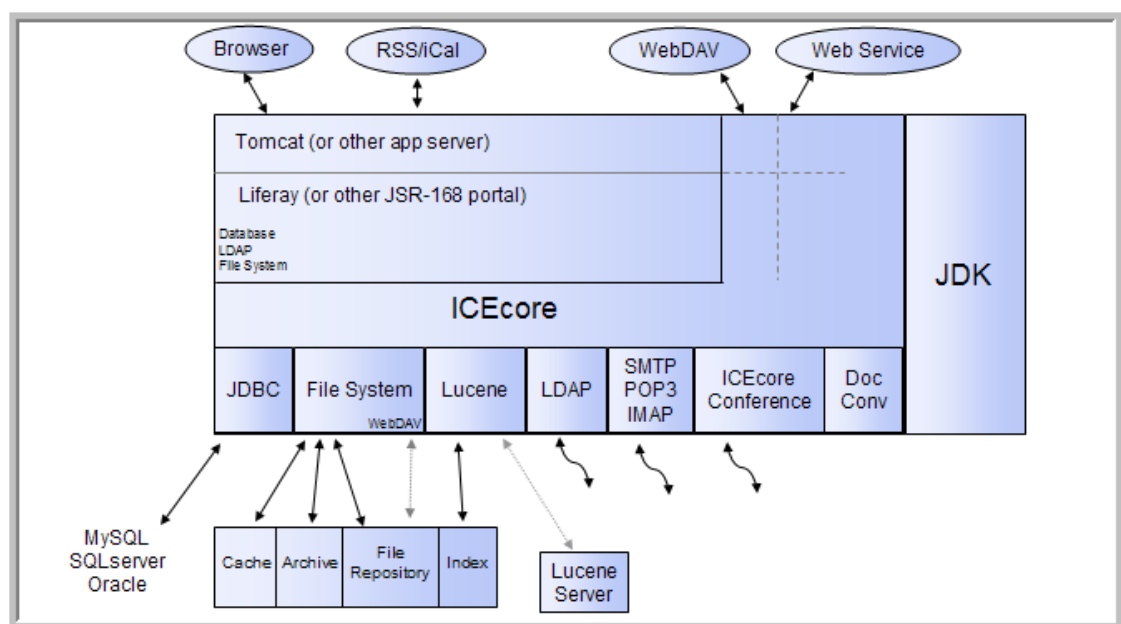
1.3 Database Planning

ICEcore and Liferay use separate dedicated databases within your database server.

A set of SQL configuration scripts are used to initialize the databases (creating the necessary tables, etc.).

ICEcore's default database for Linux and Windows is MySQL. It also supports SQL Server on Windows, and Oracle on Linux and Windows.

ICEcore's database requirements are relatively modest. The bulk of the data uploaded to ICEcore is stored in a file repository (see File System Planning - the database is primarily used for storing metadata and descriptive text.

Because the amount of data stored in the database is highly sensitive to the usage patterns of ICEcore (which are highly variable) there is no reliable formula for determining disk space usage, but the following can be used as a guideline:

- numberAttachments x averageAttachmentSize = totalAttachmentSpace
- totalAttachmentSpace * .04 = sqlDataSpace
- sqlDataSpace x 5 = sqlStorageSapce

MySQL

- MySQL 5.0.37 (or higher) Server and Client for Linux or MySQL 5.0.26 (or higher) Server and Client for Windows are required with "innodb support" enabled

  NOTE: MySQL 5.1 is not yet supported.

- Specify `root` for the administrator password (or make commensurate changes in the ICEcore `installer.xml` file)

- Set the default character set to UTF-8 by selecting "*Best support for Multilingualism*" in the Windows Configuration window, or edit the `my.cnf` configuration file to the following:
  ```
  [mysqld]
  character_set_server = utf8
  [client]
  default_character_set = utf8
  ```

  NOTE: This file is located in `/etc/my.cnf` for Linux and in `c:\my.cnf` for Windows.

Microsoft SQL Server

- You can use SQL Server 2000 or SQL Server 2005
- Make sure to select SQL Server and Windows for authentication (the default is Windows only)
- Set the administrator password to "`sa`" (or make commensurate changes in the ICEcore `installer.xml` file)

Oracle Database

- Supported versions: Oracle 9, Oracle 10.

  NOTE: Oracle's default database name is "orcl". We use this name in our examples. If you have chosen a different name, replace "orcl" with your database name.

- ICEcore is a Unicode-enabled application and requires you to set up the Oracle Database Character Set to support Unicode character encodings. The recommended value is AL32UTF8.
- To check your database character set execute the following command with SQL*Plus:
  ```
  select value from SYS.NLS_DATABASE_PARAMETERS where PARAMETER =
  'NLS_CHARACTERSET';
  ```
- Before you install the ICEcore application software, use the "Create Initial Database Scripts" option of the installer to obtain the two database creation scripts for oracle (one for the portal and one for ICEcore).

  a. Copy these scripts to a directory where you have access to the SQL*Plus utility and your database.
  b. Edit the supplied database scripts to set the passwords for the users (these are defined in the top few lines of each script).
  c. Use the SQL*Plus utility with the SYSTEM account to run the scripts:
  ```
  sqlplus SYSTEM/systemPassword
  sqlplus SYSTEM/systemPassword @create-database-oracle.sql
  sqlplus> quit
  ```
  d. Edit the `installer.xml` file to use the `Oracle_Default` configuration and change the JDBC URLs to reflect the database and username/passwords you have chosen.
  e. Install the ICEcore software using the UPDATE option (not the FULL INSTALL option). This installs the software, but does not run the database creation scripts, which you have already run separately.

Non-Local Database Setup

When installing the ICEcore software for the first time (the "FULL INSTALL" option) one of the steps involves creating two databases: one for the portal and one for the ICEcore application.

If you have granted the database user specified in the configuration the privileges needed to create a database, the installer creates the databases during the installation process.

For example, in MySql you can first create the databases and grant full access to the database user specified in the installer.

If this is done, the installer can create the rest of the database schema without further intervention:
```
create database lportal;
grant all on lportal.* to dbuser@host identified by 'dbpassword';
create database sitescape;
grant all on sitescape.* to dbuser@host identified by 'dbpassword';
```

However, there may be a number of reasons why this is not desirable.

If your database server administration doesn't allow this for security reasons, or if you have a special database setup, the installer can initially be run to extract the schema setup files and place them on the disk for you to examine or forward to the database administrator.

Once the schema is in place and the database user has been given the appropriate access rights for full database access, the installer can be run with the UPDATE option, which installs the software but doesn't create the databases.

The following are a list of "generic" database rights that are needed for normal operation of ICEcore:

```
DELETE, INSERT, SELECT,UPDATE,
ALTER TABLE, CREATE TABLE, CREATE VIEW, DROP,
CREATE INDEX, DROP INDEX, DRI
```

The first four are obvious. The rest are related to schema changes that may be invoked during upgrades or configuration changes.

NOTE: "DRI" refers to Microsoft SQLServer foreign key constraints.

The initial database creation scripts may CREATE/DROP USERs, but that is the only time users are defined.

1.4 File System Planning

ICEcore software and configuration files are stored in a tree shared with Liferay, Tomcat, etc. There are some temporary files also located here, but mainly locks, etc.

ICEcore data is stored in the database (see "Database Planning" on page 3) and on the file system. The file system usage is divided up into several functional areas:

- ◆ filerepository - This is where all attachment files are located, so it tends to be a large consumer of disk space. The tree is roughly organized by site, binder (folder/workspace), and entry.

- ◆ archiveStore - Only activated in the Enterprise version of ICEcore, this is where previous versions of files are stored. The files are stored here to meet compliance and archival goals.

- ◆ cachefilestore - This tree holds information derived from the attachments, such as thumbnails, scaled images, text, and HTML renderings. Depending on the nature of the attachments this tree consumes somewhat less space than the file repository (but it can, conceivably, store more).

- ◆ lucene - This tree holds the search index for the data. It tends to be a fraction of the space consumed by the file repository, but it is also sensitive to the type of information stored.

- ◆ Other trees - These are other trees that you cannot configure which typically consume a small amount of space (relatively speaking).
  - ◆ rss - Caches of RSS feeds for folders
  - ◆ temp - Temporary files

1.5 Network Planning

ICEcore is a complete Java/J2EE web application and includes a web server (Tomcat). Because the web server listens on ports and processes network connections, you should consider the following as part of the installation process:

Firewall Setup - The default installation uses port 8080/8443 for the web server. Some local firewalls (such as the Windows Security Center's firewall) may restrict traffic to port 8080/8443 and thus require proper configuration for access by other systems.

If you can access ICEcore on the local server, but cannot access it from another system, examine your firewall settings.

Port Conflicts - The Tomcat software uses a number of TCP/IP ports for both web traffic and management messages. If you have other web servers (Apache, IIS, or Tomcat) or other software installed that uses the same port numbers, your ICEcore software will not function properly.

NOTE: Novell OES2 systems have another Tomcat application running by default.

The `netstat -anp tcp` command on Windows and the `netstat -tan` command on Linux can help find which ports are currently being used. For more information on network ports, consult your operating system networking guide.

When you are in this situation, make sure that in addition to the http/https ports (8080/8443) you also assign free port numbers to the `ajpPort` and `shutdownPort` settings in the Network section of the `installer.xml` file.

1.5.1 Port 80/443 configuration on Linux

The default installation of ICEcore uses the Tomcat web server. Although the Tomcat server is part of the Apache project, it is not the same thing as the Apache web server. Tomcat is written in Java and can not do some of the special privilege behaviors that Apache can.

In particular, Linux does not allow non-root processes from allocating TCP/IP ports less than 1024. For this reason the default configuration for Tomcat (and ICEcore) uses ports 8080 for http and 8443 for https (SSL). Unfortunately this requires specifying the port number in the browser's URL for ICEcore (e.g., http://icecore.mycompany.com:8080).

WARNING: While running Tomcat as "root" solves this problem, it creates many (far worse) problems. Do not do this!

If you want ICEcore to be available on the default http/https ports, use an operating system feature called "kernal space port forwarding". The `iptables` command is used to map requests from port 80 to port 8080 (or whatever port you specify). For example:

```
iptables -t nat -A OUTPUT     -d localhost    -p tcp --dport 80 -j
REDIRECT --to-ports 8080
iptables -t nat -A OUTPUT     -d yourHostname -p tcp --dport 80 -j
REDIRECT --to-ports 8080
iptables -t nat -A PREROUTING -d yourHostname -p tcp --dport 80 -j
REDIRECT --to-ports 8080
iptables -t nat -A OUTPUT     -d localhost    -p tcp --dport 443 -j
REDIRECT --to-ports 8443
iptables -t nat -A OUTPUT     -d yourHostname -p tcp --dport 443 -j
REDIRECT --to-ports 8443
iptables -t nat -A PREROUTING -d yourHostname -p tcp --dport 443 -j
REDIRECT --to-ports 8443
```

If you install ICEcore as the "root" user, it asks if you want to use `iptables` to set up this mapping. See the `iptables man page` for more information about port forwarding.

1.5.2 Integrating with iChain

NOTE: This feature is only available in the Enterprise version.

Liferay/ICEcore contains support for iChain-based single sign-on (SSO).

When running in this mode, the iChain server performs user authentication tasks and passes a token representing the authenticated user's login name to Liferay/ICEcore in each request to indicate who made the request.

Liferay/ICEcore must be configured with the same LDAP that the iChain is using so that it can obtain and copy the user information into the portal.

However, this configuration differs from the regular portal/LDAP integration in that no password checking is performed against the LDAP when logging into the portal (because credential checking is only performed by the iChain server). This technique is safe only under the assumption that ALL accesses to the portal are routed through the iChain proxy. The SSO configuration sets up a "valve" that only permits access from the local server and the iChain proxy server.

To set up an iChain proxy, the following steps must be taken:

1 Assure that the iChain proxy's port number matches the ICEcore/Liferay port number. For example, if you have configured ICEcore to run on port 8080, the iChain proxy must also use port 8080. If you change ports through the proxy, some ICEcore features do not work properly.

2 Edit the SSO section in the `installer.xml` file and set the `SSO enable="true"`, set the `Logoff URL` to the log-off URL provided by the iChain proxy server, and set the `IP address` of the iChain proxy server.

3 Install the software or, if you have already installed ICEcore, stop the running server and use the installer's "`Apply Settings only`" option.

4 After enabling the iChain SSO, you need to log into Liferay using a direct login URL: `http://localhost:8080/c/portal/login` and log in as `admin`. Since the SSO configuration removes the "*Sign In*" link, you must type the URL manually.

5 If you have not already done this, use Liferay's *Admin* portlet to enable LDAP-based authentication. This setup is necessary since Liferay has to copy user data from the LDAP into the portal database upon user login.

6 To prevent users from logging into the portal directly through the portal's login form, remove or rename the following file from ICEcore's `liferay-portal-tomcat` directory:

`webapps/ROOT/html/portal/login.jsp`

You may also need to remove:

`work/Catalina/localhost/_/org/apache/jsp/html/portal/login_jsp.*`

7 Liferay/ICEcore is now ready to be put behind the proxy. Consult your iChain documentation on how to do this.

NOTE: To enable iChain integration-related debug log messages, modify Liferay's `portal-log4j-ext.xml` to add the following category:
```
 <category name="com.sitescape.team.liferay.security.auth">
  <priority value="DEBUG" />
 </category>
```
Use it only for testing or troubleshooting purpose. It is not recommended to have debug logging enabled on a production system.

1.6 Editing the Installer (.xml) File

The `installer.xml` file provides the ICEcore installer with detailed configuration information regarding network, memory, database, file system, e-mail, presence, and other settings. Edit this file with your specific data.

The "`sample-installer.xml`" file is included in the kit and should be used as a template for the `installer.xml` file. If you are doing an upgrade, use your existing `installer.xml` file by placing it in the same directory as the installer program. If you are doing a new installation, copy the `sample-installer.xml` file to `installer.xml` and edit that file.

For a quick installation edit the following sections:

1 Change the Host name in the Network section. Change the port number to 80 and the securePort to 443 if this is a dedicated server.

