Community Administration

Contents

Administering the Community

Learn how to configure your community, including settings related to content and people, remote connections, and customizations.

Starting the Admin Console

You can use the Admin Console to manage system settings, permissions, content (documents, discussions, and blogs), and people. This guide describes those things that only a system administrator can do in the Admin Console.

- To view the console from the command line, make sure the application is running, then go to a URL of the following form: http://<hostname>:<portnumber>/<context>/admin. By default, using the built-in application server, this URL is: `http://localhost:8080/admin`
- To open the Admin Console from your Jive Community, click the down arrow next to your name at the top right of the screen and choose **Admin Console** from the menu.

Setting Up the Community

The first time you navigate to a page in the administration console, you'll be prompted to set up Jive using the setup tool. This tool assumes that you've either already set up a database for use with Jive, or that you're going to use the local system database. This section briefly describes the setup tool.

Note: If you've just installed, the setup tool will run the first time you access the application. If you've already completed the setup process and need to use the tool again to configure LDAP, see *Starting the Setup Tool*.

Configuring the Application with the Setup Tool

After you've installed the application, finish setting it up using the setup wizard. From the wizard, you'll enter information about your license, database connection, user identity system, email system, and system admin credentials.

After you've successfully finished with the wizard, the application is set up to run. For a brand new community, when you next log in to the end user interface, you'll have a chance to create a profile, an interface theme, and simple space hierarchy. You can also send invitations to people to join the community. For more information, see *Personalizing the Community*.

Starting the Setup Tool

If you've just installed, the setup tool will run the first time you access the application. If you've already completed the setup process and need to use the tool again to configure LDAP, do the following:

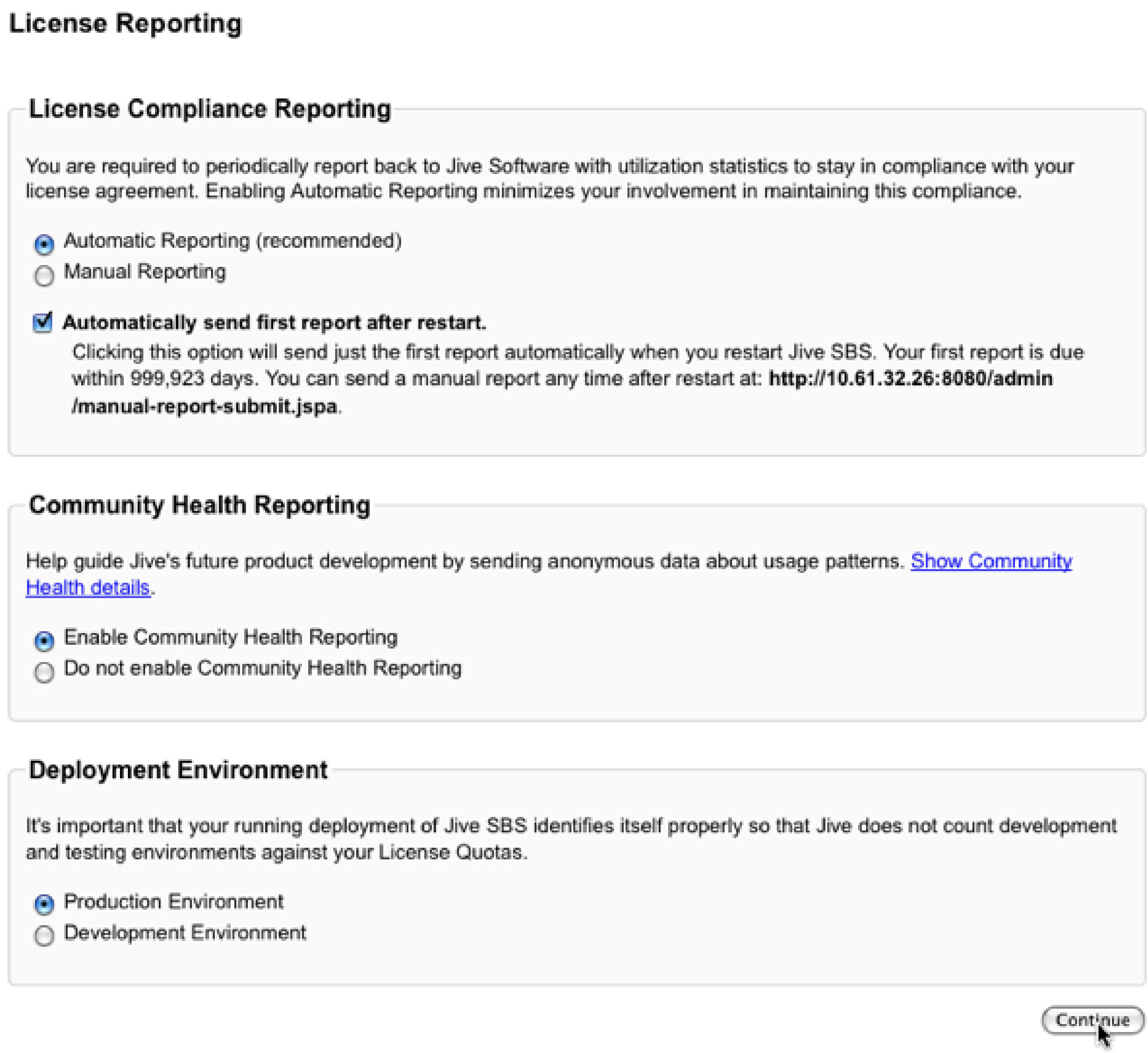
1. Stop the jive-application service from the command prompt: **/etc/init.d/service jive-application stop**
2. Edit /usr/local/jive/applications/sbs/home/jive_startup.xml so that the <setup> element has the value "false" (meaning "setup has not been run").
3. Start the jive-application service from the command prompt: **/etc/init.d/service jive-application start**
4. Point your browser at Jive using the URL above and rerun the setup tool.

License Settings

Enter the license key you purchased (you can retrieve your purchased keys by logging into www.jivesoftware.com) or click **Continue** to accept the local system license.

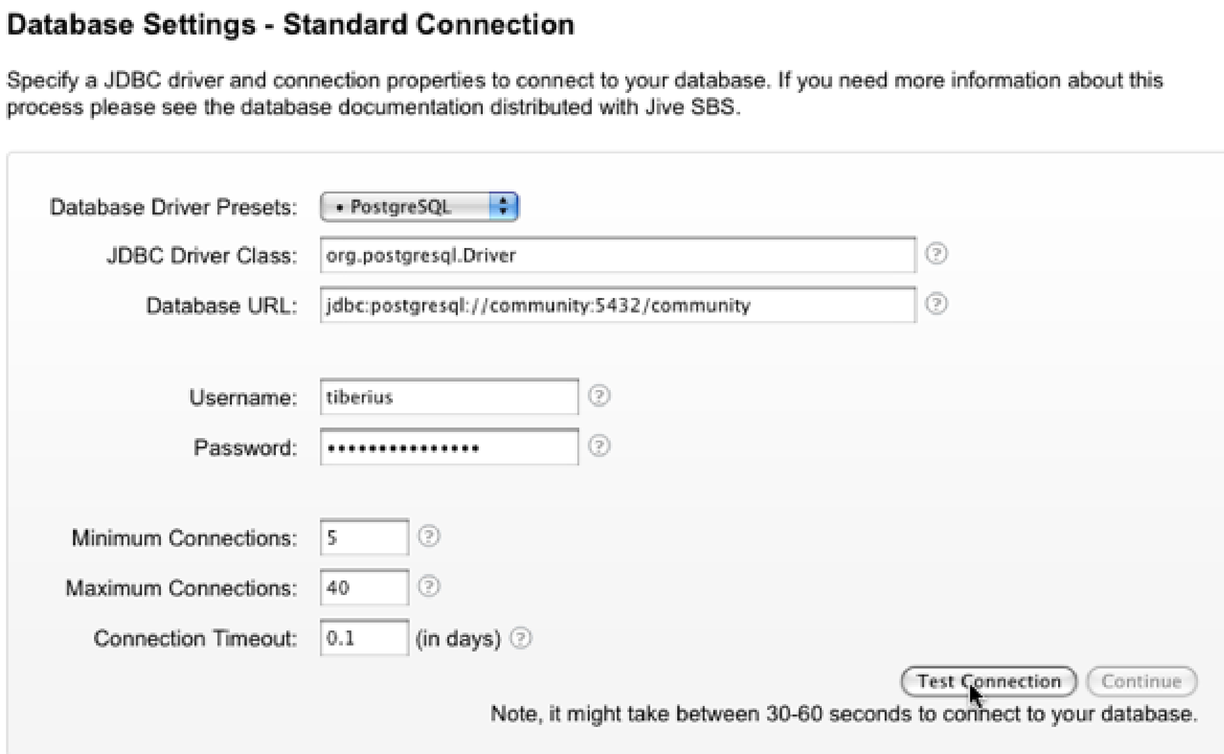
On the License Reporting page, choose whether to have your report sent automatically or to send it manually. Given that periodically sending a license report is required, having it sent automatically might save you the trouble of having to remember to send it. On this page, you also opt in or out of community health reporting, which provides feedback to the development team. Finally, specify whether this will be a production or development instance.

For more about license reporting, including what the reports include, be sure to see *Managing the Deployment License*.



Database Settings

Specify how to connect to the application database. You can use the included local system database or you can choose an external database. If you choose the standard database connection or JNDI datasource, you'll be prompted for required settings after you click Continue. Here's an example of a standard connection configuration:



User Settings

Specify the system that the application should use for user and group data.

For the Default option, the setup tool will use the user and group database tables from the application database.

- If you choose Default and then click **Continue**, you'll reach the **User Profile Name Configuration** page. There, you'll be prompted to specify whether user profiles should provide combined or separate fields for a user to enter their name. For a new installation, we recommend that you specify separate fields. If you're upgrading from an instance that used one field, you should probably stick with one field.
- On the next page, the Username Case Sensitivity Configuration page, choose whether case sensitivity should be used to look up usernames during account creation or login. For a new installation using the default user system, you should choose case-insensitive lookups. Note that with this option, username values must differ from one another in ways other than case alone.

For the Directory Server (LDAP) option, you'll be prompted to enter information for your LDAP server (such as host, base distinguished name--DN, and so on). Be sure to see *LDAP and Active Directory Guide* for details on setting up an LDAP or Active Directory connection.

Other Settings

Specify defaults for feeds (such as RSS) and email sent and received by the application. The application can send email when a account is created for a new user, for email notifications, and so on. Specify the "From" name and email address that should be used in these emails, as well as the SMTP host and port that should be used. The application can also be configured to receive email, such as when a user posts a discussion response via email. To get these emails, the application needs a client account; specify those details here.

You'll be able to change these settings later via the admin console.

Set site basics such as its URL, name, and so on.

Setting	Description
Site URL	The URL that people can enter in the browser address bar to the reach the community.
Space Name	The name that should be displayed as the name of the community, such as on the home page.

If this node is an application server node that's part of a cluster, use these settings to enable clustering for this node and to specify the address of the cache server that the cluster will use. For more information on clustering, see *Clustering Overview* and *In-Memory Caching*.

Setting	Description
Clustering Enabled/Disabled	Select **Enabled** to indicate that this node is part of a cluster of application server nodes. If you enable clustering, you'll need to specify at least one cache server address.
Cache Server Addresses	For clustered installations, enter the domain name or IP address of at least one cache server.

Enter information that will be used outgoing emails sent from the community, typically to users.

Setting	Description
Server Email Name	The name displayed in the From box in email sent from the community, such as to welcome new users.
Server Email Address	The email address for the sender in email sent from the community.

Set details for handling outgoing email. For more on mail server configuration, see *Configuring Outgoing (SMTP) Email*.

Setting	Description
Email Host	Host name of an SMTP email server that the community will use to send email.
Email Port	Port to be used for sent email.

Set details for handling incoming email. For more information, see *Configuring Support for Content Created Via Email*.

Setting	Description
Client Protocol	Select the protocol used by the incoming email server that the community will use when receiving email to post discussion replies.
Client Account Host	Host name of the incoming email server.
Client Account Port	Port of the incoming email server.
Username	Username for authenticating with the incoming email server.
Password	Password for authenticating with the incoming email server.

Admin Account

Specify the system administrator's name, email, and password. Be sure to change the admin email password from the default value, which is "admin".

Note: After you finish with the setup tool, you'll be prompted to restart the application. You can do this using the *appstop* and *appstart* commands from a command prompt as the jive user on the target computer. Here's an example:

```
[root@targethost ~]# sudo su - jive
[1016][jive@targethost:~]$ service jive-application stop
sbs stopped successfully.
[1016][jive@targethost:~]$ service jive-application start
sbs started successfully.
```

Personalizing the Community

The first time you log in to the end user UI as an administrator, you'll be prompted to get the site going. After adding a little information about yourself, setting a visual theme and basic structure for your community, you can invite others to join. All of the settings you make here are things you can change later.

When you first arrive, you'll see a "Welcome back" page. Click **Personalize your site** to get started.

Completing Your Profile

By adding profile information, you start to give the new community a face. Your completed profile can also be a great example for other people who are creating their own profiles.

- Add the photo that will be displayed on your profile page. This can be anything, but it's best to pick something that looks like you.
- Pick an avatar, which is the little image that will be displayed next to things you're associated with, such as content you create. Keep in mind that some images look better at a small size than others. For example, even at a small size, people can tell what they're a picture of.
- Add information about yourself. Keep in mind that people will be able to find yours and others profiles when they search. So it's a good idea to use words in your biography and expertise that people might search for.

Click **Continue** to see a preview of your profile. At the preview, you'll get a chance to go back and change things. If you've got something that works, click **continue to site theming**.

Setting Theme and Display Properties

Here you'll make simple changes that people will see across the site.

- Choose a background color for the bar that goes across the top of each page.
- Enter text that will appear in that top bar. This is essentially the name of your community.

Note: For more on making basic changes to the way your site looks, see *Making Simple UI Changes*.

When you're done, click **Continue** to start adding spaces to organize content.

Creating a Site Structure

Starting a structure for content is one of the most important things you'll do to get started. Most space lists tend to reflect interests or structure of the communities they serve. The spaces for a company site, for example, might be organized to reflect the organization of the company itself. A public site, on the other hand, might reflect areas of interest.

Note: The included spaces, such as Getting Started, are created automatically. In a new community, it's good to have a place for people to ask questions about the community. But you can delete these later if you want to.

It's a good idea to have thought through your space list before creating actual spaces. Once people start adding content, changing things might confuse your users or slow your site's adoption. If you've got a list of the spaces you think you'll want, pick the two that are most likely to help get things started. For example, you could create two spaces that are sure to provoke people to read and add content.

Note: For more on editing your space list, see *Creating and Arranging Spaces*, *Designing Space Hierarchies*, and *Creating a New Space*.

Click **Continue** to go on to where you can invite people to join.

Send Out Invitations

Get the right people involved by inviting them to join.

Note: For more on how to invite people later, see *Inviting New Community Members*.

Starting the Setup Tool

If you've just installed, the setup tool will run the first time you access the application. If you've already completed the setup process and need to use the setup tool again to configure LDAP, do the following:

1. Stop the jive-application service from the command prompt: /etc/init.d/jive-application stop
2. Edit /usr/local/jive/applications/sbs/home/jive_startup.xml so that the <setup> element has the value "false" (meaning "setup has not been run").
3. Start (or restart) the jive-application service from the command prompt: /etc/init.d/jive-application start (if you are restarting, use jive-application restart).
4. Point your browser at Jive using the URL above and rerun the setup tool.

Changing the jiveURL

If your Jive community is deployed on-premise (and not hosted by Jive Software), you can change the jiveURL, which is the Web address of your community. Be aware, however, that several features of the application rely on the jiveURL. To change your jiveURL, go to **Admin Console: System** > **Management** > **System Properties**, and then make sure you update the following to reflect the change:

Note: This list may not include all relevant considerations for your specific deployment configuration.

Feature:	**How to update with the new jiveURL:**
SSO	Update the base metadata URL by going to **Admin Console: People** > **Settings** > **Single Sign On** > **SAML** > **Advanced**, or by editing the system property saml.baseURL. In addition, update the Location attribute in the metadata itself. After you have made these changes, you'll need to restart the server.
Mobile	We strongly recommend that your Mobile Gateway Access URL matches the jiveURL (this is not required, however). If you change the jiveURL, update the Gateway Access URL to reflect the change (**Admin Console: Mobile** > **Connection Setup**).
Video	Changing the jiveURL causes your site to lose connection to your Video library. You'll need to *create a Support case* to update your Video library with the new URL.
SSL/Tomcat	Update the new URL in the server.xml file for the Tomact connector.
Apache	Ensure that any redirects you have configured previously are reconfigured to point to the new URL.
Twitter	You will need to reconfigure your Twitter plugin with a new Twitter app. For instructions, see *Setting Up Access to Twitter*.
LinkedIn (internal communities only)	You'll need to *create a Support case* to update your LinkedIn connector with the new URL.
Jive for Office and Outlook plugins	Ensure that the account configured in the Jive for Office/Outlook plugin contains the new URL (even if the change was due to adding SSL support).

Feature:	How to update with the new jiveURL:
Emoticons	Update the URL setting for the emoticon post-processing filter (**Admin Console: Spaces** > **Settings** > **Filters and Macros** > **Emoticon Filter** > **Settings**).

Getting Basic System Information

You can get basic, system-wide information about the deployment context for Jive from the Admin Console. It's a good idea to have this information when *contacting Jive Support*.

Fastpath: Admin Console: System > Management > System Information

- **System Info** lists fundamental information about the application system, including the application version, server, operating system, and so on.
- **Datasource Info** lists information about the database that contains application data. This includes the DBMS in use, connection information, and information about transaction support. Click **Edit Connections** to edit the number of connections that the connection provider will make.
- **Java System Properties** lists properties and values used by the Java subsystem. This ranges from commonly sought information such as the contents of the library classpath the application is running with, to the character Java is using as a path separator.

Root Space

You can change the name and description for the root space from the admin console.

Fastpath: Admin Console: System > Settings > Space

Deployment Environment

You'll find information about the environment into which Jive is deployed in the admin console. This information includes the Java environment (JVM version and Java system properties), operating system, uptime, and user, group, and authorization managers in use. It also includes information about the data source.

Fastpath: Admin Console: System > Management > System Information

Managing the Deployment License

The license you received when you purchased Jive enables the features included in your purchase, keeping your community running and available to your users. The terms of the license are based on your community's allowed usage (number of page views or users, for example), the duration of your license, and the modules your license supports.

You manage the license by regularly sending reports that summarize your community's usage level, and by updating your license with the key you receive in return. Because these reports are essential in evaluating your community's usage against the terms of your license, they're a required part of managing your license.

You can view your license type, version, capacity, current usage (how many users you're currently supporting), and license creation and expiration dates in the admin console.

Fastpath: Admin Console: System > Management > License Information

On the **Overview** tab you'll find:

- Basic license information, such as your license ID, the number of members in your server cluster, and so on.

- A means to submit your license report (such as by doing it automatically).
- A list of the application components you're licensed to use, along with details about when their licenses are due to expire, how much of your quota for each you've used, and so on. You can click a component's title to view more information about it, including its usage.
- Important messages about lapses in compliance with license terms.

Use the **Manual Reporting and Confirmation** tab to submit your license report manually. For more on license reporting, see the section below.

Resolving License-Related Issues

Licenses expiration reminders and warnings for the core application and modules occur by default as follows:

- 30-day friendly reminder - 30 days before the license expiration date, a notification is sent to the email inbox of all system administrators.
- Expiration notice - after the license has expired, Jive displays a notice for all system administrators in the admin console and the end user UI warning that the license has expired (end users will not see this notice). In addition, a notification is sent to the email inbox of all system administrators.
- Shutdown warning - 30 days after the license expiration date, Jive displays a red banner for all system administrators and root space administrators in the admin console and the end user UI warning that the site will be shut down in 15 days due to the expired license (end users will not see this notice). In addition, a notification is sent to the email inbox of all system administrators and root space administrators.

If your community is disabled (because, for example, you forgot to send the license report), contact Jive Software for a resolution.

Note: The Jive core application and any modules that you have purchased and added on have different licensing time frames. You will receive a number of notifications that the license has expired before the core application or module will be disabled. In the case of a module, only the module will be disabled, not the core application.

Your community might be partially disabled for the following reasons (after repeated attempts to warn you):

- Your subscription has expired.
- Your community's usage has exceeded what your license allows. The Jive application warns you when the usage level allowed by your license is being exceeded. In extreme cases, the community can be partially disabled by Jive Software. This disabling will cause the community to be inaccessible to all users but administrators, who will still be able to resolve the licensing issue.
- You failed to send a license report.
- Jive Software remotely locked the community.

License Reporting

Through regular reporting, you manage your license by validating your community's usage against the usage level your license allows. With each report, you receive an updated license confirmation key. As described below, you can send your reports automatically or manually.

Note: A report is required within the first 14 days of starting the application for the first time.

Data Included in a License Report

The license report includes usage information collected by the application. You can preview what's contained in the usage report by going to the Manual Reporting tab on the License Information page in the admin console.

- Number of page views (total count for all time).
- Number of users who have logged into the system at least once.
- Total number of users.
- Date and time of the report.

- The following is included for each entitlement (licensable unit of functionality), including modules, centers, features, or marketplaces.
  - Number of registered users related to the entitlement.
  - Total number of users related to the entitlement.
  - Number of page views related to the entitlement.

If you choose, your license report can include information about the health of your community. You enable this by editing the License Reporting Options and selecting the **Enable Community Health Reporting** check box.

Your community health information would include the following:

- This information is intended to provide aggregate calendar monthly values, so each measure is over the calendar month within which the activity took place.
- A count of the distinct users who have triggered an activity event (such as reading content, creating content, replying/commenting, updating their status, editing their profile, and so on).
- The content points for the month for the entire instance, which is a point sum of discussions, documents, and blog posts.
- The collaboration points for the month for the entire instance, which is a point sum of comments, tasks, and replies to threads.
- The average total number of connections per user.
- The average number of status updates per user.

Enabling Automatic Reporting

Automatic usage reporting is the easiest way to keep your community up-to-date and running smoothly. You can preview what's contained in the usage report by going to the Manual Reporting and Confirmation tab on the License Information page in the admin console and clicking **Preview Report**.

Note: You're encouraged to use this feature to avoid the trouble of remembering when to send a report. When you fail to send a report, your community may be adversely affected.

When you enable automatic reporting, the application sends a current report to Jive Software on the first day of each month. If the send is unsuccessful, you will receive an email with tips on what to do next.

To enable automatic reporting:

1. In the admin console, go to **System** > **Management** > **License Information** and enable Automatic Reporting under the License Reporting Options.

Reporting Manually

You can send your license report manually by using the admin console. You'll need to send a current report once per quarter. System administrators will be reminded via email and the admin console that a report needs to be sent.

Fastpath: Admin Console: System > Management > License Information

1. Enable Manual Reporting under the License Reporting Options.
2. Go to the Manual Reporting and Confirmation tab and click **Download License Report** to download a text version of your license report. Save that text file. (The file contains the report in a signed base 64-encoded format. To see the information that the text includes, click **Preview Report**.)
3. Upload the text file at *https://license.jivesbs.com*.
4. After Jive validates the report, copy the text of your new license confirmation key. If the report isn't validated, use the information provided to contact Jive Software.
5. In the admin console, under **License Confirmation**, paste the contents of the license confirmation key you copied, then click **Confirm**.