2 Consider changing the JavaVirtualMachine setting in the Memory section if you have a large installation.

3 Use the default file system configuration. This stores the files in `/home/icecoredata`

4 The default database configuration is MySQL, with the default MySQL passwords.

5 Use the default Lucene configuration (unless you are installing a standalone Lucene Index Server.

6 Modify the `Email` section with your SMTP and POP/IMAP servers.

7 If you are using ICEcore Conference, change the settings in the `Presence` configuration.

To view the `sample-installer.xml` file, see Appendix A, "The sample-installer.xml File," on page 47.

1.7 Running the Installer

The following procedure shows you how to run the installer.

1 Run the installer (on Linux, do a `chmod +x -(liferay|jboss).linux` to make the installer executable).

The installer is named one of the following according to your operating system and portal server:

- ◆ `installer-liferay.exe`
- ◆ `installer-liferay.linux`
- ◆ `installer-jboss.exe`
- ◆ `installer-jboss.linux`

2 Answer `Yes` to the license agreement:

`Have you read and agree with the license? : yes`

3 Enter the type of install you are performing:

WARNING: A full install erases the existing databases for an existing ICEcore application (use the UPDATE installation for existing ICEcore applications).

```
Enter the type of installation:

   1. ICEcore Enterprise with Liferay/JBoss - FULL INSTALL
   2. ICEcore Enterprise with Liferay/JBoss - UPDATE
   3. ICEcore Enterprise Lucene Server
   4. Apply settings only    (Use with care)
   5. Create Initial Database setup scripts for DBA
   6. Exit (no changes)

Installation type [1]: 1
```

1. **FULL INSTALL** - This option installs the ICEcore application software and creates the initial portal and ICEcore databases.

   The software is installed in the following dedicated directory: `/opt/icecore`

2. **UPDATE** - This option installs the ICEcore application software and uses the existing portal and ICEcore databases. Schema updates are applied as necessary.

3. **Lucene Server** - This is an advanced configuration option that allows you to locate the Lucene Index Server on a different system than your ICEcore application server. See Section 1.12, "Installing the Lucene Index Server," on page 16 for details on configuring your systems to use this option.

4. **Apply Settings** - The installation program uses configuration information in the `installer.xml` file to write a number of application configuration files. Most changes to the configuration do not require a reinstallation of the software, but just an update of the settings. Use this option to update those files without reinstalling the software.

   NOTE: The *Apply settings only* option can potentially corrupt your existing system (USE WITH CARE).

5. **Create Initial Database Scripts** - By default the software installation process creates the database schemas needed for operation of the software. If your database server administration does not allow this, use this option to extract the schema setup files for review and execution by your database administrator (DBA). This option installs no software or makes any changes to the application configuration.

4 Review the installation messages and enter `Y` to continue the install or `N` to cancel:

`Enter Y to continue, enter N to cancel installation [Y]: Y`

5 The install process asks you if want to create the ICEcore databases at this time; select `1` to create the databases or `2` to skip this step:

```
About to create the databases for ICEcore:
  1: Create the databases now.
  2: The databases were created by my DBA, don't create them now.
(1/2)  [1]: 1
   Creating jboss database for SQLServer ...
```

1.8 Starting and Stopping ICEcore

Starting ICEcore/Liferay

NOTE: These are Liferay only instructions.

On Windows:

```
C:\yourinstall\liferay-portal-tomcat-5.5-jdk5-4.3.0\bin\startup.bat
```

On Linux:

```
/yourinstall/liferay-portal-tomcat-5.5-jdk5-4.3.0/bin/icecore start
```

NOTE: While this is dependent on your system configuration, it can take upwards of 60 seconds before ICEcore/Liferay starts accepting web transactions. Initial transactions also tend to be slower as various caches load into RAM. These delays are amplified somewhat when working with a new installation or updated software as the JSPs are recompiled as they are referenced.
In Windows, startup is complete when the Tomcat window displays:

```
INFO:Server Startup in ##### ms
```

Setting up ICEcore to start on system startup

On Windows:

1 `C:\yourinstall\liferay-portal-tomcat-5.5-jdk5-4.3.0\bin\service.bat install icecore`

2 Use the Services Control Panel to configure the service to your needs.

   2a Select *Control Panel > Administration Tools > Services*.

   2b Right-click on the *ApacheTomcat icecore* service and select *Properties*.

   2c Change the *Startup Type* to *Automatic* and click *OK*.

   2d Set your firewall to allow port 8080.

On Linux, from the root account:

1 `cp /yourinstall/liferay-portal-tomcat-5.5-jdk5-4.3.0/bin/icecore /etc/init.d`

2 `chkconfig --add icecore`

Log Files/Monitoring

On Windows:

A Tomcat window appears when you issue the `startup.bat` command. Messages (good and bad) appear here.

On Linux:

Unlike Windows, the Tomcat process starts as a background process and no window appears. To monitor the messages in real time:

```
tail -f /yourinstall/liferay-portal-tomcat-5.5-jdk5-4.3.0/logs/catalina.out
```

Stopping ICEcore

On Windows:

```
C:\yourinstall\liferay-portal-tomcat-5.5-jdk5-4.3.0\bin\shutdown.bat
```

On Linux:

```
/yourinstall/liferay-portal-tomcat-5.5-jdk5-4.3.0/bin/icecore stop
```

1.9 Memory Guidelines

ICEcore is a Java/J2EE application and therefore executes within a "Java Virtual Machine" (JVM). The JVM exists as a process on your system and all of the ICEcore and portal software run within it. Consequently the amount of memory available to the JVM process is a critical aspect of overall ICEcore performance.

The key JVM memory setting is the "Java Heap Size", which roughly corresponds to the amount of memory available to the Java applications (such as ICEcore).

The `installer.xml` file's Memory section allows you to determine how much physical memory to devote to the Java Virtual Machine.

The default configuration assumes that the JVM uses 1g (one gigabyte) of memory. It is possible to run ICEcore with less than 1GB of assigned memory, but this is only applicable to very small test configurations, and is not suitable for production use. (In such a test configuration, 512MB is the minimum amount of memory required to produce a functioning ICEcore application.)

A general rule of thumb is that no more than 75% of the available physical memory should be allocated to the JVM. This means that you need to account for other processes (including the operating system itself) that use memory. Databases, in particular, tend to be memory-intensive, so take special care when co-locating a database server with the ICEcore application server.

WARNING: A JVM on a 32-bit system should never be configured to take more than 1.5GB (1500MB) of memory. Larger memory allocations require 64-bit servers.

ICEcore memory usage is driven by a number of factors:
1. Number of sessions (users logged in)
2. Number of active/concurrent sessions
3. ICEcore internal database caches
4. Lucene index cache

Items #1 and #2 do not represent a significant amount of memory.

Item #2 generally correlates to heavier CPU utilization (as this number increases the need for clustered configurations becomes more important).

Item #3 can be a significant fraction of memory use (these are separate from any caching or memory use by the database server itself, which may or may not be on the same server). Internal tuning settings have been set to handle a wide range of deployment sizes.

Item #4 can also be a significant consumer of memory. Large data stores (particularly with large files or a high number of files) can create a very large index. Installations with this type of demand should consider separating the Lucene Index Server to a dedicated standalone server for optimum performance (see Section 1.12, "Installing the Lucene Index Server," on page 16).

1.10 Security Guidelines

This section contains security guidelines for the following:

- Role-Based Access Control

  ICEcore controls all access to folders and entries using role-based access controls. See Section 2.6, "Adjust Access Control for the Site," on page 31 to learn more about the default roles and access settings.

  NOTE: Please keep in mind that ICEcore is intended to be used primarily for the sharing of information, so many default access rights lean towards allowing at least universal read access.

- Inbound Email

  You can configure ICEcore to read e-mail and "post" those e-mail messages as entries in a folder. Because e-mail is inherently insecure there is no way to be sure that the sender is who they claim. ICEcore marks the entries posted by e-mail to alert users about their origin.

- Web Services are enabled by default

  The default ICEcore installation allows authenticated access via web services. If you are not using web services, you can disable them by setting `enable="false"` in the `Network/WebServices` section of the installer.xml file.

- RSS feed URLs

  Because RSS readers are outside of the authentication system, the URL provided by ICEcore for an RSS feed embeds some authentication information about the user. This means that the RSS URL must be protected and not shared between users.

  For this reason RSS is not recommended for use on highly sensitive data.

  To disable RSS feeds, modify the RSS section of your `installer.xml file` to: `enable="false"` either during the initial installation or use the installer's `Apply Settings only` option to disable it at any time after installation.

- LDAP (directory service) Proxy User

  You can configure ICEcore (and the portal) to utilize information in the LDAP directory service to provide basic user account information (and group memberships). Access to the LDAP server is done via a configuration page that requires specifying a username and password to LDAP directory. This user should be created in the LDAP directory service with the minimum number of privileges needed to perform the job.

  In particular, all LDAP synchronization activities are one-way, so the proxy user only requires READ access to the directory.

- Mirrored Folder Proxy User

  See Section 2.10, "Mirrored Folders Configuration," on page 46 for more information about the mirrored folder feature of the Enterprise version of ICEcore.

  You can configure ICEcore to use server directories (either the local file system or via file sharing) as repositories for ICEcore folders. Because the ICEcore application server is accessing those directories, the user id that the application server runs as acts as a proxy user for all file system access (i.e., the file system only sees one user accessing the files on behalf of all ICEcore users who have access to the ICEcore folder). This proxy user should be used to configure any local file system access (or shared file access) appropriately.

  If you configure a mirrored folder to a WebDAV or Microsoft Sharepoint directory, the resource driver is configured to use a proxy username and password. The same access control practices should be applied to these resources as with the file system resource driver.

- Password Storage in the Server File System

  A number of application accounts and passwords are stored in the file system. These files should be protected against unauthorized access on the server.

  The `installer.xml` file contains a majority of the account and password information. You should protect this file accordingly. The installation "Apply Setting" phase uses this information to create and/or update a number of configuration files within the application software directory tree.

  These files are outlined below:

  - Database user ids and passwords for the portal and ICEcore software are stored in XML files are stored in:
    ```
    conf/Catalina/localhost/ssf.xml (ICEcore)
    conf/Catalina/localhost/ROOT.xml (Liferay Portal)
    all/deploy/portal-mysql5-ds.xml (JBoss Portal)
    all/deploy/portal-sqlserver-ds.xml (JBoss Portal)
    ```
  - Mirrored folder resource drivers to WebDAV/Sharepoint shares store the proxy user and passwords in:
    ```
    WEB-INF/classes/config/ssf.properties
    ```
  - The email access (both inbound and outbound) may contain usernames and passwords for authentication (e.g., authenticated SMTP). These are stored in:
    ```
    conf/Catalina/localhost/ssf.xml (ICEcore)
    conf/Catalina/localhost/ROOT.xml (Liferay Portal)
    ```

  Some application accounts and passwords are stored in the database. These are protected by application access controls, but are available if access to the database is obtained through other means:

  - LDAP proxy user and password.

- Database access is unencrypted by default

  Depending on your local security guidelines, you may want to encrypt the database connections between the ICEcore and Portal software and their respective databases. Please note that SSL encrypted data between the applications and database servers imposes a performance penalty due to the increased overhead of encrypting/decrypting the retrieved data.

  Support for this is highly dependent on the database client drivers and JDBC connector support and how you are configuring your client and server certificates. You should check with the database vendors on how to set up SSL connections on both the client and server sides of the connection. At minimum you need to update the JDBC URLs in the Database section of the `installer.xml` file (e.g., for MySQL you might add "`useSSL=true&requireSSL=true`" to the options part of the URL).

- LDAP Directory access is unencrypted by default

  See Section 2.4.4, "Secure LDAP/eDirectory Setup," on page 29 for information about configuring ICEcore to use SSL when communicating with the LDAP directory.

- File System Repositories contains unencrypted data

  See Section 1.4, "File System Planning," on page 5 for details about how ICEcore uses the local file system for data storage. These directories contain uploaded information in various formats (both native file formats and potentially a number of rendered formats (e.g., cached HTML versions of files, thumbnails, RSS feeds, etc.) as well as archived data.

  These files are managed exclusively by the ICEcore application software and the file system protections should be set to protect those directories from unauthorized access.

1.11 Document Support

When a file is uploaded into ICEcore it is processed in a number of ways:

1. Textual content is extracted and sent to the search engine. For some file types (e.g., word processing documents) the textual content is obvious. For others, such as graphics files, there may be little or no textual content beyond basic metadata.

2. If possible, a thumbnail (and scaled image - somewhat larger than a thumbnail) of the file is created. The thumbnail of a multi-page document shows the first page.

3. If possible, an browser-only renderable (HTML) version of the file is created. This allows people who do not have the ability to open the file with its native application to get an idea of what is in the file. The rendering is on a "best effort" basis and the level of detail and fidelity of the rendering varies greatly.

The Open and Enterprise versions of ICEcore vary greatly in their ability to perform the above tasks.

The Open version uses OpenOffice to provide access to common Microsoft and OpenOffice document formats, and that is about it.

The Enterprise version uses a licensed technology from the Stellent* company (now part of Oracle*) which provides processing capabilities to a wide spectrum of file types (over 200).

Editing Support

There are two ways of editing files stored in ICEcore:

1. Download the file to your desktop. Edit the file. Upload the file to the entry (as an attachment). A new version of the attachment is created reflecting your changes.   It is possible to manually "lock" the entry if you want to prevent other people from modifying any of the attached files.

2. Certain file types provide an [Edit] button which allows for "edit in place". When available, clicking on the [Edit] button will launch a small Java applet which, in turn, launches the associated edit program for the file. The program accesses the file stored in ICEcore through WebDAV and is subject to the individual file locking protocols that WebDAV provides. Saving the file (or exiting the application) creates a new version of the attachment - no interaction with the browser is needed.

Because the "edit in place" option requires the WebDAV URL support by the application, which is not universally supported by the operating systems, ICEcore must be configured to know which applications are "WebDAV-aware."

The following table shows the planned default configuration of file/document support in ICEcore.