Moving or Copying an Instance

Caution: Several features of the application rely on the jiveURL. If you need to change the jiveURL, be sure to read *Changing the jiveURL*.

Jive's security and licensing service keeps track of your production and development environment(s) and the license(s) required for production environments. To understand how automatic and manual license reporting works, see *Managing the Deployment License*.

If you change the URL of your instance by copying your instance (changing the jdbcURL) or moving your instance (changing the jiveURL system property), the fingerprint sent to Jive's security and licensing service will differ from the one already recorded. In clustered environments, the master node communicates with Jive's security and licensing service.

Your system will try to communicate with the security service, either automatically or manually (if automatic is not available), on system startup after you've completed the move/copy wizard (which is what pops up when the system figures out you've tried to either move or copy an instance due to URL changes). If your system is unable to successfully communicate within five days, it will stop working except for the Admin Console. Note that you will be warned if automatic license verification with the security service is not an option.

Using the same license, you can:

- Move a production instance to a different server (using a different URL)
- Copy or move a test/development environment

Note: You **cannot** copy a production instance and declare the new instance as a production instance with the same license!

Locale & Time Zone Settings

You can set default locale, time zone, and character set for the site.

Locale represents a set of user interface properties -- including language and time zone, for example -- that are often related to the user's geographic region. The locale setting determines what language UI default text is displayed in. It also determines how dates are formatted, what the character encoding is, and so on. The correct locale helps to make people's experience in the community feel more familiar and comfortable. For sites that want to support a broad variety of languages, Jive requires using "UTF-8" (Unicode) as your character encoding. For more about this, see *Localizing the Application*.

Here you can set the server time zone, which dictates the time zone Jive uses for the midnight start time and 11:59 end time for announcements, polls, projects, tasks, and checkpoints. Blog posts obtain their settings from the user's time zone.

Fastpath: Admin Console: System > Management > Locale

Note: Only a subset of the languages listed are actually available in the application by default. For a list of languages in the subset, visit your user preferences page and view the Languages list on the Preferences page.

Locale Inheritance Rules

As a community administrator, be aware that when you modify locale settings for the application (global) or a space, the user may have also set their own locale preferences, which will take precedence. Here is the locale precedence hierarchy, with the first given the highest precedence:

1. Locale set by the user in their Preferences. For more information, see *Time Zone and Locale Preferences*.
2. Locale set in the user's Web browser. (For example, a browser set to English will override global settings you make for another locale).
3. Locale set at the space level (in **Admin Console: Spaces** > **Settings** > **Space Settings**). See *Setting Space Name, Locale, and Allowed Content Types*.

4. Locale set at the root space (global) level (**Admin Console: System** > **Management** > **Locale**).

Configuring Content-Related Settings

Look in this section for information on making settings related to how the application handles content, including setting size limits and threading for discussions, plus enabling search, spell checking, and more.

Configuring Document Options

In addition to creating new text documents in the content editor (with word processor-style formatting), users can upload documents as files of other types, including PDF files, Word documents, spreadsheets, and other file types. As the administrator, you can configure how uploaded documents are handled using the Admin Console.

Fastpath: Admin Console: System > Settings > Documents

Note: For space-specific document settings, be sure to see *Setting a Space Approver*.

General Settings

Uploaded documents can add up in size. If this becomes an issue, you can limit the size of uploaded files or disable file uploads altogether.

Note: You have the option of storing binary content in storage outside the application database. For more information, see *Configuring a Binary Storage Provider*.

Content Types

If you enable uploaded documents, you can disallow content types that you don't want people to upload. You can also add MIME types that aren't in the current list.

Configuring Discussions Application-Wide

Application-wide discussion settings control useful but performance-intensive features such as read tracking and thread mode. You can also set some aspects of how threads marked as questions should be handled.

Fastpath: Admin Console: System > Settings > Discussions

Note: For space-specific discussion settings, be sure to see *Configuring Discussions for a Space*. Those settings relate to handling for posts marked as questions.

Discussion Feature Settings

Enable **Read Tracking** to have messages marked as read by the person who has viewed them. You might also want to have them marked as read automatically if you have a lot of traffic and want to ensure that more recent messages get attention from readers.

For **Thread Mode**, select either Flat or Threaded. *Flat* views display replies chronologically in the order they were received, and there is no indentation between responses. In a *threaded* view, users can see which reply a person is responding to because replies appear indented beneath the post to indicate embedded replies. This can help users follow conversations because responses remain associated together visually. This is a global setting for all users, but note that individual users can change their Discussion View Style under their General Preferences and that their preference overrides your global setting.

When replies reach the maximum set in the system property thread.allMessageActions.messageLimit (the default is 100), replies will appear flat even if you or the user has set them to appear as threaded.

Note: If you're seeing slower performance, try disabling read tracking and turning the thread mode default to **flat**. Both of these features can tax performance on some configurations.

Expert Settings

When a discussion thread is marked as a question, the following kinds of users can mark replies as **Helpful** or **Correct** answers:

- Community administrators
- Space, group, or project owners where the question was posted
- The user who posted the question

In addition, all of these users except the user who posted the question can mark the entire thread as **Assumed Answered** if the question was answered through the course of the discussion. These signals make it easier for people reading the thread to see which responses were on track. This could save them time if they've got the same question.

As an administrator, you can specify how many **Helpful Answers** are allowed in a single thread. You might want to keep this number small if you feel that a large number of helpful responses might dilute the meaning of "helpful." Also, keep in mind that Jive is designed to award status points for helpful answers; you can increase the value of these points by keeping the number small. On the other hand, increasing the number could encourage people to respond more frequently if they think it's more likely their response will get marked as helpful.

Depending on what's best for your community, you might find it useful to have every new discussion thread start out **Marked as a question** by default (the person creating it can un-mark it if they want to). You might want them to be questions if your space is a place where people go for answers, such as a support-related space. Contrast this with a space where people go to make suggestions or merely share information.

After a discussion is published, by default there is a 15-minute grace period during which the author can change the discussion into a question. As an administrator, you can change the length of the grace period by editing the value (in minutes) of questions.markAsQuestionTimeWindow under **System > System Properties**. You may need to add the property at the bottom of the page if it is not in the list. Community administrators and space/group/project owners can mark a discussion as a question at any time (but they cannot un-mark it as a question, only the author can).

For settings that control how people should be notified when a question has been unanswered for a while, see *Configuring Discussions for a Space*.

Managing Blogs

Generally speaking, blogs are managed by their authors. They can also be managed by the owners of the place (space, project, or social group) where the blog lives. For some blogs, including global blogs such as system and personal blogs, you can use the admin console to perform such tasks as creating blogs and managing its comments.

Contexts for Blogs

A blog can live in one of several different contexts. By default, these contexts include the global context and each of the places that can contain a blog. This is important because a blog's context determines how you manage permissions for the blog, how you configure its settings, and so on.

For example, the following list captures four areas where blogs can be configured or managed.

- Creating -- This includes whether and how people create a new blog and set which people can post to it.
- Permissions -- This can include permission to create blogs and post to a blog, but varies from context to context.
- Management -- Once a blog is created, its owner will have access to a management page specific to the blog. There, they can review posts and comments. They can also configure moderation and feed preferences for the blog.
- System-wide settings -- These settings impact all blogs, regardless of context. They include enabling/disabling blogs and comments. For more information, see *Configuring Blogs System-Wide*.

The table below describes how each of the areas is exposed based on the blog's context.

Blog Type	Scope	Creating	Permissions	Management	System-Wide Settings
System blog	Global; not contained in any space. A system blog is not connected with any particular space or person.	Administrators can create blogs and assign people as authors so they can post to it.	Administrators can set specific permissions, such as for creating and viewing system blogs. For more information, see *Managing Blog Permissions*.	Blog authors and administrators can manage the blog.	Settings are shared by all blogs.
Personal blog	Global; not contained in any space. A personal blog is associated with a particular user, who is its owner. A user can have only one personal blog.	Administrators can create a personal blog in the admin console. A person who has been assigned permission to do so can also create their blog in the end user UI. Only the blog's owner can post to it.	Administrators can set specific permissions, such as for creating and viewing personal blogs. For more information, see *Managing Blog Permissions*.	A blog's author can manage the blog.	Settings are shared by all blogs.
Space blog	Associated with a particular space. A space can have only one blog.	A person with permission to administer a space can create a blog there. The blog's author list is determined by space permissions. For more information, see *Managing Space Permissions*.	Administrators can set fine-grained access for a space's blog. For more information, see *Managing Space Permissions*.	Blog authors and space administrators can manage the blog.	Settings are shared by all blogs.
Project blog	Associated with a particular project (which is contained by another place).	Settings are inherited from the space that contains the project.	Settings are inherited from the space that contains the project.	Settings are inherited from the space that contains the project.	Settings are shared by all blogs.
Social group blog	Associated with a social group.	A person with permission to administer a social group can create a blog there. Every member of the social group has full access to the blog's features except blog management.	Permissions are not editable. They provide full access to the blog for every member of the group.	Group administrators can manage the blog.	Settings are shared by all blogs.

Configuring Blogs System-Wide

You can make changes to blog configuration that impact blogs everywhere in the community. These system-wide settings are common to other blogging software.

Fastpath: Admin Console: Blogs > Settings > Blog Settings

Be sure to see *Managing Blogs* for an overview of blog configuration.

Setting	Description
Blogs	Enable or disable blogs. Disabling blogs will remove blog-related elements in the user interface. People will no longer be able to create or view blogs and their posts.
Comments	Enable or disable blog post comments. Disabling comments will cause comments not to be visible in the end user UI. It will also remove the ability to add comments to blogs.
Ping Updates	Enable or disable *ping* updates.
Ping Service URI Override	Enable or disable ability for users to customize the list of ping service URIs. When this is enabled, the blog management page for a blog provides a way for a blog's author or administrator to specify ping service URIs.
Default Ping Service URIs	The default list of ping service URIs. These are the URIs that will be pinged by default. If you enable URI override, the a blog's management page will still provide the option to use the defaults.
Akismet	Enable or disable *Akismet* service for filtering spam in comments. Enabling Akismet displays a place where you can enter your Akismet API key.

Migrating Blog Content

As an administrator, you can migrate an existing blog from one context to another. For example, you can migrate a space blog so that it becomes a group blog. There aren't any restrictions; you can migrate from any context to any other context. When you migrate, all of the blog's posts and settings will move to the destination context.

Note: Keep in mind that migrating a blog to another context can change how the blog will be managed and administered after it's migrated. For more information, see *Managing Blogs*.

Fastpath: Admin Console: Blogs > **Management** > **Migrate**

To migrate a blog:

1. On the admin console **Blog Management Migration** page, select the blog you want to migrate.
2. Under **Destination**, select a destination:
   - To migrate the blog to become a system blog at the global level, select the **System Blog** check box.
   - To migrate the blog into a space, under **Communities Without Blogs** select the space you want the blog to be in. The list is limited to spaces that don't have blogs because a space can only have one blog.
   - To migrate the blog into a project, under **Projects Without Blogs** select the project you want to migrate to. A project can contain only one blog.
   - To migrate the blog to become a user blog at the global level, under **Users Without Blogs** enter the username for the person whose blog it should become (you can also browse for the username). A person can have only one user blog.
3. Click **Submit**.

Enabling or Disabling Projects

You can disable the projects feature if your community won't be using them. Disabling the project feature essentially means hiding project-related user interface elements. For example, Projects won't appear on the Create > Places menu or the Browse > Places page. If there are already projects in the community when you disable the feature, those projects will become inaccessible -- essentially invisible. Project data, however, won't be deleted.

Note that if you *do* want to delete projects, you'll need to do it while they're still visible -- *before* you disable the feature.

Note: If you enable or disable projects, you'll need to restart the application for your changes to take effect.

Fastpath: Admin Console: System > Settings > Projects

Configuring Direct Messages

Direct messages allow users to send messages that are visible only to the receiver(s); direct messages do not appear in the Activity stream. Direct message notifications appear in the Communications stream of the receiver(s). You can enable direct messages for users from the admin console. By default, direct messages are enabled for external Jive communities, and disabled for internal communities.

Fastpath: Admin Console: System > Settings > Direct Messages and Sharing

As of Jive 5.0.1, you can require that users must be connected to send direct messages or shares to each other. In external communities, this helps to prevent spammers from spamming community users and is enabled by default in external communities (and disabled by default in internal communities). If you need certain users to be able to override this setting, for example, your HR Director to be able to send direct messages or shares with users they aren't connected to, go to **Permissions** > **Home Page Permissions** and set up a user override with "DM/Sharing admin" permission.

Configuring Sharing

The sharing feature allows users to alert others about interesting content items. Shared content notifications are private and appear only in the Communications stream of the receiver(s).

Fastpath: Admin Console: System > Settings > Direct Messages and Sharing

As of Jive 5.0.1, you can require that users must be connected to send direct messages or shares to each other. In external communities, this helps to prevent spammers from spamming community users and is enabled by default in external communities (and disabled by default in internal communities). If you need certain users to be able to override this setting, for example, your HR Director to be able to send direct messages or shares with users they aren't connected to, set up a user override; go to **Permissions** > **Home Page Permissions**, select user override and assign the user "DM/Sharing admin" permission.

Configuring Support for Images and Attachments

Jive users can insert images and attach files to documents, blog posts, and discussion messages. Using the admin console, you can configure support for images and attachments.

Fastpath: Admin Console: System > Settings > Attachments

Fastpath: Admin Console: System > Settings > Images

The Difference Between Attaching and Inserting

Users can *attach* a file to most content types. Attached files show up as links at the bottom of published content so that others may click to view the attachment. Attachments can be documents, images, videos, etc. When a user attaches an image, a preview of the image shows with its link. Users can also *insert* images by clicking the camera button in the editing pane. Inserted images are displayed in the content itself. So, *attached* files and images show up as links at the bottom of the content; *inserted* images are rendered directly in the content.

General Settings

Quantity and size. If you find that users are attaching many large files and the application is slower as a result, consider creating limits by adjusting the size and quantity settings.

Unless otherwise specified, image sizes are specified in pixels and attachment sizes are specified in kilobytes (preview in pixels).

Note that some of the settings are interrelated. For example, if you want users to be able to attach more images to a document than they are currently allowed to, you'll need to make two changes: increase the **Maximum number of images per object** on the **Images** page and increase the **Max number of attachments per document** on the **Attachments** page.

Thumbnails and previews. An image embedded in content can display as a thumbnail if it's too big (based on height and width you specify). Images that are merely attached to content can display a preview, which makes it easier for people to see whether it's the image they want before clicking its attachment link. The maximum preview or thumbnail dimensions refer to the height or width of the item; a value of 250 means a thumbnail will not exceed 250 pixels in height or width.

Content Type Settings

Content type settings let you specify which kinds of content (as determined by their MIME type) should be allowed as embedded images or attached files. You might find that some content file types aren't needed (or are in fact unwanted). You can prevent some kinds of files from being uploaded by "disallowing" them (specifying their MIME content type). If you change these settings, be sure to change it on both the Image and Attachments pages.

Configuring Spell Check

As an administrator, you can customize the spell check feature in the admin console. The spell checker uses the main dictionary you specify for all content in the community so that Jive will check spelling as users create and edit content. Consider using the technical dictionary if your community creates content with terms from the computer industry.

You can also add words to your custom dictionary; that way, words commonly used where you are (such as jargon or product names) won't be marked as misspelled.

Fastpath: Admin Console: System > Settings > Spell Check

Configuring Ratings and Liking

You can configure ratings and liking for different types of content, such as blog posts, discussions, documents, polls, and more. Ratings and likings are a great way for users to get feedback on content and earn status points. When a user rates or likes content, the community sees that action listed in the Community Activity and Recent Activity widgets if you have them enabled (**Admin Console: System** > **Settings** > **Widgets**). For example, the community might see *Joey Ramone rated The Rose City Quarterly Document* or *Joey Ramone liked The Rose City Quarterly Document*. For more information about widgets, see *Designing Pages with Widgets*.

Fastpath: Admin Console: System > Settings > Ratings and Liking

To configure ratings and liking, select the content types you want to enable and then click **Save Changes**.

Setting	Description
Allow Comments with Ratings	Select **Yes** if you want users to have the option to add a comment after they rate content.

Setting	Description
Show Likes in Recent Activity	Select **Yes** if you want to see a post in recent activity every time a user likes content.

Configuring Search

Jive provides search access to content it contains (including information about people) as well as access to external search engines that support OpenSearch. You can use the admin console to configure and optimize these for use across your community.

Configuring Main Search

Support for searching internal content and user profiles is provided by the *Lucene* open source search engine. Lucene works by periodically creating or updating an index of content, then searching against the index. Using the admin console, you can configure the search feature, including how often these indexes are updated, how the feature treats user queries and search results, and so on.

In addition to content written and published with the community's editor, the search feature also searches the following file types: .html, .rtf, .txt, .pdf, .ppt, .pptx, .doc, .docx, .xls, .xlsx, .odt, .ods and .odp (OpenOffice formats). The application will also search the contents of a .zip file.

Fastpath: Admin Console: System > Settings > Search

Note: Jive includes *Search Tips* documentation that people can use to make the most of their searches. You can reach the tips from a search page.

Search Status and User Search Status

The indexes for content and for user information are separate from each other. That means that you can enable searching for content and user information separately (you can turn user searching off, for example). It also means that you can update the indexes separately at need, which can be more practical than updating everything at once when you need to.

Click the Update button to save a status setting.

Search Settings

Most of the settings you make on the Search Settings tab are designed to adjust how people experience search, although some settings impact performance.

Setting	Description
Automatically index new content	Set to "Yes" to have content added to the search index as soon as it's published, rather than waiting for the next index update time.
Index update time	How often the index is updated.
Search attachments	Set to "Yes" to broaden searches to include not only content entered through the editor, but also attachments such as PDF and other files.
Default search query date range	The default date range for searches. People can set this to another value when they search.
Default Indexer Type	The search engine uses an indexer to break down content into constituent pieces while indexing, making searches more efficient and faster. This setting specifies the default indexer to use.
Default search operator	A default setting used when the person doing the search doesn't specify a query string that contains its own operators (see *Search Tips* for on queries). For example, with a default operator of AND, a query string given as `black`

Setting	Description
	`cat` will be passed to the search engine as `black AND cat` -- translating into a search for content with *both* "black" and "cat" in it.
Allow wildcards in search queries	Wildcards enable more powerful searches. For more on how they're used in searches, see *Search Tips*.
Group search results by thread	Discussions can include a single post and many reply messages. Set this to "Yes" to group in the results list all of the results found in a single thread (both original message and replies).
Spell check search query strings	Set this to "Yes" to have the UI display a message when search results might have been misspelled. The message will appear with a "Did you mean...?" link that searches for a suggested alternative.
Show user email addresses	Set this to "Yes" to have the content author's email address appear with their content in the results list.
Enable auto index optimization	Optimizing the index can make searches faster.

Index Tasks

Having the application regularly update the search indexes is very handy; rebuilding an index (via the Index Tasks tab) can be very time-consuming. You should only manually rebuild if you really have to; reasons for doing so are listed in the admin console.

Note: If your instance is installed in a cluster environment, there are *special instructions for manually rebuilding the search index*.

Stop Words and Synonyms

You can improve searches for people using your community by tailoring the stop words and synonym lists to best suit your needs. For example, if you realize that people will search using slang common to your industry, you could add synonyms that associate a commonly used term with slang alternatives. A software industry example could be "programmer,developer". To add synonyms, enter a pair of words separated by a comma in the Synonyms box, then click Add Synonym.

Try to settle on your list of stop words early, before you've got a lot of content. When you change the list, you need to rebuild the search index; that can take quite a while when you've got a lot of content in the database.

Note: You can set whether blog and document comments should be found when searching by setting system properties. Use the following system properties (in the admin console at System > Management > System Properties):

Property	Description	Values
blog.searchComments.enabled	Toggles whether or not comments to blog posts are returned in search results.	true (default) to enable return of comments on search; false to disable it.
document.searchComments.enabled	Toggles whether or not comments to documents are returned in search results.	true (default) to enable return of comments on search; false to disable it.

Multiple Language Search

You can enable multi-language search by specifying a separate Lucene analyzer for each language supported on your Jive instance. A language for each piece of content will then be chosen based upon the locale setting for that content's container. The analyzer specified for a language is used for indexing the content. Users can specify the language to be used when they perform a search, which causes the search to be executed using the analyzer configured for that language.

When you enable multi-language search, and a user performs a search using a particular language, only content that has been indexed in that language will be included in the results. For example, if only one space uses the Spanish locale, and there is only a single document in that space, the document will only show up in a search where the Spanish language is selected as the search language in their user Preferences.

1. To enable multi-language search, set the i18n.allowedLanguages system property to specify more than one language (**Admin Console: System** > **Management** > **System Properties**):

Property	Description	Values
i18n.allowedLanguages	Lists the languages allowed to be used when searching.	Accepts a comma separated list of language code values (such as "en" or "de"). The comma separated list must not contain spaces.

2. Restart the application.
3. Enable multiple language search by going to **Admin Console: System** > **Settings** > **Search** > **Search Settings** and selecting **Enable multiple language search**.

   Note: The Stop Word section becomes language-specific when you enable multiple language search, so make sure you go to the Stop Words tab and add stop words for the additional languages if desired.

4. Go to **Spaces** > **Settings** > **Space Settings** and select the locale for any space whose content should be indexed in a language other than the system default language or its parent space language.
5. Rebuild the search index by navigating to **System** > **Settings** > **Search** > **Index Tasks**> and clicking **Rebuild index**.

Configuring OpenSearch

You can make some external search engines available to people using Jive. If a search engine supports OpenSearch, you can add support for it so that the search engine will be used (in addition to the internal search engine) when people search for content in Jive. Examples of OpenSearch engines include *Technorati* and *Wikipedia*, plus Jive communities.