Ext	Description	HTML View		Thumbnails		Application		Edit via	Search	
		Open	Ent	Open	Ent	Windows	Linux	WebDAV	Open	Ent
doc	MS Word	?	X		X	winword	ooffice	X	X	X
xls	MS Excel	?	X		X	excel	ooffice	X	X	X
ppt	MS Powerpoint	?	X		X	powerpnt	ooffice	X	X	X
ods	OO Calc	X	X		X	soffice	ooffice	X	X	X
odg	OO Draw	X	X		X	soffice	ooffice	X	X	X
odp	OO Impress	X	X		X	soffice	ooffice	X	X	X
odf	OO Math	X	X		X	soffice	ooffice	X	X	X
odt	OO Writer	X	X		X	soffice	ooffice	X	X	X
sxw	OO Text	?	X		X	soffice	ooffice	X	X	X
docx	MS Word 2007		X		X	winword		W		X
xlsx	MS Excel 2007		X		X	excel		W		X
pptx	MS Powerpoint 2007		X		X	powerpnt		W		X
123	Lotus 1-2-3		X		X					X
avi	Windows Multimedia		X		X					X
bmp	Bitmap Graphic		X		X					X
cdr	Corel Draw		X		X					X
cgm	Computer Graphics Metafile		X		X					X
dsf	Micrographix Designer		X		X					X
dwg	AutoCAD Drawing Format		X		X					X
dxf	AutoCAD Exchange Format		X		X					X
gif	Graphics			?	X					X
hpgl	HP Graphics Language		X		X					X
htm	HTML		X		X					X
html	HTML		X		X					X
jpg	Graphics			X	X					X
lwp	Lotus WordPro		X		X					X
mdb	MS Access		X		X					X
mov	QuickTime Movie		X		X					X
mp3	Audio		X		X					X
mpeg	Movie		X		X					X
mpg	Movie		X		X					X
mpp	MS Project		X		X					X
pdf	Adobe Portable Document		X		X					X
png	Graphics			?	X					X
pps	MS Powerpoint		X		X	powerpnt				X
ps	Postscript		X		X					X
psd	Adobe Photoshop		X		X					X
qt	QuickTime Movie		X		X					X
rm	Real Movie		X		X					X
rtf	Rich Text Format		X		X	winword	ooffice			X
tif	Graphics		X		X					X
tiff	Graphics		X		X					X
txt	Text		X		X	winword	ooffice		X	X
vsd	MS Visio		X		X					X
wav	Windows Wave Audio		X		X					X
wk1	Lotus Worksheet		X		X					X
wk3	Lotus Worksheet		X		X					X
wk4	Lotus Worksheet		X		X					X
wpd	WordPerfect		X		X					X
xbm	X-Windows Bitmap		X		X					X
xml	XML		X		X					X
xpm	X-Windows Pixmap		X		X					X
zip	Compressed files (PKZIP)		X		X					X

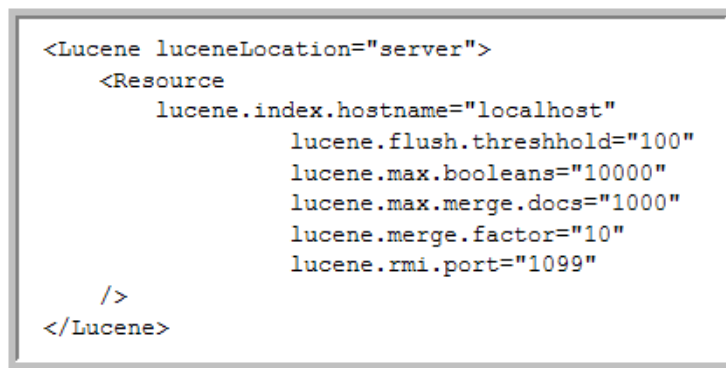## 1.12 Installing the Lucene Index Server

The following procedures show you how to install the Lucene Index Server on a different machine from ICEcore (the Lucene Index Server is included in a full install of ICEcore on the ICEcore Server):

- Section 1.12.1, "Install a Standalone Lucene Index Server for a New ICEcore Application," on page 16
- Section 1.12.2, "Install a Standalone Lucene Index Server for an Existing ICEcore Application," on page 17

NOTE: You need to install JDK (Sun JDK 1.5.0_011 or higher) before installing the Lucene Index Server.

1.12.1 Install a Standalone Lucene Index Server for a New ICEcore Application

1 On the standalone machine, edit the `Installer.xml` file (see "The sample-installer.xml File" on page 47):

```
<Lucene luceneLocation="server">
    <Resource
        lucene.index.hostname="localhost"
                    lucene.flush.threshhold="100"
                    lucene.max.booleans="10000"
                    lucene.max.merge.docs="1000"
                    lucene.merge.factor="10"
                    lucene.rmi.port="1099"
    />
</Lucene>
```

   1a In the `Lucene` section, set `luceneLocation="server"`

   1b If necessary, edit the default rmi port: `lucene.rmi.port="1099"`

2 Run the installer on the standalone machine and choose the option for: `ICEcore Enterprise Lucene Server` (see Section 1.7, "Running the Installer," on page 8).

3 Start the server at the end of the installation:

   3a Change directories to `lucene-server-installation-dir`

   3b Run the `rmiregistry-startup` script in the `bin` directory

   3c Run the `indexserver-startup` script in the `bin` directory

4 On the ICEcore server, edit the `Installer.xml` file:

   4a In the `Lucene` section set `luceneLocation="server"`

   4b Set `lucene.index.hostname` to the hostname of the machine on which you installed the Lucene Index Server (in steps 1-3).

5 Run the normal installation of ICEcore (see Section 1.7, "Running the Installer," on page 8).

1.12.2 Install a Standalone Lucene Index Server for an Existing ICEcore Application

1 On the standalone machine, edit the `Installer.xml` file (see "The sample-installer.xml File" on page 47):

```
<Lucene luceneLocation="server">
    <Resource
        lucene.index.hostname="localhost"
                lucene.flush.threshhold="100"
                lucene.max.booleans="10000"
                lucene.max.merge.docs="1000"
                lucene.merge.factor="10"
                lucene.rmi.port="1099"
    />
</Lucene>
```

   1a In the `Lucene` section set `luceneLocation="server"`

   1b If necessary, edit the default rmi port: `lucene.rmi.port="1099"`

2 Run the installer on the standalone machine and choose the option for: `ICEcore Enterprise Lucene Server` (see Section 1.7, "Running the Installer," on page 8).

3 Shutdown ICEcore on the ICEcore server (see Section 1.8, "Starting and Stopping ICEcore," on page 10).

4 On the standalone machine, check the `lucene-server.properties file` and find the setting for `index.root.dir` (you can edit this setting to change the location of the root directory).

5 Create a "`liferay.com`" subdirectory in the `<index.root.dir>` directory.

6 On the ICEcore server, look at the ssf.properties file and find the `data.root.dir` setting.

7 Copy all the files from the `<data.root.dir>/lucene/liferay.com` directory on the ICEcore server to the `<index.root.dir>/liferay.com directory` you just created on the standalone machine.

IMPORTANT: If you are using ftp, make sure to copy in binary mode.

---

8 For Unix systems, make sure permissions are set so that the ICEcore user has full access to these files and the `liferay.com` directory.

9 Start the server at the end of the installation (if not started already):

   9a Change directories to `lucene-server-installation-dir`

   9b Run the `rmiregistry-startup` script in the `bin` directory

   9c Run the `indexserver-startup` script in the `bin` directory

10 Restart ICEcore (see Section 1.8, "Starting and Stopping ICEcore," on page 10).

1.13 Load-Balancing and Clustering ICEcore

NOTE: In this release, ICEcore does not support session replication across nodes in a cluster.

To set up a scalable, clustered ICEcore configuration, use the following steps as a guideline:

1 Set up a shared file storage that is accessible to all nodes.

ICEcore's Simple File Repository is safe for use in a clustered environment with shared storage that is accessible to all nodes. Setting up shared storage is a platform-specific task.

2 Install and configure the Lucene Index Server.

See "Installing the Lucene Index Server" on page 16 for how to place the Lucene Index Server on a dedicated server system. All cluster nodes will shared this index server.

3 Make sure that the time is the same on all nodes in the cluster.

Using synchronized time services for your cluster is highly advised.

4 Install the ICEcore/portal bundle kit on each cluster node.

IMPORTANT: Since all the nodes share the same database server, it is important not to execute the database-initialization SQL scripts more than once (e.g., use the installer's UPDATE option rather than the FULL INSTALL on all but the first cluster node).

Each node in the cluster should be able to use the same `installer.xml` file. This assures that cluster nodes are configured uniformly.

The following settings must be uniform across the cluster:

- Configure the database connection settings on each node to use the same database.
- Set the file system settings to all point to the same shared file storage server.
- Set the Network settings (e.g., name, port, etc.) to the name of the LOAD BALANCER system.
- In the `Lucene` section, set `luceneLocation="server"` and set `lucene.index.hostname` to the hostname of the machine on which you installed the Lucene Index Server.

5 Set the portal up to work in a clustered environment.

For Liferay, follow the instructions at wiki.liferay.com (http://wiki.liferay.com/index.php/Clustering). If you are interested, Liferay provides additional high availability information at wiki.liferay.com (http://wiki.liferay.com/index.php/High_Availability_Guide).

For the JBoss portal, since ICEcore is bundled with the High Availability edition of the JBoss portal, the default out-of-box configuration is already cluster-ready.

6 Configure the Load Balancer.

There are a variety of load balancing solutions that work with J2EE deployments. The following example configuration uses the balancer module built into the newer Apache (version 2.2.4), and is based on a widely-used sticky session technique. We do not support session sharing/replication among Tomcat instances.

6a Edit Tomcat's `server.xml`.

Add `jvmRoute="jvm<n>"` to the `<Engine name="Catalina" ...>` element, where `<n>` should be an integer unique to each Tomcat instance. For example, assuming you have two Tomcat instances in a cluster, the Catalina engine element should look like the following in each `server.xml` respectively (`jvm<n>` is the name of the worker as declared in the load-balancer):

```
<Engine name="Catalina" defaultHost="localhost" jvmRoute="jvm1">
<Engine name="Catalina" defaultHost="localhost" jvmRoute="jvm2">
```

6b Edit Apache's `httpd.conf file` (in the `<apache installation>/conf` directory).

   1. Uncomment the following three lines:
      ```
      LoadModule proxy_module modules/mod_proxy.so
      LoadModule proxy_ajp_module modules/mod_proxy_ajp.so
      LoadModule proxy_balancer_module modules/mod_proxy_balancer.so
      ```
   2. Append the following section to the end of the file:
      ```
      <Location /balancer-manager>
      SetHandler balancer-manager
      Order deny,allow
      Deny from all
      Allow from 127.0.0.1
      </Location>
      <Proxy balancer://aspenCluster>
      BalancerMember ajp://<tomcat host name 1>:8009 route=jvm1
      BalancerMember ajp://<tomcat host name 2>:8009 route=jvm2
      </Proxy>
      <Location />
      ProxyPass balancer://aspenCluster/ stickysession=JSESSIONID
      </Location>
      ```

   > **NOTE:** In the above, you will have to substitute the real tomcat host names for `<tomcat host name 1>` and `<tomcat host name 2>` respectively. If you have more than two Tomcat instances in the cluster, make an additional line for each.

7 Configure Hibernate to use the cluster-safe second-level cache. For this, you need to modify the cache settings in `/ssf/WEB-INF/classes/config/ehcache-hibernate.xml` for each node in the cluster.

   7a First, uncomment the following section to enable distributed cache:
   ```
   <!--<cacheManagerPeerProviderFactory
   class="net.sf.ehcache.distribution.RMICacheManagerPeerProviderFactory"
   properties="peerDiscovery=automatic,multicastGroupAddress=232.0.0.1,mu
   lticastGroupPort=4446,timeToLive=1" />
   <cacheManagerPeerListenerFactory
   class="net.sf.ehcache.distribution.RMICacheManagerPeerListenerFactory"
   />-->
   ```

   7b Also, uncomment the following section in each cache definition, including the default cache:
   ```
   <!--<cacheEventListenerFactory
   class="net.sf.ehcache.distribution.RMICacheReplicatorFactory" />
   <bootstrapCacheLoaderFactory
   class="net.sf.ehcache.distribution.RMIBootstrapCacheLoaderFactory" />-
   -->
   ```

8 Start the Lucene Index Server first, and then start the application cluster nodes.

Configuring ICEcore

2

Before using ICEcore, you need to perform initial configuration tasks to set up ICEcore so that all default features are operable. The following sections are covered in this chapter:

2.1 Log in as Liferay Site Manager

You need to log in using an administrator account in order to set up ICEcore for your users.

2.1.1 To Log In Using the Administrator Account:

1 Type the ICEcore URL for your company into the browser window:

`http://<yourCompany.com>/portal/portal/default`

The *Sign In* page appears.

2 In the *Login* field, type:

`Admin`

3 In the *Password* field, type:

`Admin`

4 Click *Login*.

The ICEcore Home Page appears. You are now logged in as administrator.

The Liferay portal management links are in the upper-right corner of the page below the *Welcome Mary Admin!* text. This is the name associated with the default administration account (*administrator*). When the name appears in the upper-right corner, you are logged into the system. (You can change the name "Mary Admin" by modifying the user profile for the *administration* account.)

When you begin managing ICEcore, there are only two management levels: site managers (who manage the server machine) and portal managers.

By default, *administrator* is the only member of the Administrators group for the Liferay portal Administrators group. Members of the Administrators group have the right to perform portal management tasks. If you choose, you can add other members to this group, so that they can help manage the portal.

2.1.2 Using the ICEcore Administration Portlet

The ICEcore Administration portlet is designed to provide you with a maximum amount of flexibility when managing resources for your teams.

Access the ICEcore management options via the *ICEcore Administration* portlet.

To Add the ICEcore Administration Portlet to Your Home Page:

1 Click *Add Content* in the upper-right corner.

2 In the portlet access frame that appears in the upper-left corner, click *ICEcore* to view the available ICEcore portlets that you can add.

3 Click the *Add* button next to *ICEcore Administration* to add this portlet to your Home Page.

The *ICEcore Administration* options provides you with access to all the administration tasks controlled by the ICEcore software.

NOTE: Because ICEcore is embedded within Liferay, a portion of user management is delegated to the Liferay. For example, Liferay is responsible for all user authentications using the *Enterprise Admin* portlet.

2.2 Log in as JBoss Site Manager

You need to log in using an administrator account in order to set up ICEcore for your users.

1 Type the ICEcore URL for your company into the browser window:
`http://<yourCompany.com>/portal/portal/default`

2 Click the *Admin* link in the top bar.

3 Click *Portal Definitions*.

4 Click *local./ssf.ss_administration*.

5 Scroll to the bottom of the screen.

6 Type in the *Instance Name* (no spaces): `ICEcoreAdmin`

7 Type a window name into the *Window Name* field under *Content Definition* before clicking *Add*.

NOTE: The recommended window naming convention for ICEcore side is `<portlet name>-window`. So, for instance, to create a window from the `ss_administration-instance`, name it `ss_administration-window`, etc.

---

8 Click *Add*. (You are now in the Portlet Instances).

9 Click *Dashboard* in the top bar.

10 Click *Configure Dashboard*.

11 Select *ICEcoreAdmin* and click *Add to Page Layout*.

12 Click *Dashboard* in the top bar.

NOTE: You now see *ICEcoreAdmin* on the Dashboard.

2.3 Initial Logon

After installing ICEcore/Liferay you need to log in. The ICEcore installation creates one system administrator account and a default format for users.

1. Access your installation with a browser via the following URL:
   `http://yourhost.name.here:8080`

2. At the login screen enter: `admin`

3. Enter the following Password: `admin`
   This brings up the initial Liferay portal window.

4. To add more portlets, click on the "*Add Content*" link in the upper-right-hand corner. This brings up a panel of portlets along the left-hand margin:

   ◆ Expand the *ICEcore* section to add more ICEcore features, such as the *ICEcore Administration* portlet.

   ◆ Expand the *Admin* section to add useful Liferay features such as the *Admin* and *Enterprise Admin* portlets.

   The portlets are placed in the narrow column on the left side. To move a portlet to the wider right column, mouse down on the title and drag it over the right-hand column and release when you see a blue bar with arrows on each side appear.

2.4 Adding Users

There are two methods of managing users:

1. Basic User Management - create and manage individual accounts manually

2. LDAP/eDirectory - synchronize user account management to a corporate directory

Regardless of which method you choose it is important to realize that because ICEcore is embedded within Liferay, a portion of user management is delegated to the Liferay. For example, Liferay is responsible for all user authentications.

The section includes the following topics:

2.4.1 Basic User Management

This capability comes "out of the box" with the product - no additional setup is required.

1 Using the Liferay *Enterprise Admin* portlet, click on the *Users* tab.

Liferay has two portlets, *Enterprise Admin* and *Admin*. Both have *Users* tabs, but they do very different things. Make sure you are using the correct portlet. This brings up a list of current Liferay accounts. You can refer to the Liferay documentation (http://www.liferay.com/web/guest/documentation) for more advanced management.

2 Click *Add*.

3 Fill in the following fields: *First*, *Last Name*, assign a *User ID*, specify the e-mail address, and then click *Save*.

NOTE: Do not use any forbidden characters (`/ \ * ? " < > ; |`) in a user's names.

---

4 Liferay shows an extended form.

5 Click *Save*.

6 Click on the *Password* tab, type in the password, and then click *Save*.
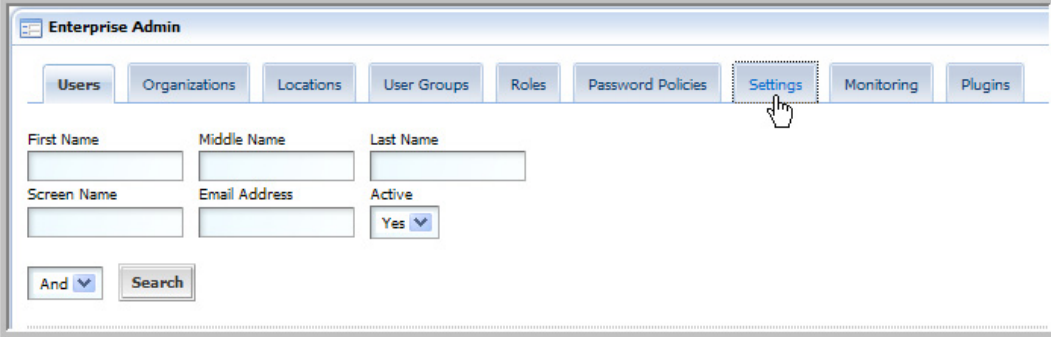
7 Repeat these steps to add additional users.

The account is now ready for use, but not fully created. The administrator and other users cannot see the new user until after the user logs in for the first time. Once the new user logs in, ICEcore creates their user workspace, including a blog, calendar, and file area.

2.4.2 User Management with LDAP/eDirectory
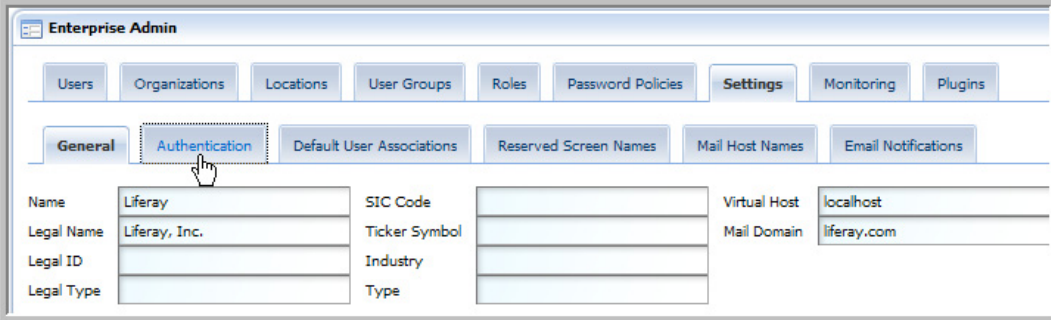
If you want to use a corporate directory as the master reference for user accounts you need to configure both Liferay and ICEcore in a similar manner. The ICEcore LDAP configuration pages are designed to look and work in a similar fashion to Liferay, easing this task significantly. You can refer to the Liferay documentation (http://www.liferay.com/web/guest/documentation) for more detailed information.

1 Using the Liferay *Enterprise Admin* portlet, click on the *Settings* tab (you may need to click on the *>>* tab to see the *Settings* tab).
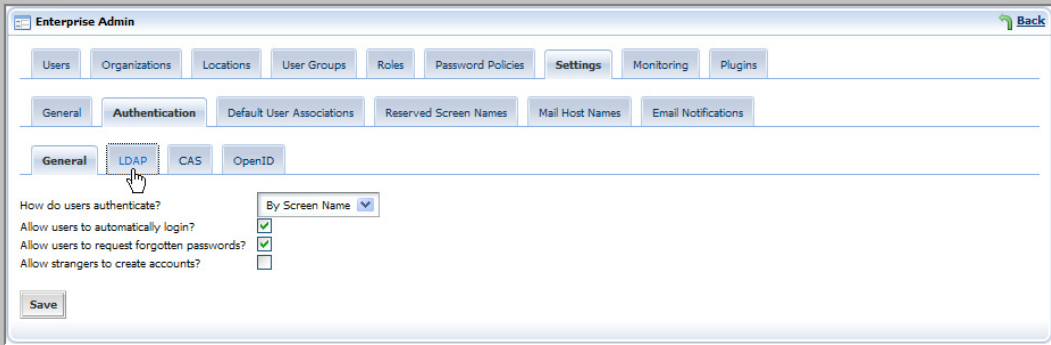
2 Click on the *Authentication* tab.

3 Click on the *LDAP* tab.

4 Fill out the form with the values needed to map to your corporate directory:

4a For the search filter use `uid=@screen_name@` or `cn=@screen_name@`, depending on your site conventions.
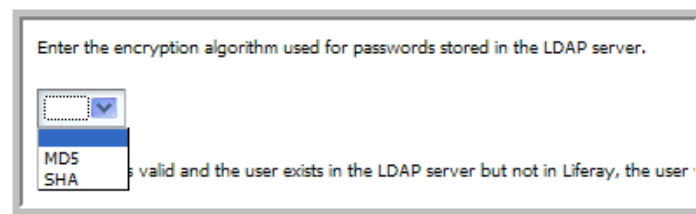
> Enter the search filter that will be used to test the validity of a user. The tokens @company_id@, @email_address@, and @user_id@ are replaced at runtime with the correct values.
>
> (cn=@screen_name@)

4b Liferay checks passwords against LDAP by either doing a comparison between the user typed password and the password stored in the LDAP server or by binding to the LDAP server using the user typed password.

This behavior is controlled by the property `ldap.auth.method` in the `portal.properties` file (`bind` or `password-compare`).

- ◆ Set this value to `bind` (recommended) if you do not want to worry about encryption strategies.

- ◆ When you set this value to `password-compare`, use the Encryption Algorithm drop-down list to specify which algorithm should be used to encrypt the user typed password before conducting password comparison (a blank value means no encryption, MD5 and SHA specify two different algorithms).
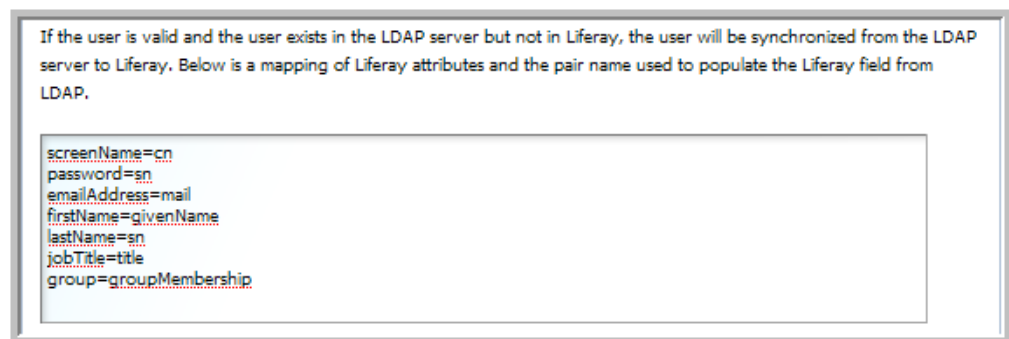
> Enter the encryption algorithm used for passwords stored in the LDAP server.
>
> [▼]
> MD5
> SHA   s valid and the user exists in the LDAP server but not in Liferay, the user

4c Under *If the user...* add: `password=givenName` or `password=sn`.
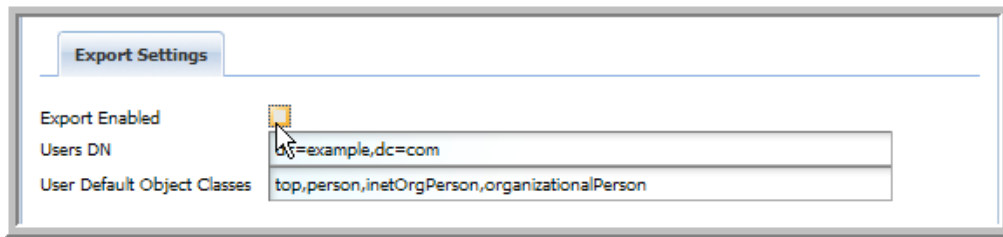

NOTE: We recommend picking one of these passwords (the Liferay default `password=userPassword` does not always appear to work).

> If the user is valid and the user exists in the LDAP server but not in Liferay, the user will be synchronized from the LDAP server to Liferay. Below is a mapping of Liferay attributes and the pair name used to populate the Liferay field from LDAP.
>
> screenName=cn
> password=sn
> emailAddress=mail
> firstName=givenName
> lastName=sn
> jobTitle=title
> group=groupMembership

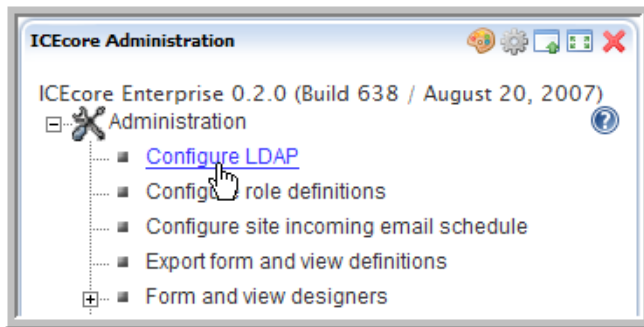**4d** Under *Export Settings*, we recommend deselecting the *Export Enabled* option.

5 Click *Save*.

2.4.3 The ICEcore LDAP Configuration Form

This form is similar to the Liferay form but includes additional information on scheduling synchronization of all users and, optionally, groups.

1 Using the *ICEcore Administration* portlet, click on "*Configure LDAP*."

2 Fill out the form using the corresponding values that were used to configure Liferay. (See below for details on this form).

3 Click *Apply*.

NOTE: Users do not show up in the user list until after they have logged in for the first time.

Connection settings:


```
▷ Schedule
▽ Connection
The LDAP URL format is ldap://host:port/searchdn, where searchdn specifies the initial search context for
users and is optional. For example: ldap://localhost:389/ou=Users,o=Example
URL          ldap://192.168.3.3:389/dc=sleepy,dc=com
Principal    cn=admin
Credentials  *****
```

- URL: `ldap://host:port/dc=foo,dc=bar`, for example: `ldap://192.168.3.3:389/dc=sleepy,dc=com`
- Principal: LDAP principal (user) to authenticate access with, for example: `cn=admin,o=itdepartment`
- Credentials: Above principal's password or authenticating token

Users settings:


```
┌─ Users ──────────────────────────────────────────────────
│
│  LDAP attribute that identifies the user.
│
│  cn
│
│  In the box below, map the internal identifiers to the LDAP attribute names of the user record. Use the
│  following syntax: internalID=ldapAttName
│  ┌─────────────────────────────────────────────────┐▲
│  │ emailAddress=mail                                │▓
│  │ firstName=gn                                     │▓
│  │ firstName=givenName                              │▓
│  │ lastName=sn                                      │▓
│  │ lastName=surname                                 │▓
│  │ phone=telephoneNumber                            │▼
│  │ description=description                          │
│  ☑ Synchronize user profiles
│  ☑ Register LDAP user profiles automatically
│  ☐ Delete users that are not in LDAP
│  ☐ When deleting users, delete associated user workspaces and content
```

- Ldap attribute that identifies the user, for example: `uid` or `cn`

   NOTE: For the LDAP attribute that identifies the user, "`cn`" may be a better choice than "`uid`" for many sites.