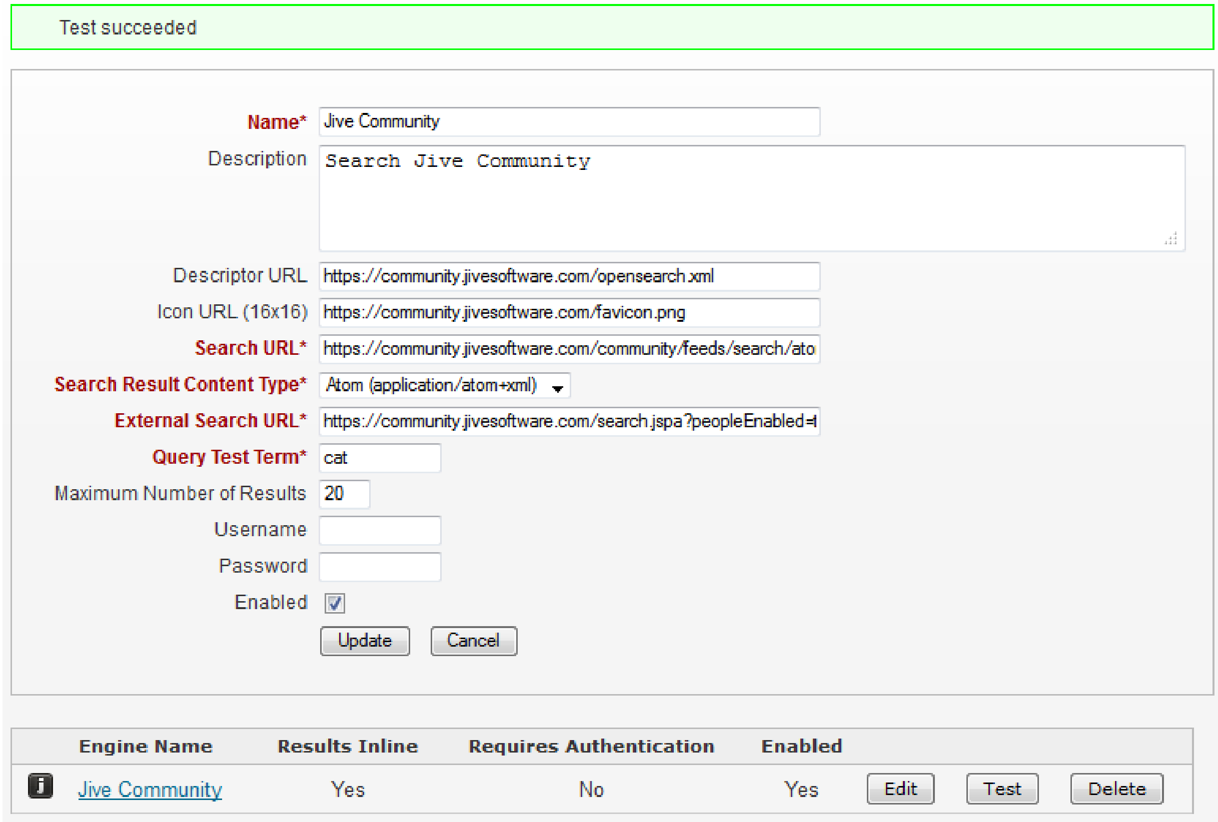
Engines that support OpenSearch provide a descriptor XML file and usually publish the file at a public URL. The descriptor tells OpenSearch clients what they need to know to query the search engine.

Fastpath: Admin Console: System > Settings > OpenSearch Engines

There are two ways you can add OpenSearch engines in the admin console:

- Enter a descriptor URL, then click **Add Engine from Descriptor URL**. The application will visit the URL to retrieve the descriptor XML file, then retrieve the needed information from the file.

  If the application gets the information it needs, you're finished. However, you might get prompted for more information, such as login credentials if the engine is secure. Note that you can edit engine properties later.
- Click **Add Engine from Form**, then fill out the form to include the required information. The information asked for here is what would be included in the descriptor XML file. This is the same information you can edit for an engine, as described below.



As you edit the engine's properties, keep in mind the following:

- The icon URL is a URL to an icon representing the search engine. Jive will display this in its UI.
- The application uses the search URL to send the user's query.
- The search result content type is the content type, such as application/rss+xml or text/html, that the search engine's results will be returned in. If this is a type that the application can parse, such as application/rss+xml, the results will be displayed in the UI; if not, the application will display a link through which the user can separately search the engine's site itself.

  If you specify HTML as the content type, the end user UI will display a link in a sidebar that people can use to search for their phrase at the OpenSearch location. If they do, their results will appear in a new window.

  If you specify RSS or Atom as the content type, the application will display a new tab with the Name value. The application will parse returned results into a format that displays on the search results page, under the new tab.
- The query test term can be anything you like to test queries.
- You might need to enter a username and password if the search engine requires login credentials.
- The Enabled check box is selected by default, meaning that user searches will query the engine. Uncheck the box to make the search engine unavailable to users.

Note: The Jive application is also an OpenSearch provider (although OpenSearch isn't a good replacement for searching content it contains). You just have to point your OpenSearch reader to Jive's OpenSearch XML descriptor. For OpenSearch readers that aren't able to autodetect the descriptor, you'll have to add it manually. The OpenSearch descriptor for your community is located at `http://<jiveURL>/opensearch.xml`. For example, for the Jivespace descriptor, go to http://jivesoftware.com/community/opensearch.xml. Provide this file as the descriptor for your OpenSearch reader.

Reindexing Browse Data

Fastpath: Admin Console: System > Settings > Browse

If you have a specific problem with your browse content synchronization and you need to reindex the browse data in your database, you can use the Browse Settings page to initiate reindexing. The Browse Settings page shows progress for all reindexing tasks in the cluster.

Managing Feeds

Users can choose to receive feeds (RSS, JSON, or Atom) to stay current on content changes they care about. As an administrator, you can configure aspects of these feeds, such as which feed technology is used, whether basic authentication is required, and so on.

Fastpath: Admin Console: System > Settings > Feeds

Table 1: Permissions Management for Non-Global Blogs

Setting	Description
Enable Feeds	Enables feeds across the community.
Author Format	Specifies how the author will be displayed in the feed.
Basic Authentication	Turns on the requirement that feed requests specify a username and password.
Default Format	Default format for feeds generated by the community.
Number of Items	The number of items returned for each feed.
Show	Specifies whether the feed results should include the full text of the content or only a summary of it.
Length of Summary	Specifies how much of the content (how many characters) should be included in the feed result summary.

For more on feeds, be sure to see *Working with Feeds*.

Filtering and Formatting Content

You can use filters and macros to make text changes to text at run time. Use the Admin Console to turn these changes on or off, or to change the settings that control how they work.

Each component type has a different role. Here's how they work in general:

- A **filter** operates on all of the text in content. So a filter is a good way to perform tasks such as changing every link URL, looking for particular text throughout a piece of content, and so on.
- A **macro** is designed to operate on a particular part of the content, such as a particular section of text. For example, a macro formats a link to a blog post with the CSS style reference needed to display the blog icon.

  Note: We no longer refer to these operations as "macros" in the user interface. Many of the macros now simply appear as selections on the content editor toolbar, for example, a button for setting text color or formatting code. Even so, the Admin Console and developer documentation continue to refer to them as macros.

Configuring Filters and Macros

The Filters and Macros page lists the filters and macros installed for the selected space. By default, each space inherits the set of filters and macros from the global configuration defined in the root space. However, the list isn't shown for sub-spaces until you choose to copy them. When you click the Copy Global Filters button on the Filters and Macros page for a subspace, the application copies the list and configuration to the page. If you want to edit the list for a sub-space, you'll need to click the button first.

Fastpath: Admin Console: Spaces > Settings > Filters and Macros

Pre-Processing Filters

Pre-processing filters are the very first filters to operate on your content. They are performed on the initial version of the content before all other macros and filters have done their work to generate content. For example, the HTML filter should be executed before any other macros or filters because otherwise it would strip out the HTML content that the other macros and filters introduce.

By default, there are no editable pre-processing filters.

Macros

A macro operates on, or adds, a specific part of content. For example, a macro could format a link or embed a window to display video.

In the list, you'll see all of the macros installed on the system. Many of these, including macros whose functionality is tightly integrated into the content editor toolbar, are not available to be disabled. Those you can disable or delete are generally macros installed as separate components, such as in plugins.

Filters

Filters -- you can think of them as mid-processing filters -- operate on text after macros have executed, but before post-processing filters have done their work. By default, the application doesn't include any editable filters.

Post Processing Filters

Post-processing filters provide a final sweep of content before it's seen by other people. This is where you catch whatever is in the text, including whatever might have been added by other filters or macros. One of the most important filters you can enable is the *profanity filter*.

Profanity Filter

The profanity filter automatically detects words in your profanity list and replaces them with ***. The profanity filter is the most commonly used filter; please consider using it. You use the filter by adding the words you want filtered out, and then turning on the filter. For more on filters, see *Configuring Filters and Macros*

Note: The Profanity filter only works with languages that have natural word boundaries. For example, this filter does **not** work with Japanese and Chinese.

On the Filters and Macros page, scroll to the Profanity filter and click **Settings**. In the Settings page, enter the list of words you want filtered out of your content. Enter words and phrases separated by commas. If you have more than a few entries, enter the longer or broader phrases before the smaller and more specific ones because they are evaluated in the order you enter them. For example, imagine that your list includes both "gleeking boil-brained nit" and just "nit". Your entries will be evaluated in the order you enter them. So if you've got "nit" before "gleeking boil-brained nit", then content that includes "That's rubbish, you gleeking boil-brained nit" will be filtered to "That's rubbish, you gleeking boil-brained ***" -- in other words, you won't have filtered out the whole phrase.

Be sure to select check boxes for the parts of the content you want filtered, then click **Save Properties**. Back on the Filters and Macros page, click the profanity filter's **On** button to turn it on.

Configuring Interceptors

Interceptors perform actions on incoming requests that seek to post content. You can configure interceptors on the Interceptors page of the Admin Console.

Fastpath: Admin Console: Spaces > Settings > Interceptors (change space)

Some of the interceptors have functionality related to features exposed for configuration elsewhere in the Admin Console. For example, the Ban User interceptor is designed to prevent the specified users from posting content. In contrast, the ban settings you can make elsewhere (see *Banning People* for more information) are designed to ban users from logging in at all.

Note: Filters and interceptors can be applied to discussions, document comments, and blog comments. You can't apply interceptors to the body text of documents, and to a blog post only when it's first created. In other words, keep in mind that people authoring documents and blog posts can create content that's less "filtered."

When you don't want any part of a post or comment with an offending word to enter the space before an action is taken, use an interceptor instead of a filter.

For more about filters, see *Filtering and Formatting Content*.

Installing Interceptors

Interceptors are included, but not installed/active by default. To set up an interceptor:

1. Verify that you have selected the correct space to enable interceptors. If you need to change the space, click **change space** at the top of the page.
2. From the interceptor list, select the type of interceptor that you want to install (Message Governor, Keyword, and so on).
3. Click the **Install** button.
4. After you've installed the interceptor, it will appear in a list of current interceptors. In that list, click the **Edit** button next to the interceptor to edit its properties.
5. Use the list of interceptor properties below to refine how the interceptor will work.
6. For the search queries, make sure to use the search conventions described in *Search Tips*. Note that you cannot enter a comma-separated list of words in the search query string boxes.

Some things to keep in mind when you are setting up interceptors:

- Interceptors are executed in the order they appear in the list of interceptors. So, if you install more than one, use the move arrows to make sure the interceptors are listed in an order that makes sense. For example, do not add a message to a moderation queue by a person whose IP is banned from posting.
- You can install an interceptor multiple times, setting it up differently each time.
- For the query strings, use the search conventions described in *Search Tips*. Note that you cannot enter a comma-separated list of words in the search query string boxes.

The following is a list of included interceptors, along with more about their properties:

- Ban User

  In the Ban List box, enter a comma-separated list of application usernames for people you want to ban from posting. You can also select to have email sent to these users when they try to post. You can edit the "User Interceptor" message template for the email (see *Managing Email Templates* for more).
- IP Address

  This interceptor provides ways to keep an eye on content coming in from certain people (or to simply ban them) based on their IP addresses. In the Banned IP List, enter a comma-separated listed of the IP addresses you want to ban from posting. Use the Email Notification boxes to send email to people you specify (such as administrators in your community) when posts come from certain IP addresses (see *Managing Email Templates* for more on the "IP Interceptor" template). In the Moderation IP List, enter the addresses of content sources whose posts should automatically be added to the moderation queue. (For more about moderation, see *Moderating Content*)
- Gateway Privacy Manager

  This interceptor gives you slightly finer control over how gateway-imported messages are handled (for more on gateways, see *Synchronizing Content with Email or Newsgroups*). You can hide the name or email address of the poster in the incoming message. If you do, you can store the hidden values in extended properties to you can take a look at them later. (For more on extended properties, see *Fine-Tuning with Extended Properties*.)

- Moderation Controller

  Use this interceptor for finer control over which users' content is moderated. The interceptor uses the user and group lists that are viewable on the People pages of the Admin Console (for more information, see *Managing User and Groups*.) Enter comma-separated lists of usernames or groups to specify who should always or never be moderated.
- Message Governor

  Use this interceptor to control how quickly a single user can post messages. For example, you might want to limit frequency if you're having trouble with auto-posting of spam messages. The message template is provided for you in the interceptor properties.
- Keyword

  Use a keyword interceptor to search strings for keywords in incoming posts. You can choose to have incoming posts:

  Caution: Make sure that you are enabling this feature in the correct place. If you need to change the space, click **change space** at the top of the page.

  - **Reviewed by a moderator** -- Enter your keyword(s) in the Moderation Query String box using the search conventions described in *Search Tips*. Whenever this word(s) is found in a post, it will be sent to the moderator for approval (or rejection) before it is published in the community. Finally, click **Save Properties** to save your changes.
  - **Blocked from being published** -- Enter your keyword(s) in the Blocked Content Query String box using the search conventions described in *Search Tips*. Whenever this word(s) is found in a post, it will be blocked and not published in the community. In the Blocked Content Error Message box, you can create a message for the user to see when a post is blocked, for example, "We're sorry, but this post contains potentially inappropriate content and has been blocked from being posted in the community." Finally, click **Save Properties** to save your changes.
  - **Alerted via email to specific users after the posts are published** -- Enter your keyword(s) in the Email Query String box using the search conventions described in *Search Tips*. In the Email Notification List box, add the email address(es) of the user(s) you want notified via email whenever this query returns something. Finally, click **Save Properties** to save your changes.

Synchronizing Content with Email or Newsgroups

You can create gateways through which Jive will synchronize data between a space and an email, newsgroup, or *mbox* data source.

Fastpath: Admin Console: Spaces > Settings > Gateway Settings

When you create a gateway, you specify the data source to synchronize with, along with the space to synchronize. In other words, each gateway is a one-to-one mapping between a space and the data source. You can either create a gateway that's automatically used for synchronizing or you can synchronize data in either direction at need. Gateway settings are scoped to specific spaces.

You can also choose to use a 24-hour buffer for importing. That means that, at the time of import, the gateway pulls in all data that has come in since the last import, plus those that came in within the 24-hour period before the last import. For example, if an email has already been imported, it won't be imported again, but any emails that came in late and were missed the last time the gateway ran will be imported. This redundancy helps ensure that you get those emails that were held up at the server for some reason and did not get delivered in a timely manner.

To create a gateway for automatic, regular importing or exporting:

1. Go to the Gateway Settings page.
2. Click the **Add Gateway** tab.

3. Select whether you want an email or newsgroup gateway and choose the space (community) with which you want to sync the external data source.
4. Click **Add Gateway**.
5. On the Add an Email Gateway page, configure basic and advanced settings as needed. You'll find more information about these settings in the tables below.
6. Click **Add Gateway**.

To use a gateway for a one-time or at-need synchronization:

1. Go to the Gateway Settings page.
2. Click the **Import Once** or **Export Once** tab.
3. Select a gateway corresponding to the data source you're synchronizing with (note that you can't export to an mbox file) and choose the space (community) with which you want to sync the external data source.
4. Click **Import Once** or **Export Once**.
5. Configure basic and advanced settings as needed. You'll find more information about these settings in the tables below.
6. Click **Import Messages** or **Export Messages**.

Gateway Settings

The following tables describe general settings available for gateways. You'll set these either globally or for each new gateway you create.

Table 2: Global Settings

Setting	Description
Gateway Importing	Enables or disables the importing feature.
Gateway Exporting	Enables or disables the exporting feature.
Time between imports	The amount of time that should pass between imports from a data source.
24-hour buffer for importing messages	Enables or disables buffered importing feature, which imports messages that might have been missed from the 24-hour time period before the last import.
Outgoing message footer	The text that should appear at the bottom of messages synced to the data source from the space. This is a way to mark exported content with a boilerplate message. In your footer text, you can use the tokens shown in curly braces at the left of the message box. For example, imagine content synced to a newsgroup from a space called "Product Suggestions". Footer text such as "Posted from {communityName}." would be posted in the exported message as a footer that read, "Posted from Product Suggestions."

Table 3: New Gateway Settings

Setting	Description
Gateway Importing	Enables or disables message importing for the new gateway.
Gateway Exporting	Enables or disables message exporting for the new gateway.
24-hour buffer for importing messages	Enables or disables the buffered importing feature, which imports messages that might have been missed from the 24-hour time period before the last import.

Newsgroup Gateway Settings

You can create a gateway between a space in your community and a *Network News Transfer Protocol (NNTP)* newsgroup. Using this gateway, you can have messages transferred, or synchronized, between the newsgroup and a specified space in your community.

When creating a newsgroup gateway, you specify newsgroup connection information, as well as details about how outgoing and/or incoming messages should be handled.

Note: These settings are available when you're creating a gateway for regular use or creating it for one-time (or at-need) use. The following tables summarize all of the settings you might see, although not all settings will be available wherever you configure a newsgroup gateway.

Table 4: Newsgroup Settings

General settings that are required to connect to the newsgroup.

Setting	Description
Host	The name of the NNTP server host. This is often a domain, such as news.example.com, or an IP address.
Newsgroup	The newsgroup hosted by the server with which messages will be synchronized.

Table 5: Outgoing Newsgroup Settings

Setting	Description
Default "From" address	The address to use for the message's source when no address is specified. This is usually an email address.

Table 6: Advanced Newsgroup Settings

Setting	Description
NNTP server port	The port number to use when connecting to the NNTP server. The default is port 119; for SSL the normal port to use is 993.
NNTP server username	The username needed to authenticate with the NNTP server.
NNTP server password	The password needed to authenticate with the NNTP server.
Debug	Enables or disables debugging for the NNTP transport layer, writing debug information to System.out.err. Debugging shouldn't be enabled for a production instance.
Allow import/export of attachments	Enables or disables attachments in messages synchronized with the newsgroup. If disabled, attachments are stripped before import or export.
Default character set	The character set that will be used to decode incoming messages that have no explicit character set defined.

Table 7: Advanced Incoming Newsgroup Settings

Setting	Description
Enable threading via subject line matching	Enables or disables the feature in which incoming messages are organized into threaded discussions by grouping messages that have the same subject.
Enable email address to user mapping	Enables or disables the feature in which the email address of the newsgroup message poster is matched with a user on the system. Where a matching address is found, the user associated with that address is shown as the author of the imported message. If an address is not found, the user is shown as guest.
Temporary parent body	The text that should be used when creating temporary parent messages. It's possible with email accounts and mailing lists to get a response to a message before getting the original message. If this happens and only the child message is available at the time of the gateway import, the application must still have

Setting	Description
	a way to establish a correct parent/child relationship. Therefore, a temporary fake parent message is created using an extrapolated subject from the child, and a body with the value you specify. You might want to create a short message that explains the nature of the fake parent message to the user. On subsequent imports when a real parent message is found, the fake data will be replaced with the correct subject and body.
Empty subject string	The text to use for a message's subject where an imported has no subject text.
Default character set	The character set that will be used to decode incoming messages that have no explicit character set defined.

Table 8: Advanced Outgoing Newsgroup Settings

Setting	Description
Organization	The value for the NNTP Organization header field. This is usually short phrase that describes the sender's organization, such as "Example Company, Product Community". Something with the name of the space might be useful, for example. The default is for the field to be empty.
Honor user email preference	Choose "Yes" to honor email privacy settings of the user who posted the exported message (in other words, whether they want their email address displayed).
Export messages after (date)	The earliest date from which messages should be exported.
Allow messages to be exported again	Enables or disables re-exporting of messages. By default, a message that has previously been exported or imported, or which was automatically created for threading purposes by an import gateway, is not exported again. You can specify instead that messages should be re-exported again if absolutely needed. This is typically not enabled, and should only be enabled with care.
Update NNTP message ID stored in Jive	Enables or disables updating a message's ID in the application system when the message is exported. When this is disabled, the message ID is left unchanged in order to prevent the message from being re-exported. This setting has no effect unless the re-exporting is enabled using the "Allow messages to be exported again" setting.

Email Gateway Settings

You can create a gateway between a space in your community and an email server. Using this gateway, you can have messages transferred, or synchronized, between the server and a specified space in your community.

When creating an email gateway, you specify connection information as well as details about how outgoing and/or incoming messages should be handled.

Note: These settings are available when you're creating a gateway for regular use or creating it for one-time (or at-need) use. The following tables summarize all of the settings you might see, although not all settings will be available wherever you configure a newsgroup gateway.

Table 9: Incoming Mail Settings

Setting	Description
Type	The protocol that will be used to retrieve incoming email. Note that advanced incoming mail settings differ depending on whether you choose *POP3* or *IMAP*.
Host	The name of the email host, such as mail.example.com

Setting	Description
Username	The username to use for authenticating with the email server.
Password	The password to use for authenticating with the email server.

Table 10: Outgoing Mail Settings

Setting	Description
Host	The name of the SMTP host for outgoing email, such as mail.example.com
Default "From" address	The email address to send mail from when exporting. This is used for messages from anonymous users or users who hide their information.
"Reply-To" address	The email address that should appear in the To line when the exported email is replied to.
"To" address	The email address that messages will be sent to during exports. If the gateway is for a mailing list, this would be the mailing list address (for example, your-list@example.com).

Table 11: Advanced Incoming Mail Settings

Setting	Description
POP3 server port IMAP server port	The port number that will be used when connecting to the server. For POP3, the default is 110, the standard POP3 port number; for IMAP, the default is 143.
SSL	Enables or disables connecting to the server using an SSL encrypted connection. Currently, if an encrypted connection cannot be made, an unencrypted connection will be attempted.
Folder (IMAP only)	The name of the root folder from which to import. By default, the IMAP provider will use the normal 'INBOX' folder, or whatever is specified as the default according to the IMAP server.
Delete messages from server (POP3 only)	Enables or disables having messages deleted from the server after they've been downloaded.
Allow import of attachments	Enables or disables allowing attachments to be imported with their messages.
Enable threading via subject line matching	Enables or disables the feature in which incoming messages are organized into threaded discussions by grouping messages that have the same subject.
Enable email address to user mapping	Enables or disables the feature in which the email address of the message sender is matched with a user on the system. Where a matching address is found, the user associated with that address is shown as the author of the imported message. If an address is not found, the user is shown as guest.
Temporary parent body	The text that should be used when creating temporary parent messages. It's possible with email accounts and mailing lists to get a response to a message before getting the original message. If this happens and only the child message is available at the time of the gateway import, the application must still have a way to establish a correct parent/child relationship. Therefore, a temporary fake parent message is created using an extrapolated subject from the child, and a body with the value you specify. You might want to create a short message that explains the nature of the fake parent message to the user. On subsequent imports when a real parent message is found, the fake data will be replaced with the correct subject and body.
Empty subject string	The text to use for a message's subject where an imported has no subject text.

Setting	Description
Default character set	The character set that will be used to decode incoming messages that have no explicit character set defined.
Debug	Enables or disables debugging for the email transport layer, writing debug information to System.out. Debugging shouldn't be enabled for a production instance.

Table 12: Advancted Outgoing Mail Settings

Setting	Description
SMTP server port	The port number to use when connecting to the SMTP server. The default is 25, the standard SMTP port number.
SSL	Enables or disables SSL connections to the SMTP server. Unlike most standard SSL, connections to the SMTP server are often on the same port as unencrypted connections (port 25).
Username	The username to use when authenticating with the server.
Password	The password to use when authenticating with the server.
Organization	The name to set in the Organization header of the outbound message. This is usually short phrase that describes the sender's organization, such as "Example Company, Product Community". Something with the name of the space might be useful, for example. The default is for the field to be empty.
Only use default "From" address	Set to "Yes" to use only the default "From" address when sending email, ignoring user preferences.
Honor user email preference	Set to "Yes" to honor email privacy settings of the user who posted the exported message (in other words, whether they want their email address displayed).
Allow export of attachments	Enables or disables exporting attachments with their messages.
Custom character set	The character set that will be used to encode outgoing messages.
Export messages after (date)	The earliest date from which messages should be exported.
Allow messages to be exported again	Enables or disables re-exporting of messages. By default, a message that has previously been exported or imported, or which was automatically created for threading purposes by an import gateway, is not exported again. You can specify instead that messages should be re-exported again if absolutely needed. This is typically not enabled, and should only be enabled with care.
Update email message ID stored in Jive	Enables or disables updating a message's ID in the application system when the message is exported. When this is disabled, the message ID is left unchanged in order to prevent the message from being re-exported. This setting has no effect unless the re-exporting is enabled using the "Allow messages to be exported again" setting.
Debug	Enables or disables debugging for the email transport layer, writing debug information to System.out. Debugging shouldn't be enabled for a production instance.