- Attribute mapping - This is how you map the LDAP attribute names of the user record to the ICEcore internal identifiers. Syntax is: `ICEcoreId=ldapAttName`, for example:
  - `lastName=sn`
  - `name=uid`
  - ICEcoreIds: `lastName, firstName, name, description, email, Address, phone`
- Select *Synchronize user profiles* (recommended)
- Select *Register LDAP user profiles automatically* (recommended)
- Select others as appropriate

Groups settings:
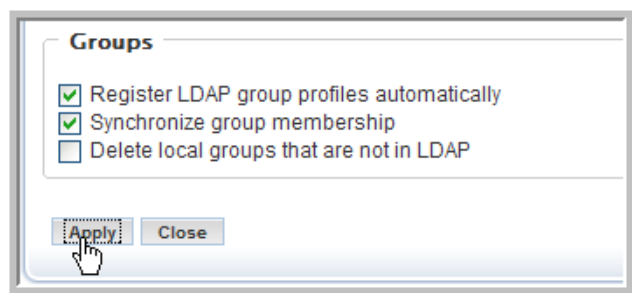
- Select *Register LDAP group profiles automatically* (recommended)
- Select *Synchronize group membership* (recommended)

2.4.4 Secure LDAP/eDirectory Setup

To connect to a secure LDAP server, you need to import the server's certificate into ICEcore's keystore. If the LDAP server is `ldap.company.com`, and it's running on the usual ldaps port (636), then you can follow these steps using the command line interface:

NOTE: An administrator who understands the "openssl" tool should perform this procedure.

1 Make sure you have `openssl` available.

2 Type: `openssl s_client -connect ldap.company.com:636`

3 Copy everything from the '`----BEGIN CERTIFICATE----`' to the '`----END CERTIFICATE----`' lines (inclusive) into a file, say `cert.ldap` (the name does not matter).

4 Type:

```
keytool -import -alias ldap.company.com -keystore /sitescape-team-
0.1.0/liferay-portal-tomcat-5.5-jdk5-4.3.0/conf/.keystore -file
cert.ldap
```

NOTE: The path to the keystore depends on your install path.

5 Restart Tomcat.

NOTE: This technique only works for real certificates. If the LDAP server is using a self-signed certificate, you also need to get the certificate for the "fake" CA and add it to the `cacerts` file on the ICEcore machine. The code at `http://blogs.sun.com/ andreas/entry/no_more_unable_to_find` to get the other certificate appears to be a good example.

6 Make sure you use `ldaps://ldap.company.com:636` as the LDAP URL, rather than the default `ldap://ldap.company.com:389` (note protocol and port number changes).

2.5 Mail Setup

ICEcore e-mail integration is divided into two primary functions:

1. Notification - e-mail messages generated by ICEcore to inform people of events (e.g., new entries, changes) occurring within ICEcore.

2. Posting - the processing of e-mail messages sent to ICEcore with the intent of having the e-mail content added to a particular folder (as a new entry or reply).

System Configuration

As part of installing and configuring ICEcore, the system administrator must supply information related to the address and access to the mail system. E-mail integration is not required and you can configure the level of integration.

The installer.xml file contains sections on e-mail configuration for both notification (Outbound) and posting (Inbound).

Outbound configuration requires the basic information for generating SMTP mail messages: server, port, and optional authentication information.

ICEcore posting works by the system accessing a single e-mail account (sometimes referred to as the "posting account"). Using your e-mail system, multiple e-mail addresses (aliases) can be mapped to this account. ICEcore periodically reads e-mail sent to this account and forwards the messages to individual folders (more on this below).

Create the account using your normal e-mail system management tools. You can configure the posting account to use either POP3 or IMAP. ICEcore needs a host, port, e-mail account id, and password for the posting feature to work.

Setting up Incoming Mail schedule

In the *ICEcore Administration* portlet, click on the *Configure site incoming email schedule* link. This brings up a form that instructs ICEcore when to check the posting e-mail account. You may choose to poll at specific times during the day or at some regular frequency.

The right-hand side of the setup page lists any aliases and the folder that is using that alias. You set up the alias address to folder mapping within the folders themselves (see next section).

Associating an E-mail Address with a Folder

If you enable incoming e-mail the final step that you need to take is to associate a particular e-mail alias address with a folder. When this is done, e-mail sent to that address is "read" by the folder and turned into entries (or replies).

1. Navigate to the folder you want to receive e-mail and click on the *Manage this folder* menu item, then select *Email settings*.

2. Enter the e-mail alias address you want to associate with this folder. Click on the *Apply* button to save the address.

You can optionally set up the notification schedule for this folder at the same time (see next section).

Establishing a Notification Schedule for a Folder

You can configure each folder to send out e-mail messages highlighting activity within the folder.

1. Navigate to the folder you want to send e-mail for and click on the *Manage this folder* menu item, then select *Email settings*.

2. Enable outgoing mail and select the type of schedule you want for notification. You can configure the schedule for specific times of the day or a regular frequency. You also need to specify who is to receive the e-mail. This can be a combination of users, groups, and arbitrary e-mail addresses.

3. Click *Apply* to save the schedule.

2.6 Adjust Access Control for the Site

One of your first tasks as a site manager is to set the access roles to control how different users can view and participate in the site workspaces according to what access role they are assigned. All Access Roles are assigned to users in individual workspaces or folders, except for the Site Administration access role, which grants access to the whole site. There are specific Role Definitions that you can edit to accomplish this. See the default Role Definitions below.

Key Ideas to Keep in Mind:

* Understand the default access control settings and the philosophy behind them (quick team formation, open communications, etc.)

* Determine the values and needs of your organization and adjust the access control settings accordingly

* The best way to delegate administrative tasks is to create groups and use the access-control tools to delegate folder and workspace administration accordingly

2.6.1 Default Role Definitions

The following are the default Role Definitions, which should more than enough to configure your site, though your site administrator can add new Role Definitions if required.

* *Workspace and Folder Administrator*

  Assigns every access right, but *Site Administration*, to users for the specific workspaces and folders that the administer.

* *Participant*

  Assigns the following default access rights to users for any workspaces or folders in which they are participants:

  * Add Comments
  * Create Entries
  * Delete His or Her Own Entries
  * Modify His or Her Own Entries
  * Read Entries

* *Site Administrator*

  Has every access right selected by default. These rights apply to every workspace and folder.

- *Team Member*

  Assigns the following default access rights to users for any workspaces or folders in which they are team members:
    - Add Comments
    - Add Folders
    - Add Workspaces
    - Create Entries
    - Delete Entries
    - Delete His or Her Own Entries
    - Generate Reports
    - Manage Community Tags
    - Modify Entries
    - Modify His or Her Own Entries
    - Read Entries

- *Visitor*

  Assigns the following default access rights to users for workspaces or folders to which they are only assigned as visitors:
    - Add Comments
    - Read Entries

- *Workspace Creator*

  This Role Definition is a special definition assigned to All Users at the Top Team Workspace to give every user the right to create a new Team Workspace. The Site Administrator can edit the Top Team Workspace access rights so that only specific users can add Team Workspaces, see Section 2.6.3, "Edit Default Team Workspace Access Rights," on page 34.

2.6.2 To Change a Default Role Definition:

For example, you may choose to prevent visitors from adding comments in the site.

1 In the *ICEcore Administration* portlet, click *Configure Role Definitions*.
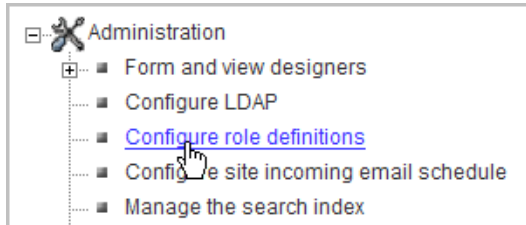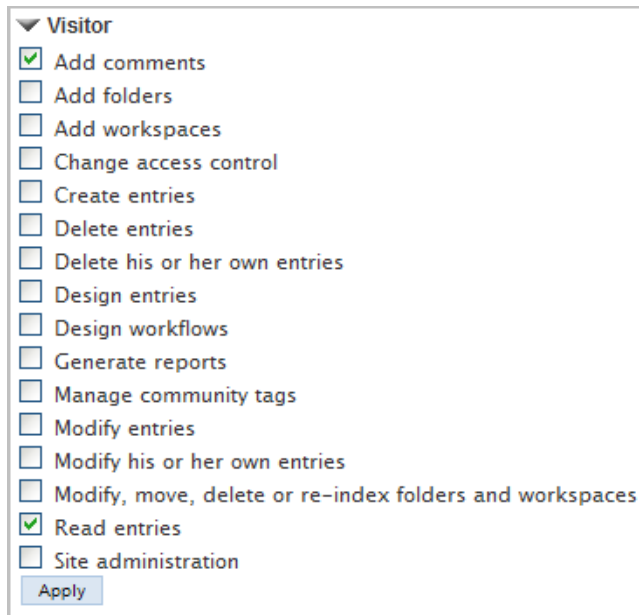

The *Configure Roles* page appears.
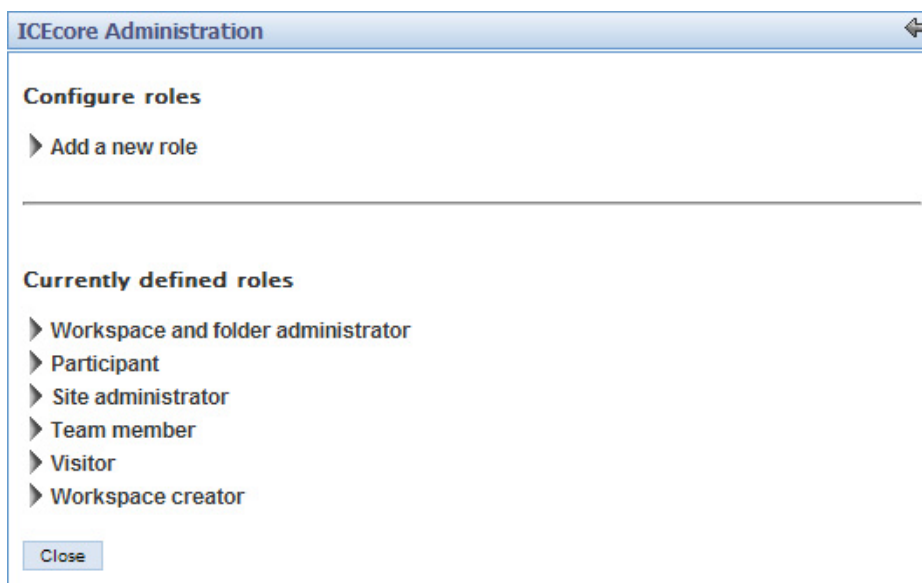
2 Click *Visitor*.
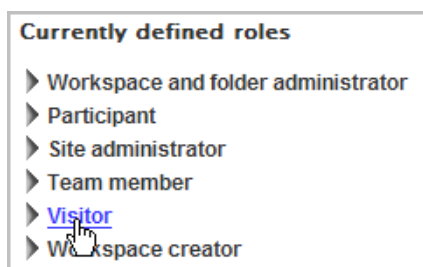
3 Under *Visitor*, deselect the *Add Comments* option, and then click *Apply*.

4 Click *Close* to return to your Home Page.

Visitors to your site can now view entries, but can no longer add comments.

2.6.3 Edit Default Team Workspace Access Rights

Every workspace and folder has their own access rights. Access rights are the assignment of the Role Definitions to groups and individuals for a workspace or folder. When you create a new workspace, it starts off with the default access rights according to the type of workspace you created: Global, Personal, or Team.


NOTE: A personal workspace is created when a user signs into ICEcore for the first time.

The Site Administrator can edit these default settings, for example, you might want to edit the Top Team Workspace access rights so that only specific users or groups can add Team Workspaces.

First you want to create a *Team Creator* group to be in charge of Team Workspace creation, and then you want to remove the *Workspace Creator* Role Definition from *All Users* and assign it to the *Team Creator* group in the Top Team Workspace access rights. The site administrator can add new users to the *Team Creator* group at any time.
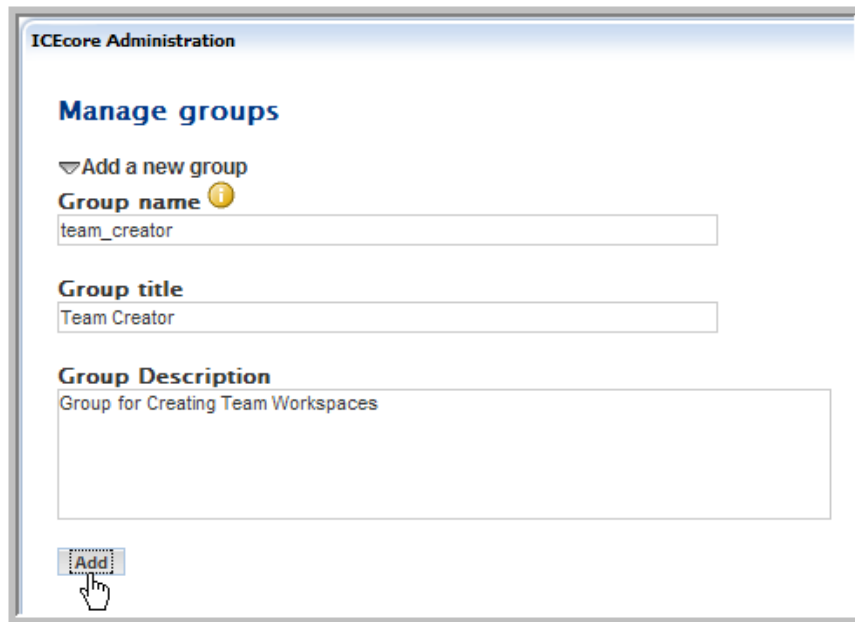
Create the Team Creator Group:

1 In the *ICEcore Administration* portlet, click *Manage Groups*.
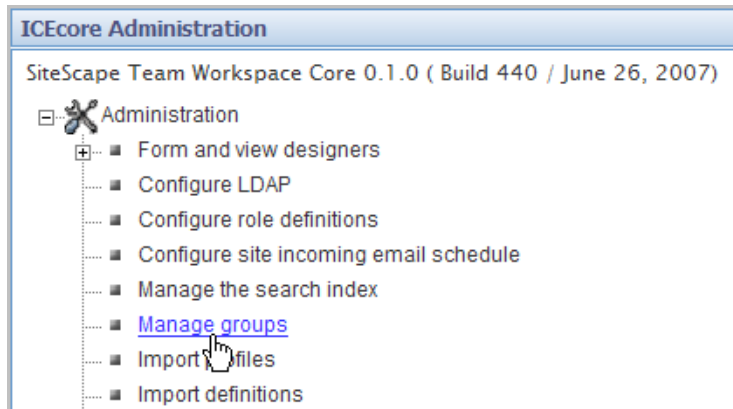
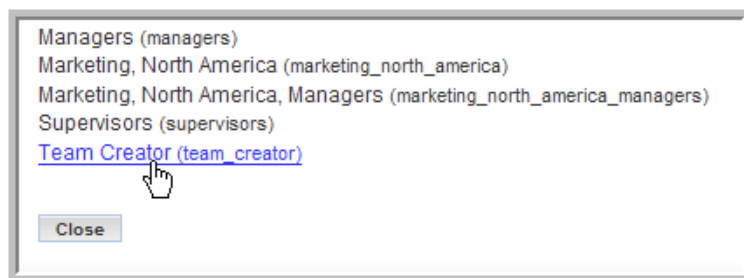**2** In the *Manage Groups* window, click *Add a New Group*.
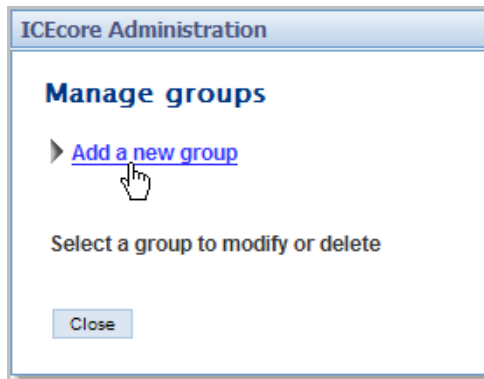
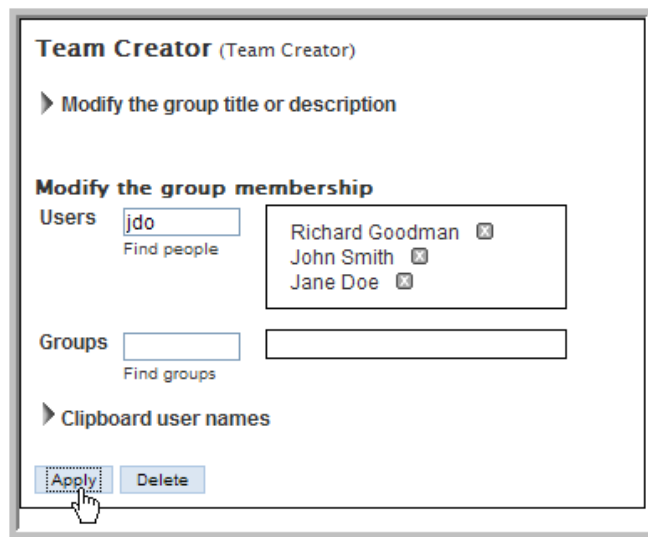**3** Enter the new group's name, title, description, and then click *Add*.

The new group appears on the page.

4 Under *Select a Group to Modify or Delete*, click the *Team Creator (Team Creator)* group.

5 Add users to the group and click *Apply*.

6 Click *Close*.

NOTE: See the Online Help or ICEcore User Guide for details on adding users to groups.

Grant the Team Creator Group Sole Team Workspace Creation Rights:

1 Click *Team Workspace*.
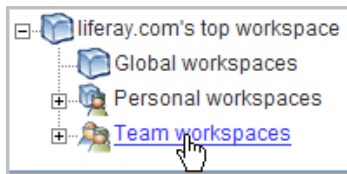
2 Select the *Manage > Access Control* menu item.
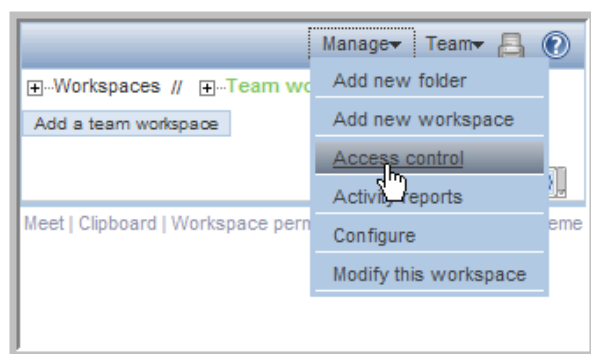
The *Configure Access Control* page appears. This page allows you to assign the Role Definitions to specific groups and users from the workspaces and folders. The current page controls the access rights for the Top Team Workspace area.

3 Click *Add a Group* in the *Access Rights* table.

Add user names from clipboard

		Add a role ▾				
		Workspace and folder administrator	Participant	Workspace creator	Site administrator	Visitor
	Owner of workspace or folder	✓ ☑	☐	☐	☐	☐
	Team members	☐	✓ ☐	☐	☐	☐
Add a group ▾	Group title — Group name	Workspace and folder administrator	Participant	Workspace creator	Site administrator	Visitor
	All users — allUsers	☐	✓ ☑	☑	☐	✓ ☐
Add a user ▾	User title — User name	Workspace and folder administrator	Participant	Workspace creator	Site administrator	Visitor
	administrator — administrator	☐	☐	☐	✓ ☐	☐

Save changes

4 Start typing `Team Creator` in the *Add a Group* dialog that appears and select *Team Creator* from the drop-down list that appears.

Add a group
Team
Team Creator

The Team Creator groups appears in the *Access Rights* table.

5 Deselect the *Workspace Creator* option for the *All Users* group and select the same right for the *Team Creator* group.

Add a group ▾	Group title	Group name	Workspace and folder administrator	Participant	Site administrator	Visitor	Workspace creator
	All users	allUsers	☐	✓ ☑	☐	✓ ☐	☐
	Team Creator	Team Creator	☐	☐	☐	☐	☑
Add a user ▾	User title	User name	Workspace and folder administrator	Participant	Site administrator	Visitor	Workspace creator

6 Click *Save Changes*.

Save changes
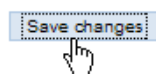
7 Click *Close*.

You have now created a specific group to control the creation of Team Workspaces. This is an example of how you use Role Definitions and access rights to configure your site. You want to map out the access issues for your site so you can edit the default Role Definitions and default access rights for your workspaces prior to granting all your users access to the site.

2.7 Create Your Initial Workspaces

There are three types of workspaces in ICEcore: Global Workspaces (company wide), Personal Workspaces (individual), and Team Workspaces (smaller teams). Once a new workspace is created, every sub-workspace and sub-folder inherits its access rights from the parent workspace by default. The workspace or folder administrator can de-select this option for any individual sub-workspace and sub-folder (on the *Access Control* page for the individual workspace or folder).

Planning the initial content for your site is an important step in regards to how your users learn and use the site. Without some content, users are lost. However, too much content (especially empty containers and a complex structure) might cause users to have trouble mapping to the real work they have to do. So, before letting end users into the installation, the Global Workspace should have enough content to engage them, but not so much as to overwhelm them. Also, we have seen time and again that a workspace hierarchy and set of dedicated applications are best developed in parallel with users using the product and providing feedback about what best serves their needs.

The best approach is to plan out a tight minimal set of content in the Global Workspace to provide the end users with a functional site that they can quickly navigate and start using.

Creating Teams

The team creation process can be simplified with some up front planning:

- Although, by default, anyone can create a team (unless you edit the default access rights, see Section 2.6.3, "Edit Default Team Workspace Access Rights," on page 34) the process is a lot easier if a site administrator creates group names for teams before team creation occurs.

- Thinking through how you want to architect group names is a useful up front task.

- Access control is greatly simplified and enhanced by utilizing well-planned group names for your site.

2.7.1 Create an Administration Team Workspace

NOTE: You should create an *Administration* group first to simplify the process for editing your administration access rights. You can then add this group to the administration team and set the access rights to this group. In the future, you can add or delete users from this administration group and not worry about editing the administration team's access rights for individual members since they are assigned correctly to the group. Assume the `admin` group now exists.

1 From your Home Page, click *Team Workspaces*.
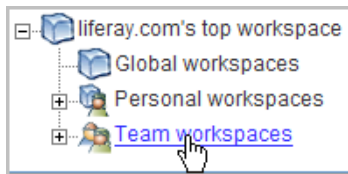
2 Click *Add a Team Workspace*.
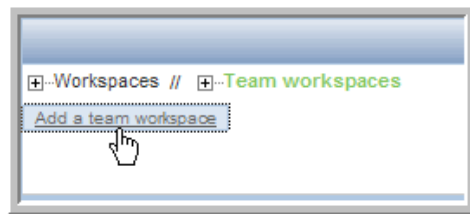
3 Type in a *Workspace Title* for the new workspace.

4 Select the team members (add the `admin` group, which we will also use for setting access rights so that you only have to control membership to this group to control administrative access rights and administration workspace membership).

NOTE: See the Online Help or the ICEcore User Guide for details on selecting users.

5 Select all the initial *Workspace Folders* you want to create in this workspace.

6 Click *OK*.

2.7.2 Set the Administration Team Access Rights

1 From the *ICEcore Administration Team* workspace, select the *Manage > Access Control* menu item.
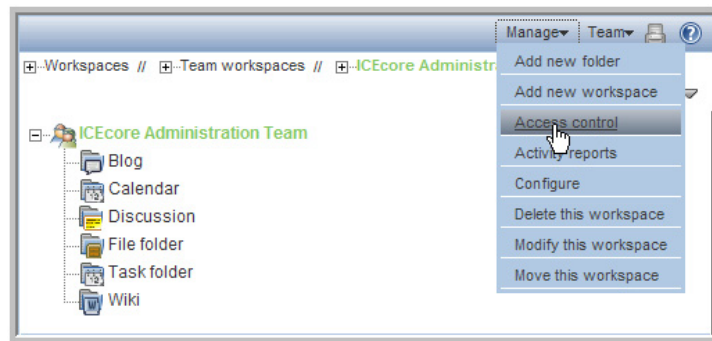
2 In the Access Rights table, click *Add a Group*.

3 Start typing in `admin`, and select *admin* from the drop-down list that appears.

4 For the *admin* group, select the *Workspace and Folder Administrator*, *Participant*, and *Team Member* roles.

Add a group ▾	Group title	Group name	Workspace and folder administrator	Participant	Team member	Workspace creator
	admin	ICEcore Administration	☑	☑	☑	☐

5 Click *Save Changes*.

6 Click *Close*.

2.7.3 Using the Root Team Workspace

You can set any workspace to be a "root" team workspace, which allows anyone with the correct access rights to add workspaces under the "root" workspace. A "root" team workspace has the *Add a team workspace* button available to anyone with the appropriate access rights.

An administrator can set a workspace to be a "root" team workspace temporarily, while the sub-workspaces your company needs to set up are added, or permanently so that users can create additional workspaces under the "root" team workspace on a continuous bases. How you configure a specific area depends on what the workspaces are used for how much control you want the users to have over the layout of the site.

Configuring a Workspace to be a Root Team Workspace:

1 From the *ICEcore Administration Team* workspace, select the *Manage > Configure* menu item.
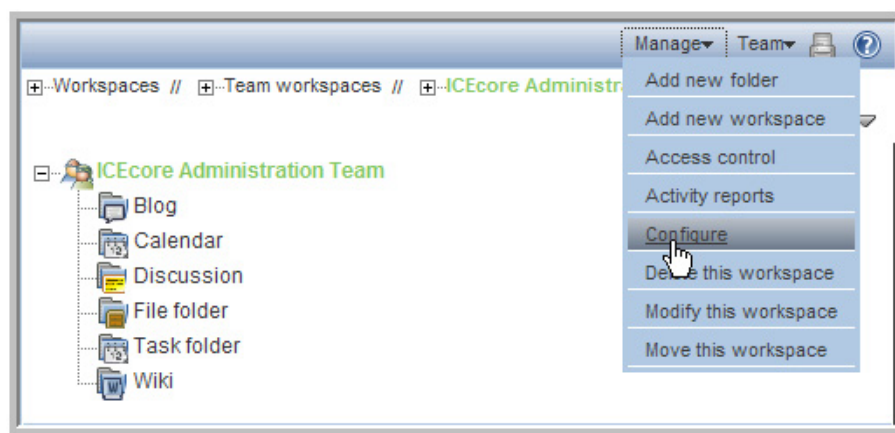
2 Select the *Team workspace root* option and click *Apply*.
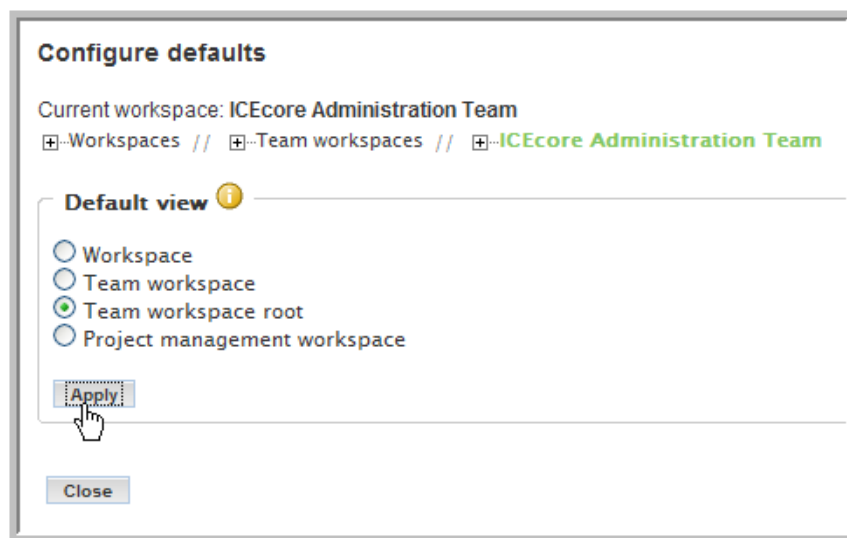
NOTE: When choosing for a workspace, you can select the default "Workspace" definition. If you want to track project tasks and milestones based on task completion, you can select the "Project management workspace" definition. Finally, when choosing for a team workspace, select "Team workspace root" for workspaces that you want to display the *Add a team workspace* button. If your team workspace is organizational in nature and not intended to have team workspaces as its subworkspaces, select the "Team workspace" definition (which omits the button for team creation).

3 Click *Close*.

The Add a team workspace button is now available in the *ICEcore Administration Team* workspace.

NOTE: Since only members (administrators) of the `admin` group have access to this workspace, you can make it a permanent Team workspace root, so any administrator can create sub-workspaces under this one.