MBox File Import Settings

You can create a gateway that imports messages into a space from an *mbox* file.

Table 13: Import Settings

Setting	Description
File	The path to the mbox file whose contents will be imported.
Allow import of attachments	Enables or disables importing attachments with their messages.
Enable threading via subject line matching	Enables or disables the feature in which incoming messages are organized into threaded discussions by grouping messages that have the same subject.
Enable email address to user mapping	Enable this to turn on the feature in which the email address of the message sender is matched with a user on the system. Where a matching address is found, the user associated with that address is shown as the author of the imported message. If an address is not found, the user is shown as guest.
Import HTML messages	Enables or disables importing of HTML email. If enabled, HTML email will be imported as the message body; otherwise it will be imported as an attachment.
Reply prefixes (comma-separated)	The prefixes that will be stripped from messages when attempting to find a parent message via subject line matching. Prefixes are lowercase, with default values including 're:' and 'aw:'

Preventing Spam

Use these best practices to avoid spam in your community.

Community administrators of external communities should develop a strategy for dealing with spam (internal communities do not typically experience spam). The following methods are available as *general spam-prevention strategies* or to *target specific spammers*. Choose the method(s) that will work best for your unique community.

General Spam Prevention Methods

Method	Description	To learn more, see this topic:
New User Registration Moderation	Assign a moderator(s) to approve or reject new user registrations.	*Moderating User Registration*
Captcha for New User Registrations	Require that users type in a Captcha image when they register for the community.	*Configuring User Registration*
Email Validation	Require that the application send an email to the address a new user provides at registration. The user must then use a link in the email to complete registration.	*Configuring User Registration*
Restrict Email Domains	Restrict the domains from which email registrations can be accepted. Set the following parameters in **Admin Console:** > **System** > **Management** > **System Properties**: `registration.domainRestriction.enabled = true` `registration.domainRestriction.domains = the list of allowed domains, separated by commas` `registration.domainRestriction.company = your company name`	
Captcha at User Log In	Require that users type in a Captcha image when they log in to the community.	*Configuring Login Security*

Method	Description	To learn more, see this topic:
View-only Guest Users	Disable the ability of guests to create content by limiting the permissions of "Everyone" to view-only (guests are members of "Everyone"). You would give only Registered Users the ability to create content.	*Managing Permissions*
Bi-directional User Relationships	Require bidirectional user relationships (friends).	*How User Relationships Work* and *Configuring Sharing*
Askimet for Blog Comments	Use Askimet to help prevent blog comment spam.	*Configuring Blogs System-Wide*
Keyword and/or Message Governor Interceptors	Limit the frequency of posts and search for spam keywords.	*Configuring Interceptors*
Content Moderation	Enable content moderation so that users must submit content for approval before it's published in the community.	*Moderating Content*

Targeting Specific Spammers

Method	Description	To learn more, see this topic:
Ban Users	Ban malicious users by blocking their login credentials or their IP address.	*Banning People*
Ban IP Addresses	Ban one or more or a range of IP addresses.	*Banning People*

Setting Up Document Conversion

Some documents -- including PDFs and those from Microsoft Office -- are supported in a preview view in Jive. If you want to convert content from its native format into a form that can be previewed without altering the original document, you'll need the Document Conversion module, which you'll need to deploy on a server that is separate from your core Jive production instances.

We support converting the following file types on Office 2003 and 2007:

- doc
- ppt
- docx
- pptx
- xls
- xlsx
- pdf

Note: For information about managing conversion attempts and reconverting documents if necessary, see *Managing Document Conversion*.

Here is an overview of the steps you'll perform to set up Document Conversion:

1. Set up a production instance of the Jive application (see *Installing the Linux Package*. When you've finished configuring and customizing it, disable the Document Conversion service with `service jive-docconverter stop`.
2. Install the application on your conversion node machine. Then disable the services not related to document conversion. For more information, see *Installing and Configuring on the Conversion Machine*
3. On the application node, *configure the application to communicate with the conversion machine(s)*.
4. If you want to set up secure communication to the conversion machine, see *Setting Up SSL for Document Conversion*.

Setting Up the Conversion Machine

The document conversion machine should be a dedicated machine that isn't used for any other Jive services. After you *install Jive on the conversion machine*, use the following commands to disable all the services other than jive-docconverter. Run all of these commands as **root** unless otherwise noted.

```
service jive-database stop
 service jive-eae-service stop
 service jive-application stop
 service jive-httpd stop
 service jive-cache stop
```

Setting Up SSL for Document Conversion

If you have an SSL certificate, you can set up secure communication by editing the docconverter/conf/server.xml file and specifying the new secure URL in your Document Conversion Settings.

Before you can set up secure communication with your Document Conversion server, you need to acquire an SSL certificate.

1. Edit the `/usr/local/jive/services/docconverter/conf/server.xml` file and add a connector to listen on port 8443.
   ```
   <Connector port="8443" maxThreads="200" scheme="https" secure="true"
   SSLEnabled="true" SSLCertificateFile="/usr/local/jive/services/docconverter/
   home/jive.crt" SSLCertificateKeyFile="/usr/local/jive/services/docconverter/
   home/jive.key" clientAuth="optional" />
   ```

   where `SSLCertificateFile` is the certificate file and `SSLCertificateKeyFile` is the key file.

   For more information on setting up Tomcat and https, see: *http://tomcat.apache.org/tomcat-6.0-doc/ssl-howto.html*
2. Make sure the SSL engine is on.
   ```
   <Listener className="org.apache.catalina.core.AprLifecycleListener"
   SSLEngine="on"/>
   ```
3. Restart the document conversion service.
   ```
   /etc/init.d/jive-docconverter restart
   ```
4. Go to **System** > **Settings** > **Document Conversion Settings** and edit the Conversion Service Settings to specify the new secure URL and port.
   https:// conversion-node :8443 /conversion/v1
5. Verify that you can run all conversion tests successfully.

Configuring a Conversion Node Connection

Use the Document Conversion Settings page to configure the node that hosts the coreJive application, so the main application knows how to communicate with any conversion machines you've set up. Before you use the settings on this page, you should already have set up a document conversion node. For an overview of Document Conversion setup, see *Setting Up Document Conversion*.

Fastpath: Admin Console: System > Settings > Document Conversion

The Document Conversion Settings page is pre-populated with the default values for most installations. Use the following steps to ensure your setup is correct.

To enable document conversion:

1. Select **Enabled**.
2. Click **Add a Node** to start configuring a conversion machine.
3. Enter the IP address or hostname for the conversion machine.
4. If you want to exclude some file types from conversion, enter a comma-separated list in **Disabled Extensions**. For example, if you don't want to convert Excel files, type:

```
xls, xlsx
```

Troubleshooting Document Conversion Machine Setup

If your document conversion tests are failing, try investigating the following areas to resolve the problem:

1. Check that port 19003 is open between the application node and the conversion node by executing a telnet command. For example, run `telnet 10.61.32.156 19003`.
2. Check the log for the doc-converter service for startup exceptions. You can find the log at `/usr/local/jive/var/logs/docconverter.out`.
3. If the office to pdf test is failing in the Document Conversion Setup screen, execute `ps aux | grep soffice` to verify that the OpenOffice processes managed by the Java doc-converter process are running.

Managing Document Conversion

As the application converts PDFs and Office documents for preview, you can manage the conversions and troubleshoot them when necessary. For example, you can delete failed conversion attempts, prompting the application to reconvert the document.

You manage conversion in the admin console.

Fastpath: Admin Console: System > Management > Document Conversion Status

In the admin console, on the Document Conversion Management page, you can view the status of conversions. For each conversion in the list, you'll find the following information. You can filter the list of items using the box at the top of the page. For filtering, you can use either the full document ID number or a partial document file name.

Item	Description
File Name	The document's file name. If you have rights to the document, you can click the file name to see the document in the community or to re-run the conversion, or click **View** to see only the converted document if available. You won't have access to private documents or documents in secret groups.
Size	The file size in bytes.
PDF Status	Shows whether PDF conversion succeeded.
Pages	The number of pages in the document. This will be blank for failed conversion attempts.
Preview Status	Shows whether a preview was successfully created.
Thumbnail Status	Shows whether a thumbnail view was successfully created.
Time	Shows when the conversion attempt completed.
Error	Shows any errors that occurred during the conversion attempt.

Configuring People-Related Settings

This section includes information about configuring features related to user access (such as password resets), user relationships, user status, and so on.

Managing Access

You can manage people's access to Jive features through the admin console. A few of these features are available to system administrators only. But the work of granting permission for specific user and administrator tasks is available to both system and space administrators.

Configuring Password Reset

You can give people the ability to change or securely reset their own passwords. Enabling the password reset feature does two things:

- Displays a link on the login page through which people can request a password reset if they forget their password.
- Displays a "change password" link on people's profile page. They can use this to change the password with the help of password strength tips and a strength meter.

Fastpath: Admin Console: People > Settings > Password Reset

Click **Enabled** to enable the password reset feature, then click **Save Settings**.

Note: You can customize the email that's sent when someone requests to reset their password. For more information, see *Managing Email Templates*. For more on configuring registration and login, see *Configuring User Registration* and *Configuring Login Security*.

Configuring User Registration

You can configure the application so that new users can create their own accounts and current users can invite others to join. Use the Registration Settings page to *enable user-created accounts* and to *set up how account creation works*.

You can also configure registration so that the application displays a terms and conditions page when people register. For more information, see *Configuring Terms and Conditions*.

Fastpath: Admin Console: People > Settings > Registration Settings

Note: People using the community must set their browsers to enable cookies. The application doesn't encode session IDs in URLs.

Allow User-Created Accounts

Click **Enabled** to allow user-created accounts and to allow current users to let other to join. When user-created accounts are enabled, people can sign up for a new account from the login page. The registration process takes them through a brief set of screens through which they add the information you've requested in the admin console's Registration Settings page.

When user-created accounts are enabled, users can invite others to join the community from their Profile page. For more on inviting new community members, see *Inviting New Community Members*

New User Account Settings

Use the following table to conifgure user account settings. You must enable user-created accounts so the New Account Settings section of the Registration Settings page is available for editing.

Setting	Description
Password Strength Check	You can specify how strong you want user passwords to be. The password strength indicator will help the person registering create a password that's strong enough to qualify.

Setting	Description
Human Input Validation	Enable this to require that a person registering be prompted with a *captcha* image. The image displays text (distorted to prevent spam registration) that the person must enter in order to continue with registration. This is a way to discourage registration by other computers simply for access to community in order to send spam messages. Human input validation generally isn't needed for internal communities that aren't accessible to the public.
Email Validation Settings	Enable this to have the application send an email to the person registering at the address they provided (you can edit the contents of the template used for the email). By default the email includes a link that the person must use to prove that the email address they gave is a valid one. This is another means to discourage false registration.
Welcome Email Settings	Enable this to have the application send the new user an email when they've finished registering. You can edit the template for emails like this.
User Wizard Settings	Enable to send new users through a wizard that helps them set up their profile. If your disable, then users will need to click their name to the upper right corener and then click **Edit profile & privacy** in the Actions list.
Registration Moderation	If you enable moderation for membership requests, new registration requests will appear on administrators' Pending Approvals profile tab. To get to the tab, in the end user UI click Your Stuff > Items Awaiting Approval. (If you have a user administrator, that person will approve or decline requests; otherwise, the system administrator will get those requests.)
Fields displayed at registration	You can define the fields that are displayed to prompt a user for information while they're registering. The fields you can choose from here are based on the fields defined for user profiles. For more on profile fields, see *Defining User Profile Templates*

Configuring Terms and Conditions

You can write a page that describes your community's terms and conditions, then prompt users to accept them when they register for access to the community. In the admin console, you can indicate what the terms and conditions page should include.

Fastpath: Admin Console: People > Settings > Terms and Conditions

Setting	Description
Enable/Disable Terms & Conditions	Click **Enabled** to enable the terms and conditions feature, meaning that the registration user interface will display the terms and conditions form you specify (either by writing your own or linking to them at the URL you give in the admin console).
Force existing users to re-accept modifications	Click Yes to require that users who've already accepted the terms and conditions do so again. You might want to do this, for example, if you update your terms and conditions and want people to accept the new ones.
Terms & Conditions source to be used	Indicate whether you want the terms and conditions page to consist of the text you type in the box at the bottom of the Term & Conditions Settings page, or to be displayed from a URL that you give.

Specifying the Terms and Conditions Text to Display

At the bottom of the admin console's Terms & Conditions Settings page, you can either type the text that should be displayed for terms and conditions, or link to a page at a particular URL.

To use text you type:

1. Next to **Terms & Conditions source to be used**, click **Internal, from the editor below**.

2. In the editing window near the bottom of the console page, type or paste the terms and conditions text you want to use. Notice that you can format the text with the buttons at the top of the editing window.
3. Be sure to click **Save Settings** when you're finished configuring on this page.

To use an external page reachable via a URL:

Note: Due to Microsoft security issues in the Internet Explorer browser, the Terms & Conditions will not display correctly if they are not stored on the same server as the Jive app when the Jive app is set up to use HTTPS. Therefore, we strongly recommend that you store the Terms & Conditions within the Jive app or on the same server as the Jive app. If this is not possible, you could prevent this error by adding the Terms & Conditions URL to the list of IE's trusted sites or set IE to allow iframes to load remote sites.

1. Next to **Terms & Conditions source to be used**, click **External, from the URL below**.
2. Next to **External Terms & Conditions URL**, enter the URL that points to your terms and conditions page.
3. Be sure to click **Save Settings** when you're finished.

Configuring Login Security

You can set up the application to discourage automated (computer-driven) registration and login. Automated registration is usually an attempt to gain access to an application in order to do malicious (or at least annoying) things. By taking steps to make registering and logging in something that only a human being can do, you help to prevent automated attacks.

This topic is about configuring login security in particular. You configure registration security on the Registration Settings page. For more information, see *Configuring User Registration*.

Fastpath: Admin Console: People > Settings > Login Security

On the admin console's Login Security Settings page, you can set up login throttling and login captcha.

Login Throttling

Enabling login throttling slows down the login process when the user has entered incorrect credentials more than the specified number of times. For example, imagine that you set the number of failed attempts to 5 and a forced delay to 10 seconds. If a user failed to log in after more than five tries, the application would force them to wait for 10 seconds until they could try again on each subsequent attempt.

Login Captcha

Enabling login captcha displays a *captcha* image on the login page. The image displays text (distorted to prevent spam registration) that the person must enter in order to continue with registration. This is a way to discourage registration by other computers simply for access to community in order to send spam messages.

The login captcha setting is designed to display the captcha image when throttling begins. In other words, after the number of failed attempts specified for throttling, the captcha image is displayed and throttling begins. You can't enable the login captcha unless login throttling is enabled.

The captcha size is the number of characters that appear in the captcha image, and which the user must type when logging in. A good value for this 6, which is long enough to make the image useful and short enough to keep it from being too annoying.

Enabling Username Reminders

You can configure Jive to send out reminders for users who forget their usernames. If a user forgets their username, you can add an **I forgot my username** prompt to the login screen. This prompt directs the user to a place where they can generate an automatic email to the address they used when they registered their account.

Fastpath: Admin Console: People > Settings > Forgot Username

To allow users to request their username, select **Enabled - Users are allowed to request their usernames be sent by email** and click **Save Settings**.

Note: You can edit the Forgot Username message template in **System > Settings > Message Templates**. Edit this template to customize the email that is automatically sent to users who forget their username and request it. For more on message templates, see *Editing Email Notification Templates*.

Banning People

You can block a person's access to Jive. For example, if someone becomes abusive in their messages (or moderating their content is too time-consuming), you might want to ensure that they can't log in any more. You can ban them through their login credentials or their IP address.

For each person you ban, you set a ban level that determines whether you're banning them from logging in or merely posting content. You can also set an expiration date for the ban. Typing a comment, such as a note about the reason you banned them, you can leave a record for other administrators.

Fastpath: Admin Console: People > Settings > Ban Settings

Ban Settings

Use the Ban Settings tab to set general properties for the ban feature. You can enable or disable the feature. Disabling the feature will disable all bans that you currently have in effect.

You can arrange to send email to people that you ban. This message is based on a template you can edit; for more information, see *Managing Email Templates*.

Ban a User Account

Through the Ban User Account tab, you can ban someone by specifying their username.

Ban an IP Address or a Range of IP Addresses

If you have IP address tracking turns on, you can ban an IP address or a range of addresses. First, enable IP address tracking by setting the system property skin.default.trackIP to true. (For more information on system properties, see *Fine-Tuning with System Properties*), then enter the IP address you want to ban. To ban a range of address, use a wildcard asterisk, for example, `111.111.1.*`.

Configuring User Relationships

You can configure the relationships feature so that it best fits the way people using Jive will interact with each other. You do that by making settings for the relationship graph. A relationship graph is a representation of a set of objects that are connected to one another. Here, the objects are user accounts, which in turn represent people in your community.

Fastpath: Admin Console: People > Settings > User Relationship Settings

Be sure to read the overview on user relationships, *How User Relationships Work*.

The application supports two kinds of graphs: an organizational chart graph and a friend/connection graph. As you might expect, the organizational chart graph represents relationships that are usually hierarchical, such as between a manager and their direct reports.

Disable relationships by clearing the **Is graph enabled** check box.

Connections Settings

- Make connection relationships **bidirectional** when you suspect that people will want to keep up with those who want to keep up with them. These are friend relationships, in which a person is invited to connect with someone who has requested to connect with them. Clear this check box, on the other hand, when you think that people won't necessarily want to keep up with someone who is keeping up with them.

- Enable the **approval process** to require that the person being connected to must approve the connection.

Organizational Chart Settings

- The **manager choice** and **direct report choice** options are mutually exclusive -- you need to choose either one of those or **neither**. Select neither when your hierarchical relationships between users are managed by an external system, such as LDAP. Select the manager choice option to allow people to choose from the user list who should be displayed as their manager. Select the direct report choice option to allow people to choose who is listed among their direct reports. If you select neither, but relationship data isn't managed externally, you can create these relationships yourself. For more information, see *Defining User Relationships*.
- Enable the **approval process** to require that the person being connected to must approve the connection.
- In the **Notified Users** box, enter the user names of people who should be notified when relationships are created (such as someone in the human resources department).

Configuring Status Levels

Enable status levels to encourage people to get involved in the community. People can accrue status by earning points as they create and respond to content in Jive. Assigning status levels this way is sometimes known as "badging." Over time, people develop a reputation for reliability and authority in their favorite areas. The more people participate, the more information that is available for the community as a whole. Where a person's name is displayed, the user interface displays a status icon or badge such as

corresponding to the number of points the person has accrued.

Fastpath: Admin Console: People > Settings > Status Level Settings

You can use the following suggestions to make the most of status levels:

- *Set the number of points per scenario* based on the kinds of activity you want to reward. For example, if you want to provide a context in which questions are usually answered, award more points for correct and helpful question responses.
- Define status levels or badges that people will be enthusiastic about -- make it fun. For example, you could think of it as a kind of game. Is the highest level a "Ninja"? A "Genius"? "Indiana Jones" or "Nobel Laureate"? Devise a list of levels that goes well with the culture of people using the community and *edit the existing status levels*.
- Offer rewards or recognition for people who reach or maintain certain status levels.

Note: When content is deleted, status points are also deleted.

Adjusting Status Scenarios and Points

You can set how many points are awarded for a given scenario or action the user takes in the application. If you give the action *User's status was liked* 1 point, then a user's status points will increase by one point whenever someone likes their status.

You can also define the status levels themselves, setting the point range that the status level represents. By default, for example, the application includes the following status levels: master (501-1000 points); junior (101-500 points); newbie (0-100 points). You can configure the levels, along with how many points correspond to an action.

Disable a scenario when you want that scenario not to be included in status level calculation.

Adding and Editing Status Levels

You can edit the existing status levels or create new ones. In addition, the application includes more than 50 status level images for you to use. You can also replace existing images with new ones or add your own images and associate them with status levels that you create.

Fastpath: Admin Console: People > Settings > Status Level Settings

- To edit an existing status level, locate the level in the list and click its **Edit** button. Its current property values will appear in the **Add/Edit status level** box. Change the values as you like, then click **Save**.
- To add a new status level, make sure the **Add/Edit status level** fields are all blank (clicking the **Cancel** button clears the fields). Now enter the values you want and then click **Save**.

Table 14: Status Level Properties

Setting	Description
Name	The name that should appear for the status level.
Description	Additional text to describe the status level. By default, this doesn't appear in the user interface.
Add or replace existing level icons (in versions 5.0.4 and higher)	In Jive versions 5.0.4 and higher, you can add your own status level images by clicking **Add or replace existing status level icons**, and then selecting your image and uploading it. Images uploaded this way will be stored in <jive.instance.home>/www/resources/images/status. After you've uploaded an image this way, you will be able to see it as an available image option when you associate an image to a status level using the Image Path/Large Image Path image picker.

Image Path and Large Image Path	The application includes more than 50 status level images. You can choose from among the included icon images by selecting Image Path/Large Image Path and then clicking **Pick Image**.
	
	To add your own images, add your custom image files to <jive.instance.home>/www/resources/images/status. If the <jive.instance.home>/resources directory doesn't exist, you can create a symlink to /usr/local/jive/var/www/resources/images/status using the following commands:
	
	`cd <jive.instance.home>`
	`ln -s /usr/local/jive/var/www/resources resources`
	
	You can use GIF or other types of image files, but you should use the same naming scheme as the existing images: statusicon-<number-in-sequence>.gif. You might want to start your numbering at some higher level to avoid problems if application upgrades include more images. For example, to add five new images (where included images currently end at number 52), you could add images called statusicon-100.gif, statusicon-101.gif, statusicon-102.gif, statusicon-103.gif, and statusicon-104.gif.
	
	(Note that in versions 5.0.4 and higher, you can upload your custom image files to the Jive file server using the **Add or replace existing level icons** feature. This is useful if you don't have scp or other direct access to the application file server.)

Point Range or Group	You can asssociate this status level with either a point range or a user group. Entering a point range will tie this status level to users' activity in the community. Alternatively, if you select **Unbounded**, no point range will be associated with this status level. If you want certain users in your community to always have a particular status level regardless of their activity, select **Group**. This will associate this status level with a user group that you select. For example, you could define a user group made up of a few community managers or gurus, then associate a special status level to them in order to have a recognizable name and icon visible to other people.

Avatar Settings

An avatar is an image that represents a person in the community. A person's avatar is displayed when they contribute. Avatars are one way for people to make their participation in the community more personal. You can configure avatars in the admin console.