2.8 Invite Users to the Site

Most end users require some minimal guidance before entering the site. They need to be invited (there is no automatic way to do this, unless you invite them during team creation (ICEcore is designed to be team-centric). The invitation should contain the URL to the site. Also, you may want to include the ICEcore Quick Start Guide and ICEcore User Guide in the e-mail invitation.

Your organization may want to run some training sessions before having people enter the site. As another option, the administrators may want to customize the getting-started information available on the static web page off the *Welcome* portlet.

2.9 Set Up E-mail for a Workspace

To set up notifications in a workspace, enable them on one of the top level folders in your workspace first. Once this is done, e-mail notifications are enabled on all sub-folders. For postings, you need to configure the workspace with a valid e-mail alias. See your e-mail administrator to get a valid e-mail alias address for your workspace.

1 From your workspace, select the top level folder for which you want to enable e-mail.
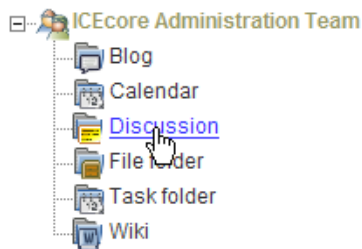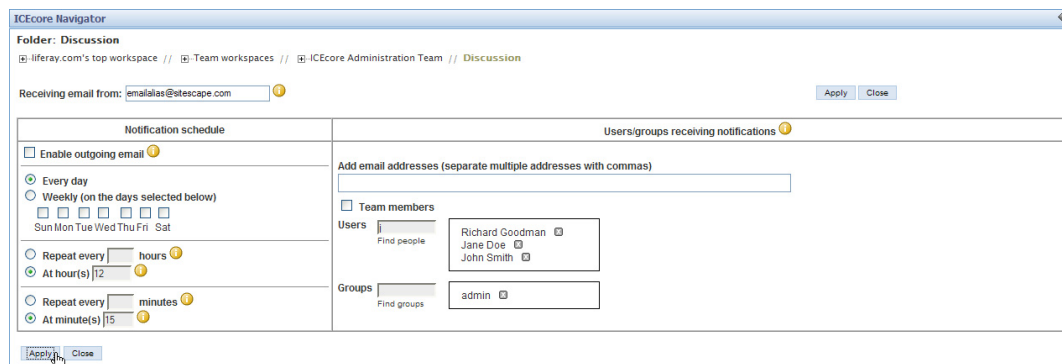
2 Select the *Manage > Email Settings* menu item.
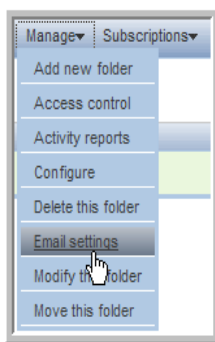
3 Type in the e-mail alias you received from your e-mail administrator in the *Receiving Email From* field.

This enables the folder to receive e-mail posts.

4 Configure the e-mail *Notification Schedule* and add the users, groups, and any individual e-mail addresses you want to receive e-mail notifications, and then click *Apply*.

NOTE: See the Online Help and the ICEcore User Guide for more details.

2.10 Mirrored Folders Configuration

NOTE: Mirrored Folders are available in the Enterprise Edition only.

A mirrored folder is an ICEcore folder that uses a server file system directory as its file storage area instead of the normal ICEcore repository. Typically the directory is a "file share", accessed via normal file sharing mechanisms. ICEcore attempts to keep its knowledge about the folder contents in sync with whatever is in the directory.

Because of the way mirrored folders are configured they are intended to be used to bring common, relatively static, file shares into the ICEcore environment -- they are not appropriate for individual file shares. ICEcore can then be used to add additional metadata around these files, including ICEcore-specific access controls.

The server directories that are to be made available to ICEcore must be specified in the server configuration files. The `installer.xml` has a section devoted to specifying mirrored folder resource drivers. These drivers then make the files in the specified directory available to the ICEcore folder(s). It is important to note that access to the directories is done by the ICEcore process, and the user id that ICEcore is running as acts as a proxy for all ICEcore users.

To Create a Mirrored Folder:

1 Add a "MirroredFolder" section to the `installer.xml` file. This creates a Mirrored Folder Resource Driver. (You may want to use one of the disabled samples as a template.)

Remember to set the "enabled" attribute to "true" and specify a unique id and title, the path to the directory to share, and the users and/or groups that can utilize this resource. To prevent accidental modifications to the file share, set the "readonly" attribute to "true".

After updating your `installer.xml` file, you need to run the ICEcore installer with the "Apply settings" option, and then restart ICEcore to create the resource drivers.

2 Log into ICEcore as one of the users you specified in the mirrored folder resource driver (or as a member of one of the specified groups).

3 In ICEcore create a folder of type *File folder*.

4 Within the folder, select the *Manage > Modify this folder* menu item.

5 Select the *Mirror external folders* option.

6 Select the mirrored folder resource driver that you created in step 1.

7 Optionally, you can specify a subdirectory within the resource driver's root directory structure that you want this folder to mirror.

8 Click *OK* to make the folder a mirrored folder.

NOTE: Once you make a folder a mirrored folder, it can not be reverted back to a regular folder, and the information you provided (i.e., resource driver name and path) can not be subsequently changed.

9 Perform initial synchronization/loading by selecting the *Manage this folder > Synchronize* menu item from the folder listing.

NOTE: For the current release of ICEcore only synchronous/manual synchronization is supported.

The sample-installer.xml File

<div style="text-align: right; font-size: 3em;">A</div>

The `sample-installer.xml` file is shown below:

```
<!--                                                       -->
<!--            ICEcore Installation Configuration File    -->
<!--                                                       -->


<ICEcoreConfig version="4">

     <Environment>
        <!--  The path to JAVA_HOME -->
          <JDK JAVA_HOME="" type="Sun" />

          <!--  What userid to run as (Linux-only)        -->
          <!--  Also what userId and groupId to use as     -->
          <!--  owners of the data directories.            -->
          <Ids userId="" groupId=""/>

     </Environment>

   <!--                                                    -->
   <!--                   Network Settings                 -->
   <!--                                                    -->
   <!--   The host name or IP address of the server must be -->
   <!--   specified here.  The default, localhost, is only  -->
   <!--   appropriate for test configurations with no remote -->
   <!--   access.                                          -->
   <!--                                                    -->
   <!--   If you have a dedicated server, setting the port  -->
   <!--   to "80" and/or securePort to "443" will avoid having -->
   <!--   to specify a port number in browser URLs.        -->
   <!--                                                    -->
   <!--   NOTE: On Linux/UNIX based systems, it's very dangerous -->
   <!--   to run this server on any port number less than 1024, -->
   <!--   since that would require the web server to run as the -->
   <!--   root user.  If you must run on a port lower than 1024, -->
   <!--   please see the ICEcore documentation referring to port -->
   <!--   forwarding via iptables.                          -->
   <!--                                                    -->
   <!--                                                    -->
   <!--   A default certificate is supplied for SSL connections. -->
   <!--   You should replace this with your certificate.    -->
   <!--   This can be placed in the conf/.keystore file or  -->
   <!--   change the keystoreFile attribute to point to the -->
   <!--   certificate.                                     -->
```

```
<Network>
    <Host name="localhost"
          port="8080"
          securePort="8443"
          shutdownPort="8005"
          ajpPort="8009"
          keystoreFile=""
          />
    <WebServices enable="true" />
</Network>



<!--                                                        -->
<!--              Memory (RAM) Settings                     -->
<!--                                                        -->
<!--  ICEcore requires a minimum of 512m to operate.       -->
<!--  1g is recommended for basic production.               -->
<!--  Generally do not allocate more than 75% of available  -->
<!--  physical memory.                                      -->
<!--                                                        -->
<!--  Specify amounts as  Nm for N megabytes (e.g., 1500m) or  -->
<!--  Ng for N gigabytes (e.g., 3g)                         -->
<!--                                                        -->

<Memory>
    <JavaVirtualMachine mx="1g" />
</Memory>



<!--                                                        -->
<!--              File System Configuration                 -->
<!--                                                        -->
<!-- Modify the configName to your desired configuration    -->
<!-- in the FileSystem element below.  You must set the     -->
<!-- configName to the exact configuration in the file:     -->
<!--     basic     - Simple one-directory setup             -->
<!--     advanced  - Advanced multiple-directory setup      -->
<!--                                                        -->
<!-- WARNING!  Changing a directory path does NOT relocate   -->
<!-- data after the product has been installed.  You must   -->
<!-- coordinate any changes here with appropriate file system  -->
<!-- modifications (including directory protections and     -->
<!-- ownership where applicable).                           -->
<!--                                                        -->

<FileSystem configName="basic">

  <!-- The basic configuration only requires that you  -->
  <!-- specify a root directory for the data and       -->
  <!-- we'll take care of the rest.                     -->

  <Config id="basic">
    <RootDirectory path="/home/icecoredata"  />
  </Config>
```

```
<!-- The advanced configuration requires that you    -->
<!-- specify individual directory locations.         -->
<!-- Add path attributes for those directories you   -->
<!-- want to locate elsewhere.                        -->

<Config id="advanced">
  <RootDirectory path="/home/icecoredata"  />
  <FileRepositories />
  <ArchiveStore    />
  <CacheStore      />
  <LuceneIndex     />
</Config>


<!-- The liferay data dirs configuration allows you to    -->
<!-- change the directories that liferay uses for         -->
<!-- it's internal data directories.  If you want to      -->
<!-- change these, change the use attribute from "default" -->
<!-- to "custom". NOTE: If you change these after you have -->
<!-- already started using liferay, you'll need to copy   -->
<!-- all the data from the default dirs to the new dirs    -->
<!-- BEFORE you restart the server!                       -->

<LiferayDataDirs use="default">
  <RootDirectory path="/home/icecoredata/liferay"  />
  <DocumentLibraryRoot dir="documentlibrary/root" />
  <DocumentVersionLibrary dir="documentlibrary/vroot" />
  <JackRabbit dir="jackrabbit" />
  <AutoDeploy dir="deploy" />
  <Lucene dir="lucene" />
</LiferayDataDirs>

</FileSystem>

<!--                                                      -->
<!--             Database Configuration                   -->
<!--                                                      -->
<!-- Modify the configName to your desired configuration  -->
<!-- in the Datatabase element below.  You must set the   -->
<!-- configName to the exact configuration in the file:   -->
<!--     MySQL_Default     - For MySQL                    -->
<!--     SQLServer_Default  - For Microsoft SQL Server    -->
<!--                                                      -->
<!-- Change the Resources for the configuration you chose  -->
<!-- (the defaults are pretty good for a simple configuration -->
<!-- with the database running locally, but you'll probably -->
<!-- have different passwords!).                          -->

<Database configName="MySQL_Default">

   <!--                                                   -->
   <!--                 MySQL_Default                     -->
   <!--                                                   -->
```

```
            <Config id="MySQL_Default" type="MySql">
                <Resource for="liferay"
                    driverClassName="com.mysql.jdbc.Driver"
                    url="jdbc:mysql://localhost:3306/
lportal?useUnicode=true&amp;characterEncoding=UTF-8"
                    username="root"
                    password="root"
                />
                <Resource for="jboss"
                    driverClassName="com.mysql.jdbc.Driver"
                    url="jdbc:mysql://localhost:3306/
jbossportal?useUnicode=true&amp;characterEncoding=UTF-8"
                    username="root"
                    password="root"
                />
                <Resource for="icecore"
                    driverClassName="com.mysql.jdbc.Driver"
                    url="jdbc:mysql://localhost:3306/
sitescape?useUnicode=true&amp;characterEncoding=UTF-8"
                    username="root"
                    password="root"
                />
            </Config>


        <!--                                              -->
        <!--                  SQLServer_Default            -->
        <!--                                              -->

        <Config id="SQLServer_Default" type="SQLServer">
                <Resource for="liferay"
                    driverClassName="net.sourceforge.jtds.jdbc.Driver"
                    url="jdbc:jtds:sqlserver://localhost/
lportal;SelectMethod=cursor"
                    username="sa"
                    password="sa"
                 />
                <Resource for="jboss"
                    driverClassName="net.sourceforge.jtds.jdbc.Driver"
                    url="jdbc:jtds:sqlserver://localhost/
jbossportal;SelectMethod=cursor"
                    username="sa"
                    password="sa"
                 />
                <Resource for="icecore"
                    driverClassName="net.sourceforge.jtds.jdbc.Driver"
                    url="jdbc:jtds:sqlserver://localhost/
sitescape;SelectMethod=cursor"
                    username="sa"
                    password="sa"
                 />
            </Config>
```

```xml
    <!--                                                             -->
    <!--                    Oracle_Default                           -->
    <!--                                                             -->

    <Config id="Oracle_Default" type="Oracle">
        <Resource for="liferay"
            driverClassName="oracle.jdbc.driver.OracleDriver"
            url="jdbc:oracle:thin:@//localhost:1521/orcl"
            username="lportal"
            password="pw"
         />
        <Resource for="icecore"
            driverClassName="oracle.jdbc.driver.OracleDriver"
            url="jdbc:oracle:thin:@//localhost:1521/orcl"
            username="sitescape"
            password="pw"
         />
    </Config>


</Database>


<!--                                                             -->
<!--              Lucene Configuration Settings                  -->
<!--                                                             -->
<!--                                                             -->
<!--      The Lucene index can be run "local" (within           -->
<!--      the context of this application) or "server"          -->
<!--      (run as it's own server).  Additionally it            -->
<!--      can be run as it's own server on this system          -->
<!--      or on a remote system.                                -->
<!--                                                             -->
<!--      Note: The rmi port need only be set if running        -->
<!--      in server mode. (And then, only if the default        -->
<!--      port cannot be used.                                  -->


<Lucene luceneLocation="local">
    <Resource
        lucene.index.hostname="localhost"
                lucene.flush.threshhold="100"
                lucene.max.booleans="10000"
                lucene.max.merge.docs="1000"
                lucene.merge.factor="10"
                lucene.rmi.port="1099"
    />
</Lucene>
```

```
<!--                                                      -->
<!--          RSS Configuration Settings                  -->
<!--                                                      -->
<!--  RSS feeds are inherently insecure as they do not    -->
<!--  use the standard authentication mechanism.  If you  -->
<!--  do not want to have users create RSS subscriptions  -->
<!--  set the enable property to "false"                  -->
<!--                                                      -->
<!--  If you have RSS feeds enabled you can tune the maximum -->
<!--  number of days to keep in the feed and the the maximum -->
<!--  number of days to keep updating a feed when there are  -->
<!--  no clients reading it.                               -->
<!--                                                      -->
   <RSS enable="true">
         <Feed max.elapseddays="31" max.inactivedays="7" />
   </RSS>


<!--                                                      -->
<!--             Email Configuration Settings             -->
<!--                                                      -->
<!--  Edit the Outbound and Inbound settings as required. -->
<!--                                                      -->
<!--                                                      -->
<!--  For inbound mail (postings) you need to specify either -->
<!--  pop3 or imap (or pop3s/imaps for SSL connections to -->
<!--  mail servers), and fill out the settings for which one -->
<!--  you choose.  These settings are not used until you  -->
<!--  enable incoming email within the product.  If you do -->
<!--  not plan on using inbound email, you can ignore these -->
<!--  settings.                                            -->
<!--                                                      -->
<!--                                                      -->

<EmailSettings>

    <Outbound>
        <Resource
            mail.transport.protocol="smtp"

            mail.smtp.host="mailhost.yourcompany.com"
            mail.smtp.user="icecore@yourcompany.com"
            mail.smtp.password=""
            mail.smtp.auth="false"
            mail.smtp.port="25"

            mail.smtps.host="mailhost.yourcompany.com"
            mail.smtps.user="icecore@yourcompany.com"
            mail.smtps.password=""
            mail.smtps.auth="false"
            mail.smtps.port="465"

        />
    </Outbound>
```

```
<Inbound>
    <Resource
        mail.store.protocol="pop3"

        mail.pop3.host="localhost"
        mail.pop3.auth="true"
        mail.pop3.user="popEmailUserId"
        mail.pop3.password="passwordHere"
        mail.pop3.port="110"

        mail.pop3s.host="localhost"
        mail.pop3s.auth="true"
        mail.pop3s.user="popEmailUserId"
        mail.pop3s.password="passwordHere"
        mail.pop3s.port="995"

        mail.imap.host="localhost"
        mail.imap.auth="true"
        mail.imap.user="imapEmailUserId"
        mail.imap.password="passwordHere"
        mail.imap.port="143"

        mail.imaps.host="localhost"
        mail.imaps.auth="true"
        mail.imaps.user="imapEmailUserId"
        mail.imaps.password="passwordHere"
        mail.imaps.port="993"

        mail.transport.protocol="smtp"

        mail.smtp.host="localhost"
        mail.smtp.auth="false"
        mail.smtp.user="icecore@yourcompany.com"
        mail.smtp.password=""
        mail.smtp.port="25"

        mail.smtps.host="localhost"
        mail.smtps.auth="false"
        mail.smtps.user="icecore@yourcompany.com"
        mail.smtps.password=""
        mail.smtps.port="465"
    />
</Inbound>
</EmailSettings>
```

```
<!--                                                       -->
<!--              Presence Configuration Settings          -->
<!--                                                       -->
<!--                                                       -->
<!--  Use thse settings to link your Teaming and Zon       -->
<!--  servers together.   Leave the presence.service.enable -->
<!--  setting at at false if you do not use the conferencing -->
<!--  realtime (Zon) software.                             -->
<!--                                                       -->
<!--  The values to fill in this section are obtained when -->
<!--  Zon has been installed and configured.  If you don't -->
<!--  know them now, you can update this configuration later -->
<!--  and apply the settings.                              -->
<!--                                                       -->
<!--  The jabber.server is IP or host of the Zon XML Router -->
<!--                                                       -->
<!--  The default Zon admin.id is admin, and default password -->
<!--  is also admin.  Change the admin.passwd to match the -->
<!--  Zon administrator password you have set.             -->
<!--                                                       -->
<!--  The jabber.domain is the host name of the XML router -->
<!--                                                       -->
<!--  The community.id is the name of the community you    -->
<!--  created with the Zon console.                        -->
<!--                                                       -->
<!--  Change the hostname part of the zon.url to the ip or -->
<!--  host of the Zon Web Portal (don't change the port or -->
<!--  the rest the URL).                                   -->
<!--                                                       -->

    <Presence>
        <Resource
            presence.service.enable="false"
            presence.service.jabber.server="zon-server.yourcompany.com"
            presence.broker.admin.id="admin"
            presence.broker.admin.passwd="admin"
            presence.broker.jabber.domain="newzon"
            presence.broker.default.community.id="yourcommunity"
            presence.broker.zon.url="http://zon-server.yourcompany.com:8000/
imidio_api/"
        />
    </Presence>
```

```xml
<!--          Mirrored Folders Configuration Settings        -->
<!--                                                         -->
<!--   Mirrored folders are local/shared directories that   -->
<!--   are exposed within ICEcore.  The directories must be  -->
<!--   configured here first before they are available to    -->
<!--   the folder configuration interface within ICEcore (see -->
<!--   Modify a Folder).                                      -->
<!--                                                         -->
<!--   For security reasons the set of people who can map    -->
<!--   ICEcore folders to these shared directories is limited -->
<!--   Specify the specific ICEcore users or groups that are -->
<!--   allowed to map each folder.                           -->
<!--                                                         -->
<!--   Each mirrored folder configuration must have a unique -->
<!--   id (use a-z,0-9), and a title to be used in the user  -->
<!--   interface.  Set enabled to true to make the mirrored  -->
<!--   folder configuration active.  The examples below show -->
<!--   how to set up both file system and Sharepoint mirrors. -->
<!--                                                         -->
<!--   By default the mirrored folder is set to readonly.    -->
<!--   This means that ICEcore users can access the files, but -->
<!--   cannot modify them.  Set the readonly attribute to false -->
<!--   to allow read/write access to the folder (based on both -->
<!--   this server's access to the directory and the ICEcore -->
<!--   user's access).                                       -->
<!--                                                         -->

    <MirroredFolders>

            <MirroredFolder enabled="false" type="file"
                        id="fs1" title="Shared Files 1"
                        rootPath="k:/somedir" readonly="true">
                <AllowedUsers idList="administrator,u1,u2,u3" />
                <AllowedGroups idList="g1,g2,g3" />
            </MirroredFolder>

            <MirroredFolder enabled="false" type="file"
                        id="fs2" title="Shared Files 2"
                        rootPath="/sharedFiles/someDirectory"
readonly="true">
                <AllowedUsers idList="administrator,u1,u2,u3" />
                <AllowedGroups idList="g1,g2,g3" />
            </MirroredFolder>

            <MirroredFolder enabled="false" type="sharepoint"
                        id="sp1" title="Sharepoint 1"
                        rootPath="/Shared Documents/cool-dir"
readonly="true">
                <WebDAVContext hostUrl="http://hostname" user="accessId"
password="pass" />
                <AllowedUsers idList="administrator,u1,u2,u3" />
                <AllowedGroups idList="g1,g2,g3" />
            </MirroredFolder>
```

```
<!--                                                       -->
<!--               iChain Single Sign-On Support           -->
<!--                                                       -->
<!--                                                       -->
<!--  To use iChain SSO, set the enable attribute to true. -->
<!--  Set the Logoff URL to the address used to trigger an -->
<!--  iChain logoff.  Also set the ip address of the iChain-->
<!--  proxy server.  Only transactions from that address and-->
<!--  localhost will be allowed.                           -->
<!--                                                       -->

<SSO>
    <iChain type="1" enable="false">
        <Logoff url="http://something" />
        <Proxy  ipaddr="ipaddr" />
    </iChain>
</SSO>

<!--                                                       -->
<!--                 Custom Configuration Settings          -->
<!--                                                       -->
<!--  Custom properties set here will be placed in the     -->
<!--  ssf-ext.properties file.                             -->
<!--                                                       -->


<CustomProperties>
    <Resource
    />
</CustomProperties>

</ICEcoreConfig>
```