Fastpath: Admin Console: People > Settings > Avatar Settings

Managing Default Avatars in the Gallery

The application includes several avatar images. By default, administrators and moderators can choose from among these, but you can enable the choice for registered users as well. When registered users can choose avatars, they'll be able to choose from the avatars pictured in the admin console. If the community is configured to support it, they can also upload their own images to use as avatars.

With avatars enabled, users see a "Change photo & avatar" link in the Actions list of their profile page. Depending on how you've set up the feature, users will be able to select from the set of avatar images you've selected, or upload their own.

Adding and Deleting Default Avatars

As an administrator, you can delete existing default avatars or upload new default avatars. To upload a new avatar, from the Avatar Settings page, scroll down to Create New Avatar, and then browse to and upload your new image.

Supporting User-Uploaded Avatars

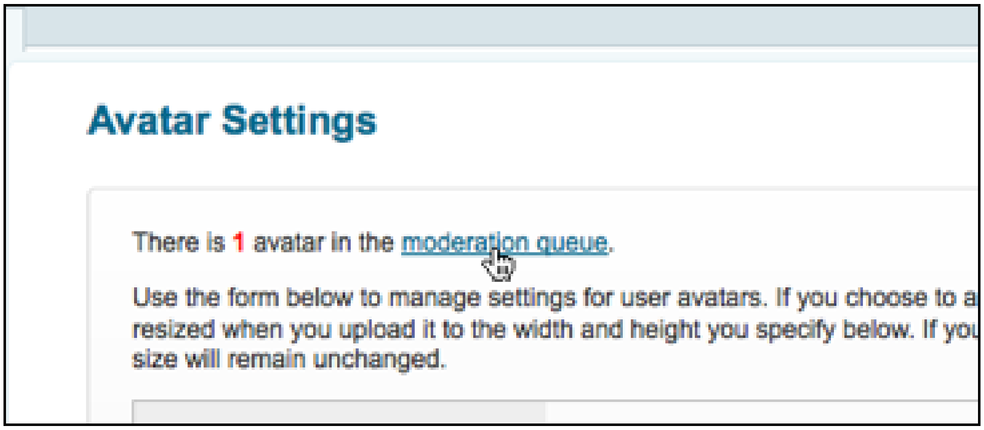
You can enable avatars for users so they can personalize their profile. You can also allow users to further personalize their experience in the community by enabling user-uploaded avatars. With this feature enabled, people can upload as many images as you specify, and choose one of these images when they want to make a change. You can set the maximum height or width that uploaded avatars should be (in pixels, by default 128 by 128). Enable auto resizing of uploaded avatars to make it easier for people to upload the images they want to use.

Moderating User-Uploaded Avatars

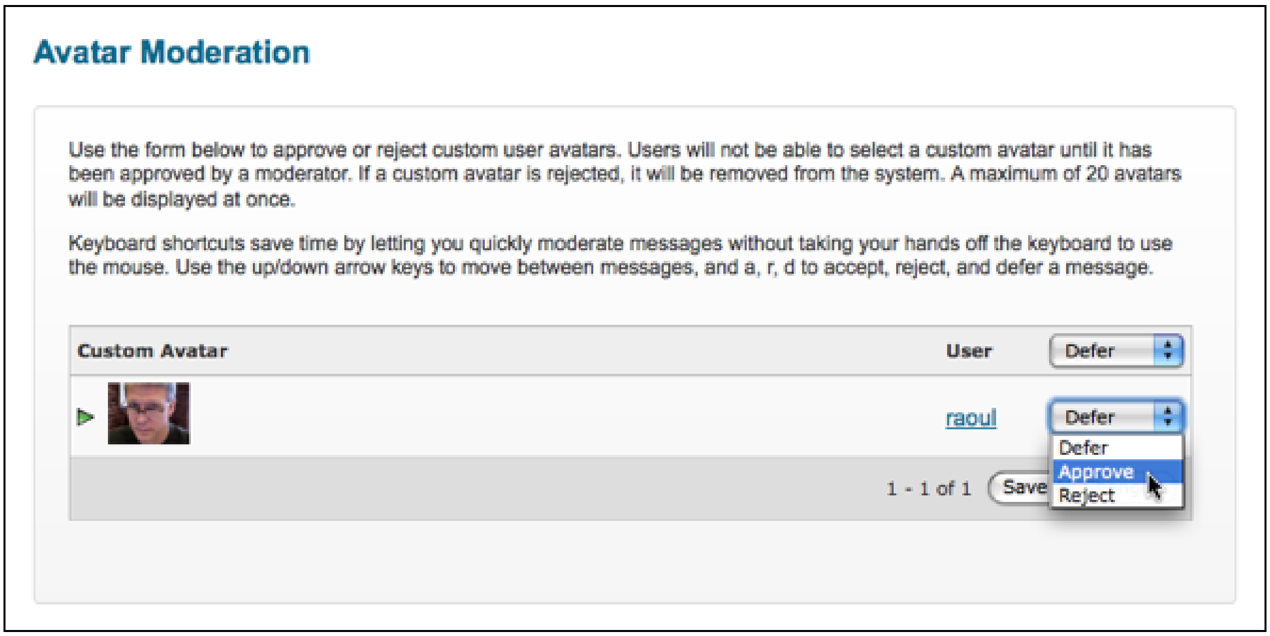
You can have every user-uploaded avatar image added to a moderation queue for approval by checking **Moderate uploaded user avatars**. When you choose to have avatars moderated, a user uploading an avatar will be told by the UI that their avatar choice is pending approval. Once approved, the avatar will be available for the user to designate it (or others) as their primary avatar. It will not become the user's primary avatar until the user manually selects it.

After a user uploads an avatar, the avatar moderation queue becomes available to a system administrator through a link on the Avatar Settings page in the Admin Console as shown in the following image.

Note: You only see the link when there are images in the queue.



The administrator will then select **Defer, Approve, or Reject** for images listed in the moderation queue.



Note: User-uploaded avatars won't appear with the default avatar images on the Avatar Settings page. You can view (and delete) a user's uploaded avatar by going to their account summary page in the admin console. To do that, click People > Management > User Search, then click the user's name in the list to view their summary page. On that page, under User Avatars, you can view and delete their uploaded avatar images.

Resizing Avatars

You can set the maximum height or width that uploaded avatars should be (in pixels, by default 128 by 128). Enable auto resizing of uploaded avatars to make it easier for people to upload the images they want to use.

Configuring Profile Image Moderation

You can enable moderation for images that users upload for use in their user profile. When you do, the request to upload the image will appear in the moderation queue of a system-level content moderator. That person must approve the image before it will appear in the profile of the person who uploaded it.

Fastpath: Admin Console: People > Settings > Profile Image Moderation

This option is either fully enabled for all users or fully disabled for all users. This feature assumes you've already turned on the user Profile Image Visibility feature. For more about that, see *Configuring User Customization*.

Note: Before setting up profile image moderation, you'll need to first assign system-level moderation permissions to a user group. People in the group will be able to view the queue that lists moderation requests for profile images. For more on assigning system level moderation permissions, see *Managing Administrative Permissions*. When assigning permissions, be sure to select the Moderate Content permission level.

Configuring User Update Settings

After setting up your community, which may include granting permissions for iPhone access, you might want to customize settings that apply to the user personal updates, such as character limits and sharing updates. For more on setting up your community to use a mobile phone to create updates, see the Jive Mobile documentation.

Fastpath: Admin Console: People > Settings > User Status Settings

To activate user status settings, select **Enabled**, then **Save**. You can also configure the following settings:

- **Reposting Enabled:** When selected, enables users to repost a status update from another user so they can share that information without retyping it.
- **Character Limit:** Indicates the character limit of a user's personal update message. The default limit is 420.

Setting Up Access to Twitter

Users in your community can write personal updates from Twitter. Once you've installed the Twitter plugin, you need to take a few additional steps to complete the set up. For more on installing plugins, see *Adding and Removing Plugins*.

Fastpath: Admin Console: People > Settings > Twitter Settings

Use the following steps to complete the Twitter setup:

1. Selected **Enabled**, but you have to register the application before you save.
2. In another browser window, open *http://www.twitter.com/apps*.
3. Click **Register a New Application**
4. Complete the **Register an Application** form using the following guidelines.

Table 15: Twitter Application Registration Form

Setting	Description
Application Icon	Select an icon to represent your application.
Application Name	Enter the name of your Jive application.
Description	Tell a little bit about how you are using your Jive application.
Application Website	Enter the website address for your Jive application.
Organization	Enter the name of your organization or company.
Website	Enter your organization or company name.
Application Type	Select **Browser**.
Callback URL	Type the Callback URL found in the Twitter Settings page of the Admin Console. For example, `http://mysbs/twitter-auth-callback.jspa`
Default Access Type	Select **Read-only**.
Use Twitter for login	Select **Use Twitter for login**.

5. Click **Save**.
6. When Twitter provides the registration details, copy the **Consumer Key** and **Consumer Secret** to the **Twitter Consumer Key** and **Twitter Consumer Secret** in the Twitter Settings page of the Admin Console.

7. You can change the default Twitter hashtag of `#sbs` to something that makes more sense for your community. For example, if your community name is Global Toolkit, you might create the hashtag #glotool to pull tweets into your community.
8. Click **Save**.

Once you set up Twitter, users can enable it by going to their **Preferences** > **Twitter Preferences** and clicking **Enable**. To see complete instructions for users to set up Twitter, see *Can I tweet into Jive?*.

Configuring Email

You can configure Jive to send email to users for stream notifications, welcome messages, and so on (customizable email templates are included). Jive can also receive email from users and create content items in Jive (discussions, blog posts, and so on) from the email.

Note: You can set up a connection between Jive and an email server so that content from email is synchronized with and displayed as content in a Jive space. For more information see *Synchronizing Content with Email or Newsgroups*.

Getting Set Up with Email

Here are some things to be aware of when setting up your community's email services.

Setup Task	Description	To learn more, see this help topic:
Configure your outgoing SMTP email server. You can do this manually via the Admin Console or during the setup process via the Setup Tool.	Jive uses an SMTP email server for sending messages such as content update notifications, task reminders, registration confirmations, and so on. You configure a connection to an outgoing email server in the Admin Console.	*Configuring Outgoing (SMTP) Email* and *Using the Setup Tool*
Configure your incoming email server for creating Jive content via email. You can do this manually via the Admin Console or during the setup	You can enable features through which people can post content to the application by sending an email to a particular address.	*Configuring Support for Content Created Via Email (Incoming)* and *Using the Setup Tool*

Setup Task	Description	To learn more, see this help topic:
process via the Setup Tool.		
In test environments, temporarily disable email to and from the application.	Your production instance is typically set up to both send email notifications (SMTP) and access an email account (Email Monitor) or server (Advanced Incoming Email). You'll definitely want to temporarily change these settings in your test production instance; otherwise, you may find that the new test instance generates email notifications that look like they're coming from your production instance. This can be very confusing to end users, and might end up unnecessarily burdening your email servers.	*Disabling Email in Test Environments*
Edit and localize the email templates that your instance will send to users.	Jive includes a set of email templates for emails it sends to users in response to certain events. You can edit the content of the templates, change their locale, or add new templates to use in other locales.	*Editing Email Notification Templates* and *Localizing Email Notification Templates*
Sync content between a space and email.	You can set up a connection between Jive and an email server so that content from email is synchronized with and displayed as content in a Jive space.	*Synchronizing Content with Email or Newsgroups*
Prevent email spam.	There are a few email-related ways to help prevent spam in your community.	*Preventing Spam*

How Incoming and Outgoing Email Works

There are two types of email interaction with Jive:

- Jive will send email to end users
- Jive can receive email from end users

When sending email, Jive uses a multi-part format, where the email contains both a plain text version of the message and an HTML version. If your email client supports HTML rendering, then you'll most likely see the HTML-formatted version in Jive.

If you are using an older email client or an email client on a mobile device with limited rendering capabilities, you may see only the plain text version of the email. This is by design.

When receiving and processing incoming emails, Jive only consumes the plain text portion of the multi-part email.

Why Does My Email Content Look Funny?

There are several different kinds of supported email clients that your community administrator can tie into Jive, such as Microsoft Windows Outlook, Mac Mail, Gmail, and so on. Each of these email clients creates emails in its own unique way. Because of this, you may notice inconsistent results when creating Jive content by email. For this reason, do not use styles or images in email content that you post to Jive.

Generally speaking, the incoming and outgoing email features of Jive were designed to handle simple replies to content and creation of content in Jive.

Jive only creates content from the "plain text" version of an email, which may look significantly different than the "rich text" version of the email you created or can view in your email application.

In addition, Jive will add email attachments as content attachments if the created content item supports attachments (for example, a new discussion supports attachments, but a comment on a document does not).

Therefore, keep your emails simple. Do not use styles or embed images. If you want to do fancy things, it's better to do them in Jive.

Configuring Outgoing (SMTP) Email

Configure the connection to an outgoing email server so the instance can send email messages to users.

Jive uses an SMTP email server for sending messages such as content update notifications, task reminders, registration confirmations, and so on. You configure a connection to an outgoing email server in the Admin Console.

Fastpath: Admin Console: System > Settings > Email Server

The main part of configuring outgoing email settings involves the settings for the *Simple Mail Transfer Protocol (SMTP)* server that outgoing email will use.

- The **mail host** and **server port** should correspond to your email server. You're likely going to have something like smtp.example.com for a host name. If your outgoing email server requires a port number, enter it here.
- Turn on **mail debugging** if you want to have messages from the outgoing server written to the application log. (Note that you should not leave mail debugging on a production instance any longer than necessary to debug a problem.) These can be useful if you suspect there's a problem with outgoing email. For more on viewing logs, see *Getting Application Logs*.
- If your SMTP server requires authentication to send email through it, set the **server username** and **password**.
- If you want to encrypt the connection between the web app node(s) and the SMTP server, select the check boxes to use *Secure Sockets Layer (SSL) or Transport Layer Security (TLS)*.

Set the **server admin email and name** to use a default email address and name for outgoing email. In practice, outgoing emails can appear to have been sent by any one of many people, depending on the reason for the message. For example, when someone posts a message to a discussion thread, the email can appear to have come from them and will be received by anyone receiving notifications for the message.

Jive Software strongly recommends using a **bounce email address**. This will prevent users' automated email replies, such as Out of the Office emails, from posting in your community. In other words, if an outgoing Jive email bounces because its recipient is no longer available, the returning email will be sent to this bounce email address. This is the best way to keep this kind of email from cluttering the inbox of an address that you use for other purposes.

Note: Avoid setting the bounce email address to a domain that is the same as the domain for registering users. The bounce email address will be placed as the return-sender address in the email header for a message sent out from the system for validation. If the email address of the user attempting validation and the bounce email address have the same domain, spam filters may see this as a spoofing attempt and drop the message.

Select the **Set Username in Notification Email From Address**, when you want a person's username to show in the FROM line of a notification email instead of their full name. In other words, if someone posts a discussion reply message, notification messages sent to other people will show the FROM line as, for example, "gladysk" rather than "Gladys Kravitz".

Best Practices for Outgoing Email Setup

Field	Example Value	Description
Server Admin Name	Community System Admin	Typically this is overwritten with the name of the person performing the action. This name is used only when it's a system function sending the email.
Server Admin Email	yourcommunity-no-reply@yourdomain.com	Use an account that doesn't exist so that if a user replies to something from email, they'll get a bounce-reply letting them know that their content did not post in the community.
Bounce Email Address	bounces@yourdomain.com	Use an account that does exist. Check the emails that come into this box and remove or disable bouncing accounts. Note that out-of-office emails would also be sent to this address.

Configuring Incoming Email

Configure the connection to an incoming email server so the instance can receive email messages from users.

You can enable features through which people can post content to the application by sending an email to a particular address.

The application can listen for email in order to support replying to or creating content via email. These are two distinct features and you can enable only one of them.

- The **incoming email monitor** provides support through which users can reply to a discussion by email. It only supports discussion reply posts made by replying to a discussion notification email that a user receives. This feature requires only that you configure the community to retrieve messages sent to a mailbox you specify.
- The **advanced incoming email monitor** provides support for replying to notifications for other content types in addition to discussions. It also supports people creating content and posting it via email. This feature involves more configuration work, including setting up email routing so that the community receives the messages intended for it.

Configuring Basic Incoming Email Monitoring

With incoming email monitoring, you support posting replies to discussions via email. With this feature enabled, the application retrieves email that lands in a mailbox you specify and uses the email's contents to post a discussion reply.

Replies posted via this feature must be emails that are replies to notification email. Although sent as text in email, the reply content will appear in the community as if the recipient had posted it with a web browser. This way, users can post when they're unable to log in to the community but are able to read content through their notifications.

Notification emails sent from the application will include a token in the subject line. The token is needed for the application to correlate the incoming email with its reply thread. Users should take care not to alter the token.

Fastpath: Admin Console: System > Settings > Email Server (Incoming tab)

Here's how it works:

1. Someone posts a discussion message (either a new thread or a reply to an existing one).
2. The community sends email notifications to those people who have requested them.
3. After reading the content of the post in the notification email, someone replies to the notification email with their response (taking care not to delete the token in the subject line).

4. The email is received by the host described in the incoming email monitor settings.
5. Watching for email received at that location, the application locates the discussion thread to which the reply belongs and posts the reply to the community.

Note that this feature supports only discussion replies -- posts of new content and replies to other kinds of content aren't supported. To support those features, use the advanced incoming email feature.

Note: This feature isn't supported when the notification reply is a digitally signed email.

When you configure this feature, start with settings for your incoming email server.

Setting	Description
Client Protocol	Protocol (POP3 or IMAP) that clients use to retrieve email from your mail server.
Mail Server Host	Host name, such as imap.example.com.
Mail Server Port	Port number that clients use to reach your server.
Email Account to Monitor	Specify the email account on the incoming mail server that the application should watch for content. For example, **monitored_account@mail.yourdomain.com**.
Account Username	Email account username.
Account Password (Optional)	Account password if the server requires one from clients.
Use SSL	Select this if the server encrypts the connection between the web nodes and the SMTP server with Secure Sockets Layer.
Mail Folder Name	If the client protocol is IMAP, enter the server-side folder name (if any) that email lands in when it is received.
Delete Unrecognized Email Messages	Select this to remove messages that *aren't* intended for the application.
Inbox Check Frequency	Set this to a value that makes sense for your community. For very active communities (particularly when many people author by email), you might want this to be a lower number so that the application is more responsive with emailed posts.

Select **Enable Incoming Email Monitoring** to turn on the reply-by-email feature for discussions.

Configuring Advanced Incoming Email Monitoring

With the advanced incoming email monitor, you can set up the application to support posting most kinds of content via email. This includes replies to content as well as new content. This feature overrides the incoming email monitoring feature. When you enable advanced incoming email monitoring, incoming email monitoring is unavailable. The advanced feature includes the functionality of the basic feature (although it works differently).

When posting content via email, a person uses one of a number of email addresses that are specifically designed for posting a particular kind of content in a particular place (such as a space or social group).

Here's how it works:

1. Using a browser, a person goes to the place (such as a space, social group, their profile, and so on) to which they might want to post content.
2. The person clicks the **Create by email** link to display a list of the content types in that place that they can post via email.
3. After selecting check boxes for the content types they want, the person downloads vCards representing each of the content types (they can also email the vCards to themselves).
4. In their email application, the person uses the vCards to add the email addresses to their email address book, where they're available when they want to post via email.

5. To post content, the person creates an email with the content they want to post, then sends the email to the address they downloaded as a vCard.

Content types supported by this feature include the following (depending on what your license allows):

For Replies	For Creating New Content
Discussion replies	Discussion threads
Document comments	Documents
Blog post comments	Blog posts
Direct messages	Status message updates
Shares	Announcements
	Project tasks
	Video

Network Requirements

With this feature enabled, the application receives email directly, rather than checking for messages dropped in a particular mailbox. Because of this, configuring this feature requires setting up email routing so that Jive receives emails containing content. Note that this might require your email server administrator to prepare the system.

You'll need to configure email servers and route requests on port 25 to the port on which the application is listening. Here are the details:

1. Configure email servers so that messages with content are sent to the community. Here are two likely configurations:
   - You've deployed Jive to a server where the DNS A record of the server doesn't have a corresponding MX record.

     Example: Your community is deployed to community.example.com. It's unlikely that an MX record exists for the DNS A record community.example.com, so you most likely don't have to add or configure any DNS records. Mail transfer agents will first attempt to look up an MX record for community.example.com; if they don't find one, they'll use the "implicit" or "fallback" A record.
   - You've deployed Jive to a server where the DNS A record of the server does have a corresponding MX record and so you've created a separate DNS A record specifically for this email functionality.

     Example: Your community is deployed to example.com/community. DNS A record for 'example.com' probably already has a corresponding MX record that handles mail for mail for the employees of example.com. To work around this, you'll need to create a separate DNS A record such as 'community.example.com' which points to the same IP address as the server that Jive is deployed on, then (optionally) create an MX record that points to the A record 'community.example.com'. If you don't create an MX record, email transfer agents use the A record as a fallback.
2. Open inbound connections to port 25 on the server where Jive is deployed, then use iptables to forward inbound requests on port 25 to the port you specify in the feature's configuration (by default, port 2500).

   Ports 1024 and below are considered privileged ports on Unix systems. (You're forwarding requests to another port to avoid running the application as root to access the privileged port, which isn't recommended.) The following is a sample `iptables` command to forward requests on port 25 to port 2500:

   ```
   iptables -t nat -I PREROUTING -p tcp --dport 25 -j REDIRECT --to-ports
    2500
   /sbin/iptables-save
   ```

Configuring to Receive Email

After you've set up email routing to ensure that Jive will receive content email, you'll want to configure the application to handle email sent to it. You do that in the Admin Console.

Fastpath: Admin Console: System > Settings > Email Server (Advanced Incoming tab)

Setting	Description
Mail Server Host	Host name, such as example.com. Destination email addresses will take a form specific to the content type, such as status@example.com. This is typically the domain used to reach the community via a web browser.
Mail Server Port	The port on which the application should listen for incoming email.
Valid IPs	IP addresses from which content email should be accepted. Use this setting to limit the locations -- such as relay servers -- from which content is allowed. Leave this blank to accept email from any server.
Email address prefix	Ordinarily, it's a good idea to leave this one blank. The prefix is a value prepended to the reply-to address in the message header (so it isn't ordinarily seen by users); the underlying default value is "jive". You might want to enter your own value here if you have multiple community instances and want to use the prefix to disambiguate among emails sent to them. In that case, each instance would have a different prefix.

Disabling Email in Test Environments

In test environments, disabling email will prevent the test instance from sending email updates to your users.

Your production instance is typically set up to both send email notifications (SMTP) and access an email account (Email Monitor) or server (Advanced Incoming Email). For your test instances, we strongly recommend changing these settings; otherwise, you may find that the new test instance generates email notifications that look like they're coming from your production instance. This can be very confusing to end users, and might end up unnecessarily burdening your email servers.

To make this problem less painful:

- Change all email addresses to a dummy value with:

  ```
  UPDATE jiveuser SET email = 'dummy@localhost';
  ```

- Turn off SMTP by changing the SMTP server name to `nomail`.
- Disconnect or reconfigure the Email Monitor to point to a different mailbox.
- Disconnect or reconfigure the Advanced Incoming Email feature.

Note that if you have customized email templates, they are not overwritten during an upgrade. We recommend testing them after an upgrade to ensure your customizations have been maintained.

Configuring Email Digests

You can customize your digest email settings by editing the following system properties in the Admin Console.

Fastpath: Admin Console: System > Management > System Properties

System Property	Description	Set to this Value
jive.digest.enabled	Turns the weekly digest email feature on or off.	true

System Property	Description	Set to this Value
jive.digest.email.sendDay	The day of the week that weekly digest emails are sent.	5 (Thursday) an integer 1-7, Sunday = 1
jive.digest.email.sendHour	The hour of the day that weekly digest emails are sent.	9
jive.digest.batchSize	The number of weekly digest emails processed at a time.	500
jive.digest.pause	The amount of pause time after a batch of weekly digest emails is processed.	5000 milliseconds

Editing Email Notification Templates

Edit the email notification templates that the application automatically sends to users after certain actions occur, such as content changes and password reset notifications.

Fastpath: Admin Console: System > Settings > Message Templates

Jive includes a set of email templates for emails it sends to users in response to certain events. You can edit the content of the templates, change their locale, or add new templates to use in other locales.

For information about changing template language and locale, see *Localizing Email Templates*.

Caution: While you can edit any of the application's email templates, and we encourage you to edit the header and footer email templates, we otherwise recommend that you limit changes to email templates because such customizations will increase your upgrade burden.

The templates cover a wide range of actions in the application. Some of these are very common, such as email notifications when content is changed or added (for blogs, documents, spaces, and so on) or when someone requests a password reset. Others are sent for actions or events that are more rare. You'll find a complete template list in the Admin Console. You can also customize the header and footer of outbound emails.

Note: You configure other specific aspects of email in other parts of the Admin Console. For example, you set whether moderation email should be sent on the Discussions settings pages.

Email messages sent by Jive can be sent as plain text or HTML. Each template includes a plain text version and an HTML version.

When you're editing templates, use the syntax of *FreeMarker*. Each template supports a specific set of placeholder tokens for email content that will vary from message to message. For example, the notification email sent to users following a document includes tokens for the followed document, the following user, and the URL of the followed document. In the template text, refer to tokens using FreeMarker syntax: ${document}, ${user}, ${docURL}, and so on.

As you edit the template, click the **Preview** button to see your work.

Here are examples designed to tell a user that an item they're following has been updated. This template begins by telling the recipient the name of the user who created or modified the item. It then provides the title of the item ("subject"). The template then checks to see if the system is configured to support other features related to content, and may display one or all of the following messages to the recipient:

- If the system allows commenting on the item by replying to the notification email.
- If the system supports updating the item by sending a new version via email.
- If the system supports creating new content via mail.

Plain Text Template Example

```
${contentAuthorName} <#if contentAuthorURL?
has_content>[${contentAuthorURL}]</#if> <#if isNewContentItem?? &&
 isNewContentItem>created<#else>modified</#if> the document:

"${contentSubject}"

To view the document, visit: ${contentURL}

<#if includePostContentInEmail && !docVerseDocument && !binaryDocument>
--------------------------------------------------------------
${contentTextBody}
--------------------------------------------------------------
</#if>

<#if emailReplyEnabled>
<#if docVerseDocument && docVerseEnabled>
By replying to this email, you can take action on this document.  If you
 attach a new version as a file to the email,
a new version of the document will be created.  The body of the reply, if
 any, will be treated as a comment.
Comment by replying to this email -or- go to the document on
 ${SkinUtils.getCommunityName()}
[${contentURL}]
<#else>
Comment by replying to this email -or- go to the document on
 ${SkinUtils.getCommunityName()}
[${contentURL}]
</#if>
<#elseif hasRespondEntitlement>
Comment by going to ${SkinUtils.getCommunityName()}
[${contentURL}]
</#if>

<#if emailCreateEnabled>
Create a new document in ${containerName} by email
[${newContentAddress}] -or- at ${SkinUtils.getCommunityName()}
[${newContentURL}]
<#elseif hasCreateEntitlement>
Create a new document in ${containerName} at ${SkinUtils.getCommunityName()}
[${newContentURL}]
</#if>
```

HTML Template Example

```
<h3 style="margin: 10px 0 5px; font-size: 17px; font-weight: normal;">
    ${contentSubject}
</h3>
<span style="margin-bottom: 10px;">
    <#if isNewContentItem?? && isNewContentItem>created by<#else>modified
 by</#if> <#if contentAuthorURL?has_content><a href="${contentAuthorURL}">
${contentAuthorName}</a><#else>${contentAuthorName}</#if> in <i>
${containerName}</i> - <a href="${contentURL}">View the full document</a>
</span>
<hr style="margin: 20px 0; border: none; background-color: #dadada; height:
 1px;">

<#if includePostContentInEmail && !docVerseDocument && !binaryDocument>
${contentBody}
</#if>
```

```
<div style="background-color: #f4f4f4; padding: 10px; margin-top: 20px;">
<#if emailReplyEnabled>
<#if docVerseDocument && docVerseEnabled>
    <p style="margin: 0;">By replying to this email, you can take action on
 this document.  If you attach a new version as a file to the email,
    a new version of the document will be created.  The body of the reply,
 if any, will be treated as a comment.</p>
<#else>
 <p style="margin: 0;">Comment by replying to this email
 -or- <a href="${contentURL}">go to the document on
 ${SkinUtils.getCommunityName()}</a></p>
</#if>
<#elseif hasRespondEntitlement>
    <p style="margin: 0;">Comment by <a href="${contentURL}">going to
 ${SkinUtils.getCommunityName()}</a></p>
</#if>

<#if emailCreateEnabled>
 <p style="margin: 0;">Create a new document in ${containerName}
 by <a href="mailto:${newContentAddress}">email</a> -or- at <a
 href="${newContentURL}">${SkinUtils.getCommunityName()}</a></p>
<#elseif hasCreateEntitlement>
 <p style="margin: 0;">Create a new document in ${containerName} at <a
 href="${newContentURL}">${SkinUtils.getCommunityName()}</a></p>
</#if>
</div>
```

Localizing Email Notification Templates

When you create email templates with the locale specified as part of the filename, Jive automatically shows the localized email content when the user's language and country selection match the specified locale. Note that for languages other than English, you may need to provide several versions of the template to cover all cases where the user sets both the language and the locale within Jive. Users who set a locale that doesn't exactly match the locale specified in the filename will see the English template by default.

For example, if you provide only a translated mail_template_fr.xml, only users who set their language to French in their Preferences but don't specify a locale will see the translated information. Users who specify France as the language and also specify either France or another place as the locale will see the English version. To ensure users who specify French as the language and France as the locale see French-language content, create a second copy of the template called mail_template_fr_FR.xml. To also show French to users who specify Belgium as the locale, provide a third template called mail_template_fr_BE.xml.

Troubleshooting Email

Use these techniques to troubleshoot email issues.

If you don't see your particular issue listed here, you may want to check out *this document in the Jive Community*. Note that you must be a registered user to view this document.

Appended Email Content Being Included

You may notice that Jive includes content appended to your email, such as confidentiality notices or signatures. You can set Jive to ignore this content by adding five hyphens or underscores ("-----" or "_____") to the beginning of the appended content template in your email application. Jive excludes anything following five hyphens or underscores.

Automated Reply Emails Causing Stream Pollution

If a user sets up an automated reply, such as an Out of the Office response, in his or her email client, your community may experience a wave of email content generated by these automated replies.

Jive Software strongly recommends using a Bounce Email Address (you set this in the Admin Console under **System** > **Settings** > **Email Server** > **Bounce Email Address**). Automated email replies are sent to the Bounce Email Address. To learn more about this feature, see *Configuring Outgoing (SMTP) Email*.

Email Digest Causing Out of Memory Errors

This can occur when the email manager has an unlimited in-memory queue of email messages. Under normal conditions, the application does not generate enough emails fast enough to encounter this situation. However, in large communities, email can be generated so quickly that creating a digest of all of them can overwhelm the application's email manager. The ideal solution is to make the email manager's queue persistent so that it can handle any number of messages without storing them all in memory. To avoid this problem, you can adjust the `jive.digest.batchSize` system property to include a smaller number of email messages.

Users Not Getting Stream Notifications Via Email

In this case, check the following:

- Have end users correctly configured their email notifications? You might want to send them to this help topic in the end user documentation, *Email or Stream Notifications?*
- Has the user logged into the community in the last 30 days? Users who don't interact with the community directly are assumed to be inactive users--they won't get email notifications. When they log in again, their streams will be repopulated, and their email notifications will resume.
- Does at least one server in the cluster think it is the senior cluster member? The senior member is the node that starts up first in the cluster. To understand how this works, be sure to read the *Clustering Overview*.
- Are emails actually being sent from the instance? To find out, check the destination SMTP server logs by turning on mail debugging on **System** > **Settings** > **Email Server** so that logs are written. For more details, see *Configuring Outgoing (SMTP) Email*.
- Send a test email to see if the SMTP server connection is working and that your outbound emails are not getting marked as spam somewhere upstream (**System** > **Settings** > **Email Server** > **Send Test Email**).

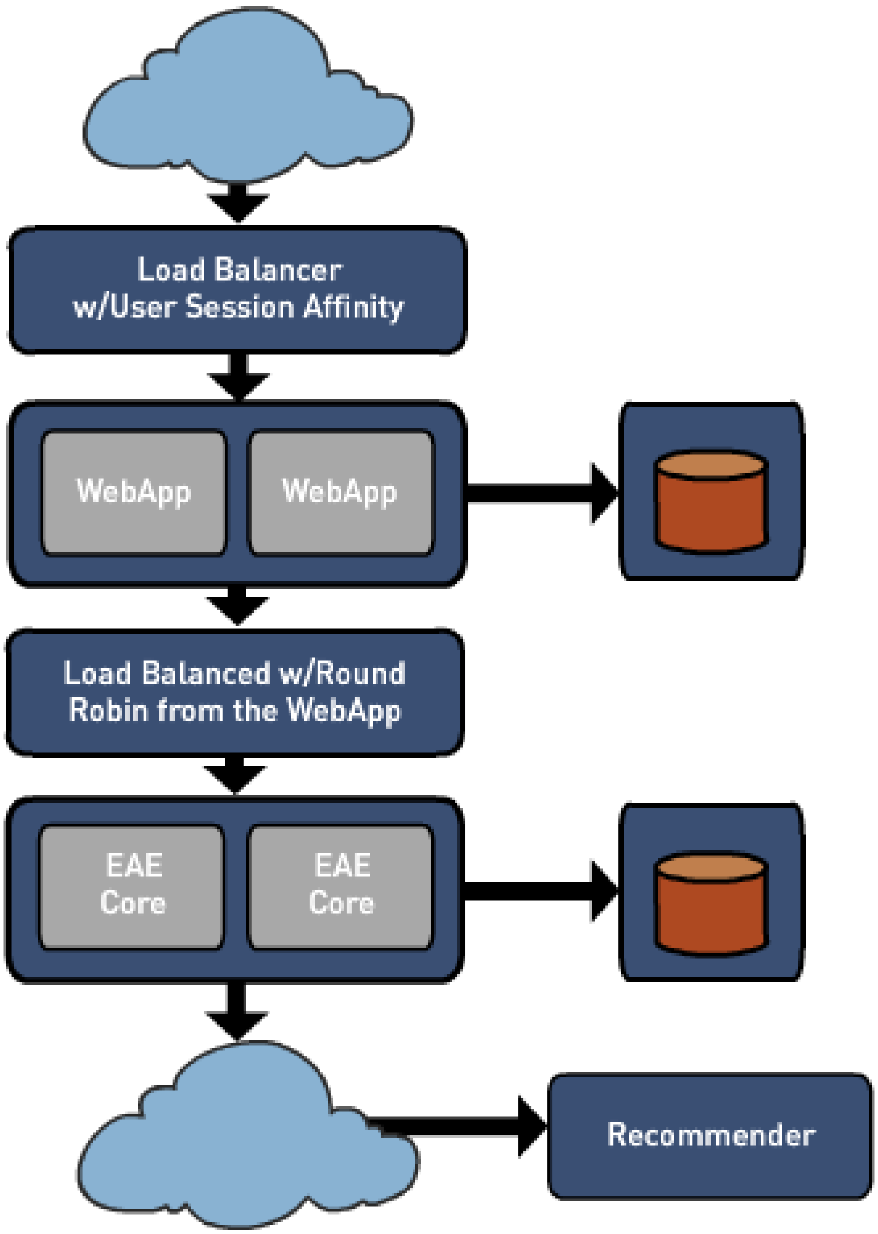
Setting Up the Activity Engine

The Activity Engine powers the What Matters functionality introduced in Jive 5.0, and is an integral part of the Jive Genius feature. This section describes how to configure and troubleshoot the Activity Engine, and provides an overview of the upgrade process from a previous version of Jive to Jive 5.0.

What is the Activity Engine?

The Activity Engine powers the What Matters functionality introduced in the user interface of Jive 5.0. In addition, the Activity Engine facilitates communication between the Jive web application nodes and the Jive Genius SaaS service, which identifies and recommends additional relevant conversations and connections for community users. The Activity Engine is a required component of Jive 5.0 for both on-premise and hosted customers. For on-premise customers, the Activity Engine will be comprised of a node and an associated database in typical configurations.

- For Activity Engine hardware requirements, see *Hardware Requirements*.
- For Activity Engine sizing recommendations, see *Deployment Sizing and Capacity Planning*.



Upgrading and the Activity Engine

Fastpath: Admin Console: System > Management > Activity Upgrade Status

After you have upgraded from a previous version of Jive to 5.0, the Activity Engine automatically runs its own upgrade, synthesizing content to deliver to the What Matters streams. This content synthesis will occur only once.

You can monitor the progress of the Activity Engine upgrade on the **Admin Console: System** > **Management** > **Activity Upgrade Status** page. During the upgrade, you'll see a progress bar showing the progress of the upgrade. After the upgrade is finished and successful, a message will tell you that all activity has been sent to the Activity Engine for processing. Immediately thereafter, your What Matters streams should show active content.

During the Activity Engine upgrade, the progress bar updates every 3-5 seconds. In the rare event that the upgrade hangs (and the progress bar stalls), go to the Logging Management page in the admin console and look at the Log Viewer. Search for error messages containing `com.jivesoftware.community.eae.upgrade`. Fix the problem and restart the upgrade with the `eae-service restart` command. For more troubleshooting tips, see *Troubleshooting the Activity and Communications Streams*.

Configuring the Activity Engine

Fastpath: Admin Console: System > Settings > Activity Engine

To configure the Activity Engine, you will first install the Jive package on the Activity Engine node as described in *Installing the Linux Package*. You can then configure the settings that control Jive's connection to the Activity Engine's core processes on the **Admin Console: System** > **Settings** > **Activity Engine**page.

You can also use this page to troubleshoot when the What Matters streams are not working properly. For troubleshooting tips, see *Troubleshooting the Activity and Communications Stream*.

Properties of the `json` Configuration File

The `core.json` configuration file is located in the service configuration directory specified at runtime, typically `/usr/local/jive/services/eae-service/etc`.

Property	Purpose	Default Value
coreAddress	Address of the Activity Engine server.	localhost
corePort	Port of the Activity Engine server.	7020
coreMinWorkerThreads	Minimum number of threads to listen for incoming socket connections from the Jive web application.	4
coreMaxWorkerThreads	Maximum number of threads to listen for incoming socket connections from the Jive web application.	2048
user-recency-enabled	Controls whether or not only active users will have their streams populated.	true
user-recency-timeout	The age in milliseconds after which a user will be considered inactive.	2592000000 (30 days)
user-recency-buffer	Update user recency time no more than once in this time period in milliseconds.	86400000 (1 day)
user-recency-rebuild-length	When rebuilding streams for an inactive user who has become active, look back no longer than this in milliseconds.	2592000000 (30 days)
remove-old-entries-time-after-midnight	When to allow the tasks that remove old items from the stream to run (after midnight, in milliseconds). For example, a value of 7200000 will allow the tasks after 2 a.m. If you want the tasks to run on a set interval (not just during a time window), set this to 0 and set remove-old-	7200000

Property	Purpose	Default Value
	entries-buffer to 24 hours (in milliseconds = 86400000).	
remove-old-entries-period	The window in milliseconds following remove-old-entries-time-after-midnight in which the old item deletion tasks will run, OR how often to run the tasks in milliseconds if remove-old-entries-buffer is set to 24 hours. For example, the default values will allow the tasks to run once between 2 a.m. and 3 a.m.	3600000
remove-old-entries-buffer	Extra buffer time to allow the old item deletion tasks sufficient time to run. If you want the tasks to run on a set interval (not just during a time window) set this to 24 hours (in milliseconds = 86400000) and set remove-old-entries-time-after-midnight to 0, then set remove-old-entries-period to the desired interval.	600000
log-monitor-directory	The path (absolute or relative to service configuration directory) where performance monitoring logs are saved.	var/monitoring
log-monitor-period	The frequency in milliseconds that samples are written to the monitoring logs.	15000 (15 seconds)
pathToQueues	The path (absolute or relative to service configuration directory) where queue data is saved.	var/data/

Deploying Multiple Activity Engines

As of Jive version 5.0.1, you can deploy multiple Activity Engine cores if a single Activity Engine core will not be enough to handle your volume of traffic. Do this by setting up the new Activity Engine core with the same settings as the first Activity Engine core, and adding the new address to the Activity Engine configuration in the admin console.

Queue Depth Settings

The queue depths displayed on the Activity Engine page of the admin console show the number of items awaiting processing by the Activity Engine node. When an activity is sent to the Activity Engine, the activity is queued and processed as quickly as possible. Each queue, or group of queues, serves a specific purpose:

- Command - Used when specific tasks need to be scheduled and run on the Activity Engine node, such as a user rebuild or Recommender reshred.
- Processing - Activities sent from the application to the Activity Engine will be immediately queued on the processing queue. This will write the activity to the non-user specific streams (All Stream, Profile Stream, Place Stream) and enqueue to the UserStream.
- UserRebuild - When a user rebuild task is running, this queue will fill with activities that need to be processed in order to rebuild the user's stream.
- Upgrade - During the upgrade from a previous Jive version to 5.0, the upgrade queue will fill up with activities that need to be processed so that old content will be displayed in the new stream format.
- UserStream - Activities sent from the application to the Activity Engine will be enqueued on the UserStream queue after being processed by the processing queue. The processing queue builds up all the information necessary to write the activity to individual user streams or communication streams that might be following the content or person on the activity.
- Shredder - If Jive Genius is enabled, this queue will fill up with items as activity comes in and needs to be shredded before being sent to Jive Genius.

- Recommender - If Jive Genius is enabled, this queue will fill up with requests for recommendations bound for Jive Genius.

Expiration Settings

The expiration settings control the number of days an activity remains in a given stream.

Caution: Do not adjust these settings without guidance from Jive Support. Doing so can lead to serious performance problems or data loss.

Troubleshooting the Activity Engine and What Matters Streams

Fastpath: Admin Console: System > Settings > Activity Engine

What Matters Stream(s) Not Working Properly

If a stream is not working properly, it may be due to one of the following. Note that on the **Admin Console: System** > **Settings** > **Activity Engine** page, servers shown in yellow are down.

- The Jive web application node may not be able to connect to the Activity Engine server. Test the connection by clicking **Test Connection**. If this test is successful, the Activity Engine server can properly process activity. If this test fails, you'll see a failure message describing the problem. Typically, test failures are caused by the Activity Engine database being down or unavailable. Note that your instance of Jive may not allow you access to the Activity Engine's core server. You'll need to troubleshoot to bring the Activity Engine back online before running another test.
- The Activity Engine server may not be able to connect to its database. Verify that the Activity Engine database has been created and you can connect to it.
- The Activity Engine server may not be able to connect to the Jive Genius Recommender. Try pinging the Recommender from the Activity Engine.

If you have fixed and verified these connections but continue to experience problems, make sure that all of the configuration settings are correct.

Long Delays Between Post and Stream Publication Times

If there are long delays between post and stream publication times, try sending a trace through the Activity Engine by clicking **Send Connectivity Trace** on the **Admin Console: System** > **Settings** > **Activity Engine** page. This sends a blank activity through the Activity Engine processing pipelines, and then reports the length of time it took to complete the trip. If you send the trace and get back a valid time measurement, the Activity Engine node is up and functioning properly. Typical return times on an idle system would be a few seconds.

Log Files Related to the Activity Engine

For further troubleshooting, look at the error messages in the application logs under **Admin Console: Management** > **Logging Management** > **Log Viewer**, or view the application log directly in `/usr/local/jive/services/eae-service/var/logs` on the Activity Engine node.

- `eae-service.log` -- this is the output of all log statements in the Activity Engine server. Server errors will be logged here.
- `eae-service.out` -- this holds anything written to the standard output stream from the Activity Engine server. Initialization and out-of-memory errors will likely be logged here.
- `eae-service-gc.log` -- analyze this log to determine garbage collection effectiveness and performance.

Understanding the Jive Genius Recommender Service

The Recommender Service, the first in the Jive Genius family of social intelligence products, provides powerful tools for suggesting content, people, and places to your community users. This section describes how the Recommender Service works.

What is the Jive Genius Recommender Service?

The Recommender Service is the first of the Jive Genius family of social intelligence products introduced in Jive 5.0. The Recommender Service is an engine that collects and analyzes user activity in the community to recommend useful content, people, and places to individual users, and reports trending content and people. The Recommender looks at business relationships, user expertise, and areas of interest based on a user's behavior in the community to suggest relevant content that Jive knows a user has not yet seen. The more users interact on the community, the better their results will become in the Recommended for You widget and their Matters Most stream. When you enable the Recommender Service, all of the following features will be present in your community. Note that you cannot choose for some of these features to be visible, but not others.

- Recommended for You widget
- Trending Content widget
- Trending People widget
- A user's Matters Most stream
- Trending and Popular Now recommendations listed in the Jive Genius tab of the Browse menus for Content, People, and Places
- Recommended for You recommendations listed in the Jive Genius tab of the Browse menus for Content, People, and Places
- Your Trending and Popular Content results listed on the Activity tab of a user's profile

The Recommender Service obeys all content permissions and will not recommend content that a user doesn't have permission to view. Therefore, users may not see the same Trending Content or Trending People, depending on their content viewing permissions, when they logged in, and when the last Recommender content poll occurred. Recommended for You and Matters Most are dynamic. Their recommendations change based on a user's shifting interests and affinities. The Recommender will even respond to changes in the org chart.

To understand the architecture of the Recommender Service and its relationship to the Activity Engine introduced in Jive 5.0, refer to the drawing in *What is the Activity Engine?*

Trending Content and Trending People

The Recommender analyzes content and people over a period of time and uses that data to display the Trending People and Trending Content in the system. The Recommender counts the things users do (create content, follow people, join groups, etc.) and, importantly, how users interact with each other's contributions. For example, users liking another user's content, marking answers helpful or correct, and viewing content all count toward the trending status of a user or a piece of content. The Recommender weights the various counts in its equations, and then creates a list of users and content with the highest trending counts over a given time period. Trending People recognizes and rewards users who are a positive influence on the community.

These widgets are updated every 15 minutes and display 10 entries by default. These settings are not configurable.

Trending Content and Trending People are based on global algorithms; they are not user-specific. However, users may not see the same trending people or content based on their viewing permissions. For example, if a user does not have permission to see trending content items 1-10, they will instead see items 11-20 if they have the correct viewing permissions for those items. The Trending People will often be the same for all community users, but it can be different depending on when users logged in and when the last Recommender content poll occurred. In addition, a person may be trending because of something they are doing in a secret group. In that case, you would not be able to see why the person is trending by looking at their recent activity.