Glossary

Items that include an "(a)" are more relevant for ICEcore site administrators.

access control
The tool that determines who has the right to perform which tasks in which places. See also role-based access control.

accessibility mode
An optimized user interface that facilitates use by assistive devices, such as auditory readers.

accessory
A section located at the top of a workspace or folder page that provides a summary view, most likely of the information contained within the item. For example, an accessory can show all of the entries within a folder authored by someone designated as a subject-matter expert.

advanced search
Extra search tools that allow you to specify more specific criteria (such as the author of an item or restricting the search to a portion of the workspace tree).

alias
See e-mail alias.

attachment
A file attached to an entry.

author
The person who created an entry.

blog
A folder that contains a chronological listing of journal entries.

blog archive
A feature of blog folders that allows you to see entries authored in a specific month.

buddy list
A list of people whose presence you want to check and whom you contact frequently.

calendar
A folder containing entries for scheduled appointments.

clipboard
A tool that gathers people's names. Later, when using a tool that requires names, you can take them from your clipboard.

comment
A reply to an entry.

community tag

A keyword tag applied to an item by the owner of a workspace or folder. Other users of the workspace or folder can perform searches based on community tags.

configuration (a)

A set of tools that alter the way item content is presented. There are many types of configuration, ranging from setting allowable views for an item, selecting a color scheme, creating custom entries, and enabling workflow processes.

default view

The configuration of the information you see when you first view a workspace or folder. Some items may be configured to allow alternate views, which you can select.

definition (a)

A set of elements for both the form and view of a workspace, folder, or entry.

designer (a)

A tool used to create definitions or workflow processes.

discussion

A folder whose entries are discussion topics and comments about those topics.

e-mail alias

An alternative e-mail address for an e-mail account. To enable e-mail posting into a folder, you must provide an e-mail alias for the one account used to post into all folders in your ICEcore installation. Consult with your ICEcore site administrator for further assistance; site administrators, consult with the IT person responsible for creating e-mail accounts to create new aliases.

e-mail notification

An e-mail message that ICEcore sends indicating new or changed entries in a folder (and subfolders).

entry

An item in a folder.

favorites panel

A tool used to save links to workspaces and folders most important to you, providing a method of accessing these places quickly.

file folder

A folder whose entries are configured to highlight an attached file and to facilitate file management.

filter

A setting that limits a folder listing to only the entries that match the filter's search criteria. For example, you can create a filter that shows only the contents of a folder authored by you or that were created past a certain date.

folder

A container for entries and other folders. Each folder has a type, such as blog, wiki, or calendar, that determines its appearance and features.

form (a)

An HTML form used to create a workspace, folder, or entry.

global workspace

workspace that, by default, allows everyone in your organization to participate.

guestbook

A folder or accessory whose entries indicate who has visited the place.

help mode

A dimmed page and information icons ("i"). When you click on an information icon, ICEcore presents a panel of information about that section of the page.

inherit (a)

A process by which a workspace or folder automatically uses configuration settings from its parent.

instant message (IM)

A quick communication between teammates using the ICEcore Conference messaging software.

LifeRay (a)

The portal software within which ICEcore runs by default.

meeting

An online communication by teammates using the ICEcore Conference messaging software. ICEcore Conference provides tools that assist with online meetings, such as people designated as running the meeting, a way for participants to "raise their hands," and a whiteboard.

milestone

A folder that, by default, summarizes the status of tasks in a task folder as they relate to meeting project milestones.

navigator

A set of tools that you can use to go anyplace within ICEcore you want to go. The tools include "My workspace," "Favorites," viewing your teams, search, Help, and a workspace tree.

owner

The person who created the workspace, folder, or entry.

parallel workflow process (a)

A set of state transitions that happen at the same time as other state transitions. A state in the main thread initiates the parallel process, and a state later in the main thread can wait for the completion of the parallel thread.

parent (a)

A workspace or folder that contains another workspace or folder. The item contained within the parent is sometimes called its child.

participant

An access role that, generally, by default, allows people to author entries in a folder.

permalink

A web address (URL) for an ICEcore workspace, folder, or entry that you can copy, paste, and send to a teammate so that they may access a page directly by specifying the address to their web browser.

personal tag

A keyword tag that you apply to an item, and that only you can see and use.

personal workspace

A workspace that serves as a person's homepage in ICEcore, including contact information, pictures, a personal blog, and more.

photo gallery

A folder whose entries are pictures.

portal page

A web page that can run various applications in sections of its page. For example, Google and Yahoo use portal pages. Sections within a portal page may display the local time, the local weather, your favorite stock quotes, and more.

portlet

A section on a portal page. ICEcore runs within portlets.

presence

A person's online status (online, away from the computer, offline, status unknown), represented in ICEcore by people icons of certain colors.

project-management workspace

A workspace configured to facilitate the tracking of tasks and completion of complex project work.

role-based access control

A mechanism that controls access by assigning people and groups to roles, and the roles determine the rights assigned to those people. See the online Help for a list of ICEcore default role definitions.

site administrator

The person or people who have the right to perform any task anyplace in the ICEcore installation.

state

See workflow state.

subscription

A way to track new or changed items in ICEcore.

tag

A keyword that anyone can apply to a workspace, folder, or entry to make it easier to find. See also personal tag and community tag.

task

A folder that, by default, contains entries that track progress in regard to completing an assignment.

team

An access role that, by default, allows people to participate in a workspace or folder, to do some minor administrative tasks, and to communicate easily with each other.

team workspace

A workspace that restricts participation to only teammates.

template (a)

A set of default configuration settings used to create a new workspace or folder. A template includes at least one definition, access control, a possible hierarchy of defined items, and possibly more.

type to find

An ICEcore tool that uses the characters you have typed so far to present a list of possible choices. This tool is active for text boxes whose values are within a defined set: for example, people, places (workspaces and folders), and tags.

view

A presentation of an item's content. For example, you can view a discussion folder in either a list or table format. By default, most folders use one view (calendar folders use a calendar view, blog folders use a blog view, and so on).

visitor

An access role that, by default, allows people to read entries and make comments on them (but not create new entries).

WebDAV

The Web Distributed Authoring and Versioning protocol. If your system provides a tool that uses this protocol, it allows you to manage ICEcore file-folder entries using the WebDAV window.

wiki

A folder whose entries are authored by all participants.

workflow

An online representation of a business process (for example, document review, paid time-off requests, document sign off, and so on). An entry can have an associated workflow process, which places the entry into various workflow states.

workflow state

A status label for an entry in a workflow process. A state determines who has the right to work with an entry (including who may see it), who needs to be notified, who needs to perform the next task, and which subsequent states are possible.

workspace

A container for folders and other workspaces.

workspace tree

A tool that allows you to navigate the hierarchy of workspaces, subworkspaces, folders, and subfolders within ICEcore.