Jive Genius Recommender Service Security and Privacy

If you have enabled the Recommender Service (it is enabled by default), your Jive instance will periodically collect information about users' behavior and send it to the service hosted in Jive Software's United States data center. The Recommender Service relies on state-of-the-art security technology, including a multi-stage encryption process that uses a powerful AES-256 encryption algorithm, to ensure your data is secure and private. Your instance locally encrypts your data into tokens using your unique customer key. This key is available only on your instance. Therefore, it is impossible for the Recommender Service to decrypt any of your data. The Recommender Service processes only data from keyword counts, content types, and user and content relationships.

Before any data is submitted to the Recommender Service, all textual data (subject and content) is processed for efficiency and security. First, keywords for the content in your instance are calculated locally and then encrypted with a unique key stored locally and known only to your instance. Then, your local instance collects activity data about how users have interacted with content, people, and places within your community. The activity data and keywords are then further encrypted and transmitted to the Recommender Service over a secure SSL channel.

The Recommender Service determines that multiple people are interested in the same encrypted keyword without knowing the true value of the keyword. The Recommender never processes the actual textual content from your instance; it processes encrypted data. In addition, the data sent to the service cannot be reversed in the Recommender. This allows the Recommender to provide social intelligence about what users find interesting without requiring access to your sensitive business data. Results are then returned to your instance, decrypted locally as necessary, and delivered to your community users.

Recommender Service Encryption Example

Caution: It is your responsibility to secure the specific cryptography used for the encryption. Jive Software will never request that you share with us your cryptographic material.

Here is an example of how the encryption process works. A document with the body "The quick brown fox caught a brown duck" would decompose into a term histogram consisting of:

Term	Count
quick	1
brown	2
fox	1
caught	1
duck	1

Before the histogram is submitted to the Recommender Service, the Activity Engine performs a symmetric encryption of each term for a given activity. Note that not all activity has terms and not all terms are preserved in this process. After encryption and term extraction, the data above would appear similar to this:

Term	Count
f8245fe13f2c4b6ca67008f40e73db44	1
bc02301ef10e49dfaeb54b29524dfbd3	2
c6c93f55cd1844e88aa8b671cd8fa4d3	1
c02d9cc6a07b406d84cc-b1a44b2f60d6	1

In this case, the word "quick" has been encrypted (using AES-256) into the raw binary sequence "f8245fe13f2c4b6ca67008f40e73db44". After encryption, only the Activity Engine that created the encrypted data has the cryptographic material necessary to unencrypt the data. This encrypted token is then hashed using JenkinsHash, which turns "f8245fe13f2c4b6ca67008f40e73db44" into a 64-bit number. At no point does the

Recommender know how to convert the 64-bit number back into "f8245fe13f2c4b6ca67008f40e73db44", nor can it convert "f8245fe13f2c4b6ca67008f40e73db44" back into "quick".

Configuring Jive Genius Recommender Service

Note: The Recommender depends on a successful connection to the Jive-hosted Recommender service that's established during installation. You can find prerequisites and best practices for connecting *here*.

You can enable or disable the Jive Genius feature. You cannot choose to send specific types of activities and not others.

To enable the Jive Genius Recommender Service (it is enabled by default), go to **Admin Console: System** > **Settings** > **Activity Engine** and select **Enabled** in the Enable Recommender Service setting.

For all new users, the Recommended for You widget will display a short notice explaining that Jive Genius is working on creating their recommendations. If you are upgrading from a previous version to Jive 5.0, all existing connections, follows, and other activities of users are processed by the Recommender engine. This allows it to capture previous activity (default is 30 days before the upgrade), which it then uses to make recommendations. Because the Recommender needs to know about the user, it will take a few days before it can provide a valid set of Matters Most stream items and recommendations.

Disabling Jive Genius Recommender Service

The Jive Genius functionality was introduced in Jive 5.0 and is a core feature of the platform. You can enable or disable the Recommender Service. You cannot choose to send specific types of activities and not others. Disabling the Recommender Service may be useful for communities with extreme security concerns, such as government entities, that do not want even encrypted behavioral information sent to and analyzed by Jive Software's Recommender Service. For security information, see *Jive Genius Recommender Service Security and Privacy*.

To disable the Jive Genius Recommender Service go to **Admin Console: System** > **Settings** > **Activity Engine** and select **Disabled** in the Enable Recommender Service setting.

If you disable the Recommender Service, your users will not be able to see the Matters Most stream, the Recommended for You widget, the Jive Genius Browse recommendations, or their Trending and Popular content results on the Activity tab of their profile. They will still be able to see the Trending People and Trending Content widgets, but the results displayed there will be based on a basic popularity algorithm (stored locally) that measures activity over the last seven days. Trending People and Trending Content will not poll or update without a manual browser refresh.

Managing Apps

When you're ready to bring flexibility and customization to your community, just go to the Apps tab in the Admin Console and open the door to Jive Apps. From here you can provide Apps for your community, configure web services for them, make Apps secure by adding a subdomain, or monitor Apps usage.

Note: Jive Apps are delivered via a service that is hosted from a secure data center in the United States.

Setting Up Apps

To set up Apps and enable purchases from the Jive Apps Market, you need to enable Apps, check that your domain security is adequate, and set up any services that need to connect to Jive in order to make enterprise Apps work. You can use your Admin rights to limit which Apps are available to your users.

By default, Apps are enabled when you set up Jive, and your users will be able to install any available Apps they want from the Jive Apps Market. You can choose to *disable Apps* on install or at any time afterward. The following steps provide an overview of the tasks used to set up Apps. Refer to the Help for each Admin page for more help with the settings used during setup.

Note: Apps depend on a successful connection to the Jive-hosted Jive Apps Market that's established during installation. You can find prerequisites and best practices for connecting *here*.

1. Plan your domain security model for Apps. The most secure implementation is to host every App on a unique subdomain: if you use this implementation you'll have to configure your domains accordingly. For more information, see *Creating Secure Subdomains for Apps*.
2. Install Jive. Make sure that your web app nodes can connect to the Apps Market: the *List of Required Ports and Domains* includes the information you need to set up your environment correctly. If you connect to the Internet using a proxy server, you should also read about *how to set up Jive correctly with a proxy server*.
3. Make sure you have enabled the legacy REST services under **System** > **Settings** > **Web Services** > **Legacy Web Services** and the Core API under **System** > **Settings** > **Web Services** > **Core API**.
4. In the admin console, click the Apps tab and view your *Apps Dashboard* to ensure Apps is enabled, the initial connection to the Apps Market was successful, and everything is running successfully.
5. Click the Domain Security link and *choose the security model* you decided on.
6. Check out the Apps Market for your site while you're logged in as an administrator. By default, Apps are enabled and users can install any available Apps from the Jive Apps Market. As an admin, you can decide to disable any Apps that you don't want your community members to use. You may also see some Apps that are Unavailable. When you hover on the **Unavailable** button, you'll sometimes see a link to information about a required connection to a third-party service. If you want to enable one of these Apps, you can use the information provided by the App developer to set up a connection to the service. See *Configuring App Services* for more information.
7. After you complete initial setup, you will do most of your administration in the Apps Market interface. You can continue to use the *Apps Dashboard* to monitor and troubleshoot any problems with your connection to Apps. You can also use the App Statistics page to monitor Apps adoption.

Enabling and Monitoring Apps

Fastpath: Admin Console: Apps > Dashboard

The primary use of the Apps dashboard is to let you enable and disable access to the entire Apps functionality within your community. When you disable Apps with this setting, users cannot see, install, or use any Jive Apps or access the Apps Market. The Apps tab will not be displayed in your community unless you re-enable Apps.

If you're an administrator, you can also enable and disable access to individual Apps. To do this, you'll need to access the Jive Apps Market while logged into the community with your administrator account.

Validating the Apps Market

If your communication with Apps Market is proceeding correctly, you'll see green check marks everywhere on this page, and you should not need to investigate further. If something goes wrong, you'll see error messages that can help you diagnose and fix problems with your Apps Market configuration, by yourself or with the help of Support.

Market Verification Status and **Gateway Verification Status** are checked at initial install to ensure Jive is connected to a secure, verified instance of the Jive Apps Market.

Registration Status and **Gateway Status** provide a health check so you can see whether the Market is currently running and you're correctly connected to it.

Monitoring Communication Between Jive and the Jive Apps Market

You can check on communication between Jive-Apps Market communication using the following areas. This communication should happen automatically according to the schedule identified in your system settings. You can also view and download logs for each of these feeds.

Incoming News Feed from Apps Market	By default, Jive checks in with the Apps Market every 15 minutes to catch up on changes such as updates to Apps

	and administrative actions. If you want to poll right away instead of waiting for the next checkin time (for example, if you are testing a fix to a communication problem), click **Poll Market Now**.
Outgoing Apps Market Notifications	Jive sends any Jive-side changes such as App installations to the Apps Market every 5 minutes. If you want to send this information earlier, click **Notify Market Now**.

Disabling Apps

If you want to disable Apps at any time and make the Apps tab in Jive invisible to users, disable it on the App Dashboard.

When you disable Apps, your users won't have access to any Apps, the Jive Apps Market, or the Apps tab. To disable Apps:

1. In the admin console, **click Apps**.
2. Select **Disabled**.
3. Click **Save Changes**.

Creating Secure Subdomains for Apps

Jive provides three levels of security when you enable Jive Apps in your community. The two more secure options require that you establish one or more subdomains. Subdomains help you isolate Apps from your instance preventing a compromised App from affecting your instance, and in the case of the Most Secure option, a compromised App also won't affect any other Apps.

Fastpath: Admin Console: Apps > Domain Security

Secure	Creates one subdomain for all Apps to share, but keeps Jive in a separate subdomain, providing an extra layer of security for your instance. Select this option and enter the subdomain. For example, type **jiveapps** to use jiveapps.YourCommunity.com as your new subdomain for all Jive Apps to be hosted.
Most Secure	Creates subdomains for Jive and each App. This level of security not only protects your instance, it protects individual Apps from an exploited App. This setup provides the highest level of security. This solution requires each subdomain to have a unique DNS entry. Typically, these entries can be created as wildcards, and can be secured using a wildcard SSL certificate.
Not Secure	Continues without setting up any subdomains. This option is only appropriate for testing environments.

Jive Apps Market Security

The Jive Apps Market is a secure marketplace for purchasing third-party enterprise apps, or apps you develop, within the Jive platform.

Jive Software partners with third-party apps developers to provide enterprise apps to users. The Jive Apps Market makes it simple for you and your users to find, install, and launch apps. As a Jive administrator, you can:

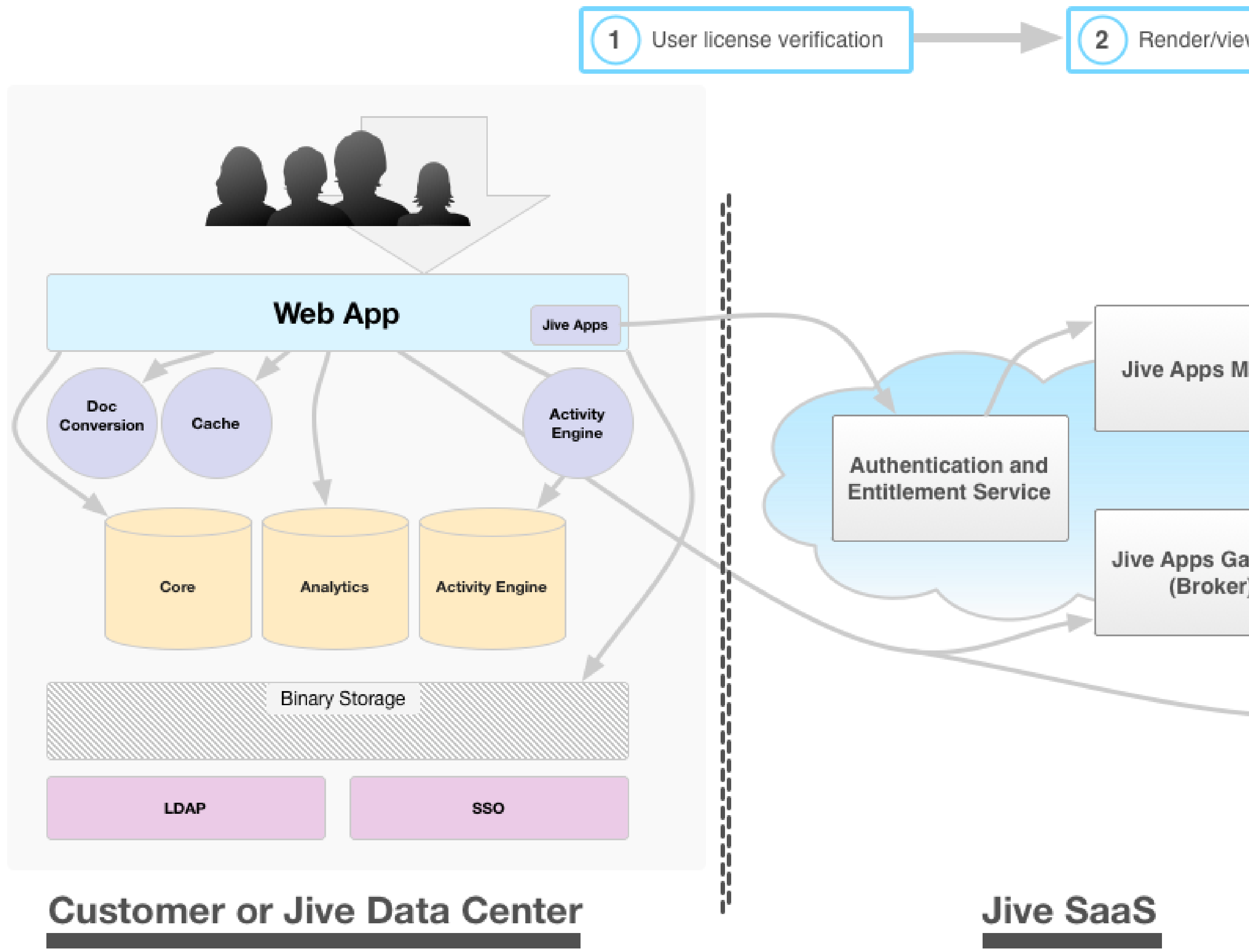
- Buy apps for individual community users or make them available for every community user.
- Develop your own apps for your specific business needs and deploy them in the Apps Market.

- Promote the apps you want your users to use.
- Disable the App Market for all users.
- Disable or enable any specific app in your community.

Caution: The security of an individual App is ultimately the responsibility of the App provider. Apps are offered as-is by Jive Software.

Because third-party Apps are cloud-delivered, users are always accessing the latest version of a given App. Partners can use only our published APIs.

Here's how it works:



Jive Software relies on its own Apps-approval and QA process to approve or deny candidate Apps submitted by Apps partners and developers. Third-party apps available from the Jive Apps Market undergo high-level functional validation.

The security of an individual App is ultimately the responsibility of the App provider. Apps are offered as-is by Jive Software.

Apps Communication and Authentication

All communication between the Jive instance and the Apps Market is authenticated with OAuth. The Apps Market uses a secure gateway proxy service to get information into and out of individual apps without transmitting or storing proprietary data. All credit card information is stored separately from the Apps Market by a PCI-compliant vendor.

Communication from a Jive App to the Jive instance is typically done via HTTPS. Jive Software does not guarantee or require that communication from an app to its home server be over HTTPS. Nor do we mandate or guarantee that the request is signed via OAuth.

An app running inside of Jive can create content and communicate directly with Jive via the JavaScript APIs that Jive Software provides. In this scenario, the user is running the app inside of the Jive instance.

An app’s home server uses the Jive Apps Gateway to post activities (and only activities) to a Jive instance as follows:

1. The app’s home server posts to the Jive Apps Gateway endpoint over HTTPS. This request is signed by the home server using OAuth.
2. The gateway endpoint queues up the incoming request in a database. The entry is not encrypted in the database.
3. The Jive instance polls the Jive Apps Gateway, retrieves the request, and posts it to the activity stream of the Jive instance over HTTPS.
4. The Jive Apps Gateway deletes the request. Note: It is possible for the request to appear in the Jive Apps Gateway log.

Apps Security Checks

Each time a user launches an app from the Apps Market, the Jive instance verifies that user has rights to use the app. The app's definition (app.xml) itself is served from the Jive SaaS infrastructure at runtime.

Data Storage

The Jive Apps Market stores data in Jive Software's data storage center in the United States. The Apps Market does not encrypt Apps, user IDs, and mappings in storage. All credit card and personal identity information for Apps billing is stored outside of Jive with a PCI-compliant provider. Apps data is stored in a database and memecache. Databases are not publicly addressable. Jive stores Apps gadget XML, app IDs, user IDs, and mappings between them for an indefinite period of time. Data is backed up daily.

Data Transmission

All data transmissions in and out of our databases are SSL encrypted, which includes JSON over HTTP for services, JDBC for database, and HTTP. Only app metadata is transmitted. Proprietary data is never transmitted.

Third-party social business applications that integrate with Jive via the Jive Apps Market may use data from the Jive instance in their business logic that allows them to post and work with content and information in the Jive instance. For example, a third-party app could be logically tied to a social group in the Jive instance so that updates to app content are posted in the associated Jive social group. Here are some examples of how that would work:

A project in a project management app.	If someone creates a new project or updates an existing project in the app, the app can post that content change to the Jive social group.
A bug in a bug-tracking app.	If someone creates a bug or updates an existing bug, the app could post that content change to the Jive instance.

An opportunity in a CRM app.	If someone creates an opportunity or updates an existing opportunity, the app could post that content change to the Jive instance.

Data Access

If your Jive community is deployed behind your organization's firewall, only you have access to your Apps data. If your Jive community is hosted by Jive Software, your data will be accessed only as needed to support your instance, and is kept strictly confidential.

Apps Cookies

The Appsmarket App does not use any cookies. However, the following cookies are used by the Dev Console and Admin Console as described:

jamSSO	Cookie maintained between the Dev Center and your Jive community for SSO.
JIVEAPPSMARKETTOKEN	Maintains the user session. This cookie is used by the Dev Center and Admin Console.

Custom Apps Security

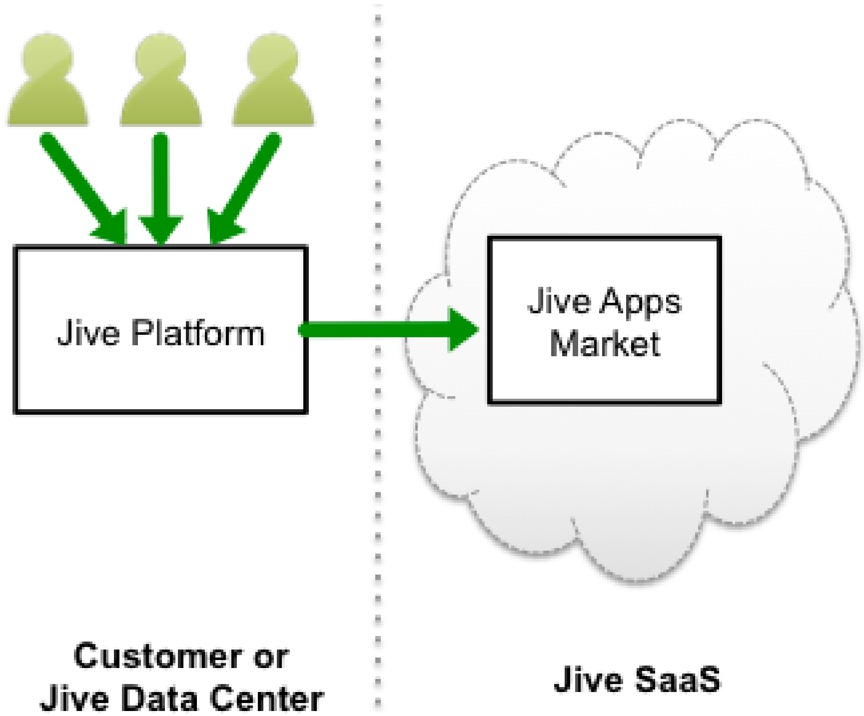
You can develop and deploy your own apps to your community through the Jive Apps Market. Your apps code is not hosted by Jive Software and only you have access to it.

Note: If you want to know how to deploy a custom app in the Apps Market, *learn how to use the Jive Apps Dev Console app here in the Developer community*.

When you create your own app, you deploy it for your users by submitting the apps through the Dev Console app in the Apps Market. This will create a private app listing in your Apps Market. Only listing information is sent to the Apps Market. All of your code and apps data remain behind your firewall and are not transmitted to Jive Software.

Any custom apps you develop and deploy in the Apps Market will appear in the private view of the market. In this way, apps that you develop are visible only to your Jive instance(s) via the Apps Market, and you can remove them at any time. All communication from your Jive instance to the Apps Market flows over HTTPS and is signed by your Jive instance using OAuth. You can publish your custom apps to all of your Jive instances, i.e., UAT and production instances that share a license.

Jive Software is not involved in the approval process for the custom apps that you develop and deploy in the Apps Market. In addition, you are solely responsible for their performance and security.



Configuring App Services

Fastpath: Admin Console: Apps > App Services

Some Apps in the Market rely on remote services in order to deliver functionality. In many cases, such as with cloud-based services, an App developer may be able to supply a known URL for accessing the service through the JiveConnects API. However, in the case of services with unknown URLs such as applications installed in the same environment as the Jive instance, the App developer may not be able to supply this information. In this case, you can use the App Services page in the Admin Console to provide the App with the required service connection information. (If you are looking at the Jive Apps Market and click on the name of an unavailable App that requires this kind of setup, you will see JiveConnects as one of the requirements listed at the bottom of the right pane.)

You can set up a single service connection for an App, or you can provide connections to several possible services which the user may be able to choose from on App installation. For example, you might need users to connect to a different remote service from the App depending on their geographic location.

The information required for setup depends on the service. See the Jive Apps Developer Community for *detailed information about configuring services for some known Apps*. For a helpful setup example, see *here*.

Click **Add New Service** to provide information about a service you plan to connect to. The required fields depend on the authentication type you select. However, at a minimum you need to provide:

- The name of the service. This name will be displayed when a user installs the app (see Apps Market Behavior, below) and is prompted to grant access to personal information, so make sure the name you choose describes the service clearly and appropriately. If users will select from several services, this is especially important. For example, you could name the services after the geographic location of the service if the user must choose from several different installations of the service in different offices. The information about the service
- The tag or tags beginning with `jive:service://` from the app's `gadget.xml` file. This information should be provided by the App developer.
- The URL that the web service will use to send requests to this service provider. This URL will be completed based on path segments specified in the application code.

Optionally, you may want to limit who can access a particular service. Use the **Groups with Access to this Service** setting to specify which Jive groups can connect to a specific App service provider. Users who don't belong to these groups will not be able to install the App.

Apps Market User-Facing Behavior

The information you supply in the App Services page determines the naming of the service(s) displayed during an app installation. When a user starts to install an app that relies on a remote service, one of three things happens:

- If the app only relies on one possible service and it's available, the user is prompted to connect to the service.
- If multiple services are available, the user is prompted to choose a service before connecting.
- If no service is available (because it hasn't been configured in the Admin Console, or because the user doesn't have rights to the service) the user is informed that a required service is unsupported and s/he should contact an administrator. The user won't be able to continue installing the App.

Viewing App Statistics

The Apps Statistics page in the Admin Console provides an overview of which apps are popular and how many people are installing apps. The app adoption rate is calculated by dividing the number of app users with one or more apps installed by the total number of users.

You can click **Download Full App Report** if you want a comma-separated value (.csv) report of how many people have installed each app. You can only see the top ten installed apps in the Admin Console, but downloading this file provides a list of all Apps downloaded.

Fastpath: Admin Console: Apps > App Statistics

Troubleshooting the Apps Market

Problems with the Apps Market can sometimes be diagnosed and fixed easily.

All Apps in the Market display a 502 unavailable error	This problem occurs because the Apps Market, which is hosted by Jive, is temporarily down. Apps will become available as soon as the Market is back online.
Apps in the Market are visible, but many of them unexpectedly have an Unavailable status.	This problem can occur because the Core API is not enabled. In the admin console, go to **System** > **Settings** > **Web Services** > **Core API** and reenable it.
Unexpected changes occur in the Market, such as banned apps being reenabled, or running apps becoming disabled. Or, your apps are not installed after the move.	This problem can occur when the jiveURL for the instance is changed, because by default, changing the jiveURL changes the jiveInstanceID which is what the apps market uses to verify your instance. For example, if you move an instance from UAT to production and change the URL, apps you installed on your test instance will not work in the production instance unless a) Apps Market was enabled at the time of the move, and, b) you selected the "instance was moved" option after restart. If you moved the installation without the Market enabled, or if you chose the "copy" option during the move, and the ID was changed, you need to contact Support to have it reset.
Error: Unauthorized. This Jive instance or user may not have been registered correctly.	This error can occur because of an incorrect instance ID. Try resetting the instance ID by removing the jive.appsmarket.id and then restarting Jive. If that doesn't work, please contact Support for next steps.

Getting Information About Performance

Jive provides tools through which you can keep track of the application's performance and usage. You can even easily connect your community to a web analytics application to get more detailed usage statistics.

To get the very best results from your community, see *Fine-Tuning Performance*.

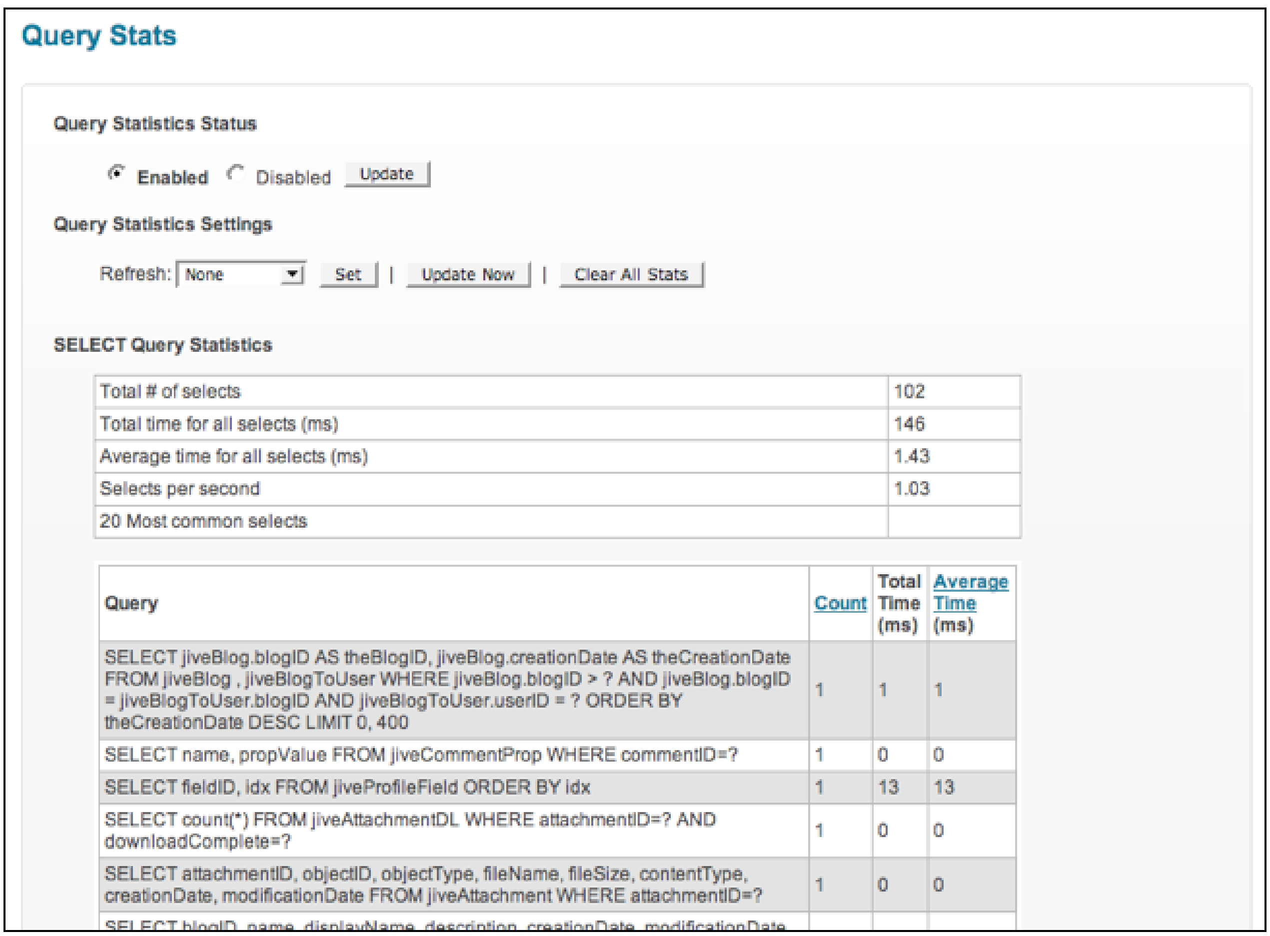
Examining Database Queries

You can view the query expressions Jive uses as it interacts with its database. This is helpful when you're troubleshooting or looking for ways to improve performance. For example, you might use it to look for long-running queries or queries that are running too often.

Fastpath: Admin Console: System > Management > Query Stats

When you turn on this feature, the admin console displays the query expressions executed (without the actual values used), the number of times a query is executed, the time it took in milliseconds to execute a query, and the average time the query took.

Note: Turning this feature on and leaving it on will slow performance. It's best to use this feature only while you're collecting performance information.



Using the Application Logs

Jive logs messages containing application information, warnings, and errors in several different log files. You can view the log files in the admin console for troubleshooting purposes. (You can also log information about database queries, as described in *Examining Database Queries*.) The logs are built using Apache's log4J system. For more information about the log4J API, see *http://logging.apache.org/log4j/1.2/manual.html*. Typically, you would only use the Logging Management pages when working through an issue with a Jive support person.

Fastpath: Admin Console: System > Management > Logging Management

Configuring Logging Settings

On the Configuration tab, you can:

- Set the logging level for the application. This should be set to Error unless you are working through an issue with a Jive support person.
- View and apply overrides to logging levels. For example, if a user is experiencing unexpected behavior in the application, a Jive support person may ask you to adjust the logging levels for troubleshooting purposes.

Using the Log Files

On the Log Viewer page, you can:

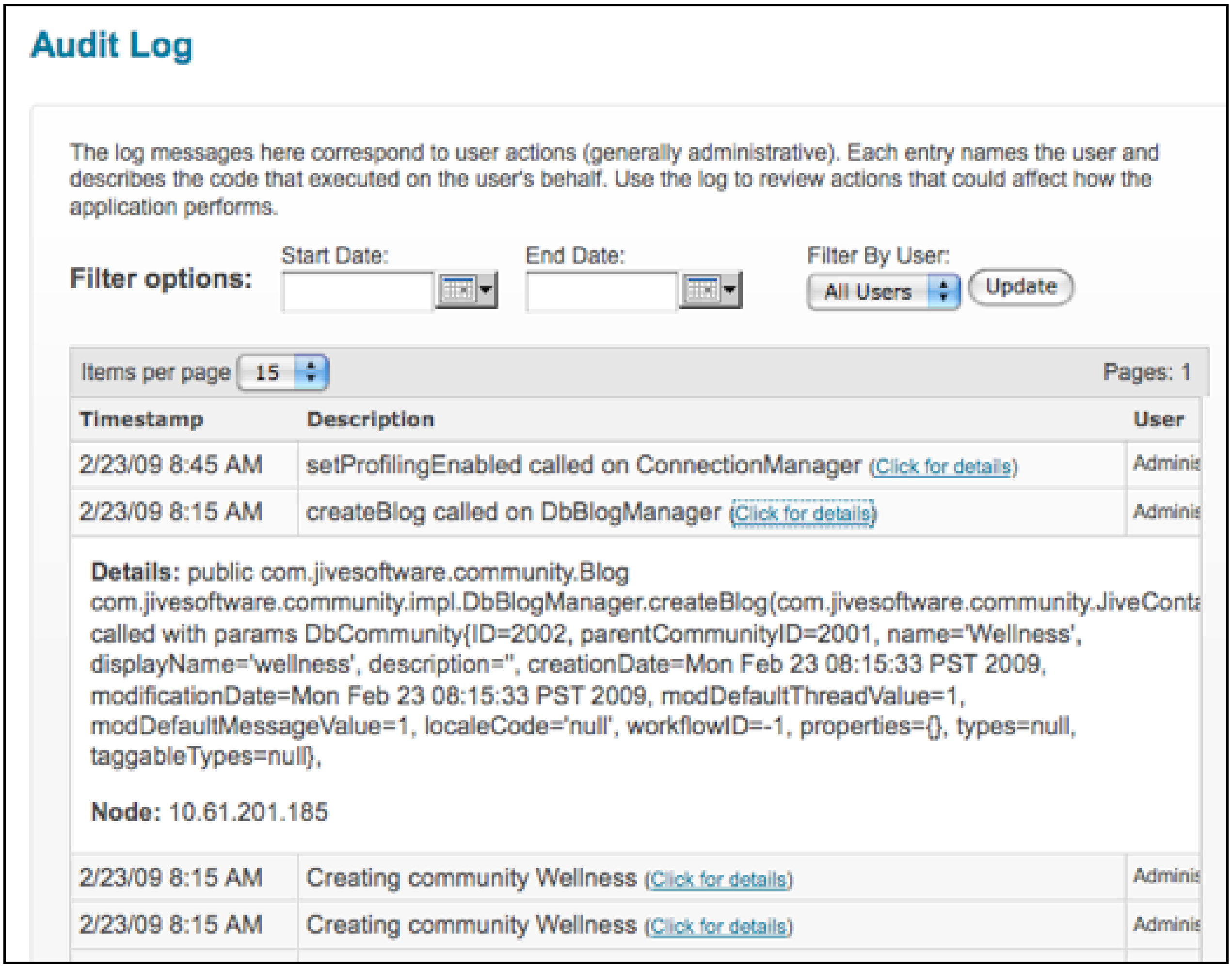
- Insert a mark in a log file. This allows you to mark the problem spot and then monitor what happens after you reproduce the behavior.
- Force a log file roll. This is useful when you're looking for something specific in the log but the file is very long. Forcing a roll restarts the log file at the beginning.
- View the log files.

Log File	Description
[name].log	The main log file where almost all logging is sent.
[name]-session.log	Contains some logging information regarding when users log in and the number of active user sessions.
[name]-profiling.log [name]-latency.log	Some profiling options in Jive log to these files. However, the settings must be enabled, so typically, these files are empty.
[name]-docverse.log	Contains logging related to the document conversion process.
[name]-appmarket-poll.log [name]-appmarket-pull.log	Contains logging information related to communication with the apps market.

Auditing Administrative Tasks

Jive logs actions you and others take through the admin console. You might find these logs useful when you're tracking down the cause of an error or misconfiguration in the system.

Each log entry includes the time the action was taken, the person whose action resulted in the entry, and the part of the application's code that executed to carry out the action.



Fastpath: Admin Console: System > Management > Audit Log Viewer

Viewing System Jobs

The System Jobs page in the admin console provides information for working with the Jive support team to troubleshoot issues. The page lists predefined tasks performed by the system as people are using the community.

Fastpath: Admin Console: System > Management > System Jobs

The jobs are grouped in categories. To view a list of the jobs for a category, select the category value (such as CREATED) in the category dropdown, select the number of items you want to see, then click **Submit Query**.

Tracking Application Usage with Analytics

You can set up Jive to capture data about the actions users take with parts of the application. Over time, this data can be a key piece of business intelligence through which you can better understand how people use the application.

The admin console provides a set of simple reports based on the data you accumulate.

How Analytics Works

As people use the application, it keeps track of the actions users perform such as viewing, creating, and modifying content (documents, blog posts, user profiles, and more). The analytics data is stored according to a data model that's commonly used for other data warehousing and applications. Through this standard model, you can more easily retrieve and analyze data you need.

In addition to this real-time activity collection, there are also batch jobs that run at night, populating the data store with supplemental data. That data includes the names of content and users associated with these activity records. This process of batch loading is known as an *"extract, transform, and load" (ETL)* process.

The final result is a data store (sometimes referred to as a "data mart" or "data warehouse"). To this data store, you can connect other reporting tools to generate visual reports. You can also connect this store to an OLAP product to achieve sophisticated exploration and analysis of the data.

Data Recorded by the Analytics Feature

By enabling the analytics feature on the Reporting page of the admin console, you can record a variety of data about the application and how people use it.

Fastpath: Admin Console: Reporting > Settings > Analytics > Events

The Events list categorizes the data by application feature, then by actions users can take within each of those features. The list includes core application features, but can also include optional features that you might have added separately.

The core features tracked by the analytics feature include:

- Discussions, including threads and messages
- Documents, including comments
- Users, including user registration, relationships, and presence
- Blogs, including blog posts
- Projects, including tasks
- Social groups
- Announcements
- Searches
- Favorites
- Polls
- Tags

For each listed feature, the application can record data for individual user actions, which vary by feature but generally include:

- creating
- modifying
- deleting
- rating
- viewing
- adding
- moving

Setting Up to Record Analytics Data

You set up the feature by configuring a connection to the database you'll be using to store the collected data, specifying whether to purge old data, and selecting activity you want to store data for. Note that only Oracle and PostgreSQL are supported as DBMSes for analytics data.

Important: The pre-packaged PostgreSQL DBMS is for evaluation purposes and should not be used for production instances.

Attention: When you provision the database you'll be using for analytics data:

- Make sure your database supports stored procedures. For example, on PostgreSQL you can use the CREATE LANGUAGE command on your server to register the needed procedural language:

  ```
  CREATE LANGUAGE plpgsql
  ```

- Make sure the database is empty and does not contain a defined schema. The analytics schema will be created automatically after you connect. If you try to manually create the schema first, schema creation will fail.

Fastpath: Reporting > Settings > Analytics

1. Configure connection settings for the analytics database.
   a. In the admin console, go to **Reporting** > **Settings** > **Analytics** and click the **Database** tab.
   b. Under Database Settings, select or enter connection settings for the database you'll be using to store analytics data. Keep in mind that the analytics database user needs to have the same permissions as the user for the application database. For more information, see .

   Table 16: Database Settings

Setting	Description
Database Driver Presets	Select your DBMS (Oracle or PostgreSQL) to automatically populate a JDBC driver class name and database URL template. Be sure to edit the database URL so that you have a valid connection the database.
JDBC Driver Class	This fully-qualified name of the database driver class is entered for you when you select a database driver preset.
Database URL	The URL for connecting to the database is entered for you when you select a preset.
Username	A username that's valid for connecting to the database.
Password	A password that goes with the username.
Min Connections	The minimum number of connections that the application can make to the database.
Maximum Connections	The maximum number of connections that the application can make.
Connection Timeout	The amount of time after which an unused connection will be dropped.

   c. Click **Test Connection** to confirm that the application can connect to the database with the settings you entered.
   d. Click **Save** after you've successfully tested the connection.
2. On the Data Load tab, configure data loading and purging.

   With the analytics feature enabled, the application will automatically extract and transform data from the application database into the analytics database each morning at 2 a.m., system time. At other times, you can begin extraction on this page.

   To control database size, you can have data purged from the analytics database when it has passed a certain age.

   Important: Before you click **Run ETL** to start copying data into the analytics database, be sure (in the next steps) that you're collecting only the data you want.

Setting	Description
Purge Old Activity	Click **Enabled** to have data purged according to the age limit you set.
Older than (months)	Select the highest number of months that each piece of activity data should be stored before it's purged.

Setting	Description
Run ETL Now	Click **Run** to begin copying data to the analytics database.

3. On the Events tab, select the application events you want to keep track of.

   a. In the Captured column, clear check boxes for those actions you don't want as part of your analysis. To start with, it's probably a good idea to collect as much as you can. You can always stop collecting certain items later.

   b. To enable analytics and start copying data, under Analytics Settings, click **Enabled**.

Viewing Reports from Analytics Data

If your community is set up to record usage data through the analytics feature, you can view graphical reports of the data collected in the admin console. You can also export the data to comma-separated values (CSV) files for use in a spreadsheet application, where you can create your own graphs.

Fastpath: Admin Console: Reporting > Dashboard

Viewing Graphical Reports from Analytics Data

On the Reporting Dashboard page of the admin console, you can view a few basic charts and tables that capture information collected by the analytics feature. The charts represent data that you might find useful for evaluating the health and vitality of your community. The reports are grouped into **system summary** and **activity** sections.

System Sumary

Under **System Summary**, you'll see charts that capture data about accounts and content created in the community.

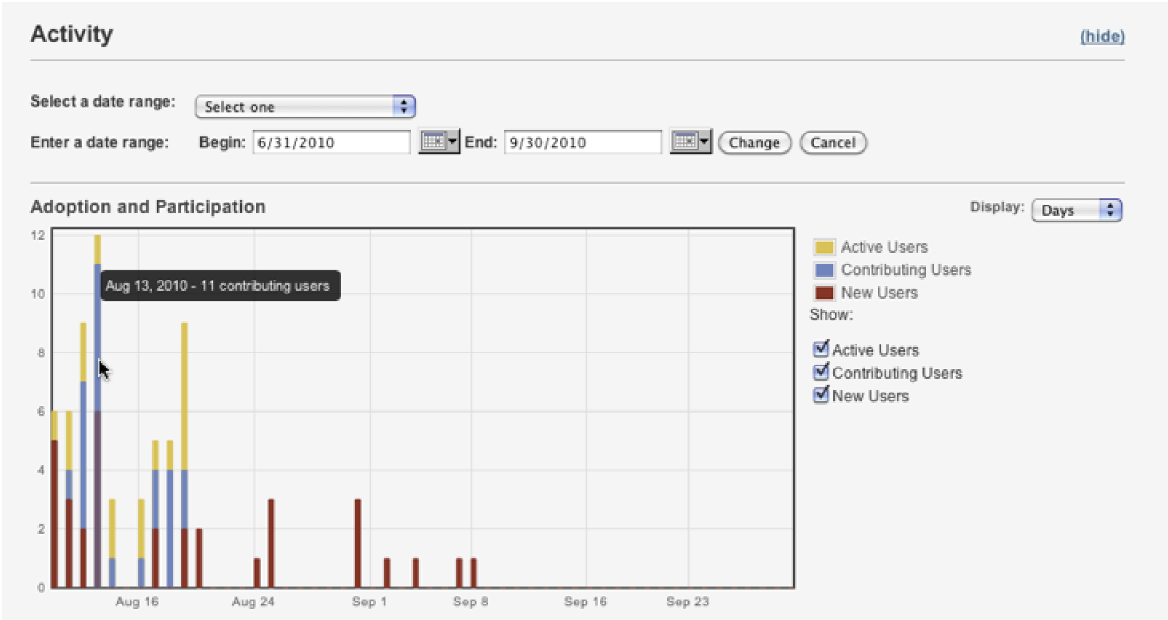
- **Cumulative account creation** illustrates how the total number of user accounts was reached. You can see how many accounts were added daily, weekly, monthly, or yearly.
- **Cumulative content creation** illustrates how the total amount of the community's content was reached. Select or clear check boxes for content types to filter the list to the content types you want to see data about. You can see how many accounts were added daily, weekly, monthly, or yearly.

Activity

Under **Activity**, you can view a chart and tables that capture community activity over a date range you specify. You can select a date range from the dropdown or enter your own.

- The **Adoption and Participation** chart is a snapshot of user activity in the community. You can filter data in the chart to show, in a given period (daily, weekly, monthly, or yearly), how many users joined, how many users were active (logged in), and how many contributed in some way (posted content, for example).
- The **Top Communities** table lists spaces in descending order of activity. In other words, spaces at the top of the list have more activity from users creating and reading content, for example. You can click the name of each space to go directly to that space.
- The **Top Content** table lists content in descending order of involvement by users in the community. The list is divided by content type, with discussion threads grouped separately from blog posts and documents and so on. Within each of these groups, content with the most activity (being read more or having more users involved with it) is shown at the top. You can click the name of each piece of content to go directly to that content.
- The **Top Social Groups** table is similar to the top communities table, but lists social groups in descending order of activity. You can click the name of a social group to go directly to that group.

Note: To get information about data behind elements in any chart on the page, hover your mouse pointer over an element in the chart. As shown in the following illustration, you'll get a popup that displays what the element represents.



Exporting Analytics Data

You can export data collected by the analytics feature using predefined export templates available through the admin console. Reports are exported as CSV files you can open with other software, such as a spreadsheet program, where you can manipulate the data into charts of your own.

To export a report, under **Data Exports** click the link for the report you want. Reports you can export include the following:

Members

With a members report, you can export either member profile data or data about member activity. When you choose to export the report, you'll be prompted to choose which one you want.

A **profile data** report includes information from user profiles, organized into the following columns:

- Member_ID
- User_Name
- User_Full_Name
- Creation_Date
- Email
- Title
- Department
- Address
- Phone Number
- Home Phone Number
- Mobile Phone Number
- Pager Number
- Fax Number
- URL
- Hire Date
- Biography
- Expertise
- Alternate Email
- Home Address

- office addres

An **activity data** report lists the count of times a user viewed or created content. It's a measure of how active the user has been during the date range you specify. You can have the exported data aggregated by days or months. The report includes the following columns:

- Member_ID
- User_Name
- Activity_Date
- View_Count
- Create_Count

Content creation

The content creation report describes how much content was created on each date, and where in the community the content was created. The report includes the following columns:

- Creation_Date
- Content_Type
- Container_Name
- Create_Count

Adoption and participation

The **adoption and participation** report describes, for each container (space, project, social group), how many users have been active or created content. The report includes the following columns:

- Activity_Date/Month
- Active_Member_Count
- Content_Creator_Count
- Container_Name

Space activity

The **space activity** report shows, for each space, counts of content created or viewed as well as active members. The report includes the following columns.

- Space_Name
- Create_Count
- View_Count
- Active_Member_Count

Group activity

The **group activity** report gives activity counts for social groups. For each group, it lists counts of content created and viewed, users who joined or left the group, as well as of active group members. The following columns are included:

- Group_Name
- Create_Count
- View_Count
- Join_Count
- Leave_Count
- Active_Member_Count

Individual container detail

With the **individual container detail** report, you can export data about the space, a project, or group that you specify by name. For the container you specify, and for a particular month in your date range, the report gives content view and creation counts by user. For all of these kinds of places, you'll get the following columns:

- Container_Name
- Activity_Month
- Member_ID
- View_Count
- Create_Count

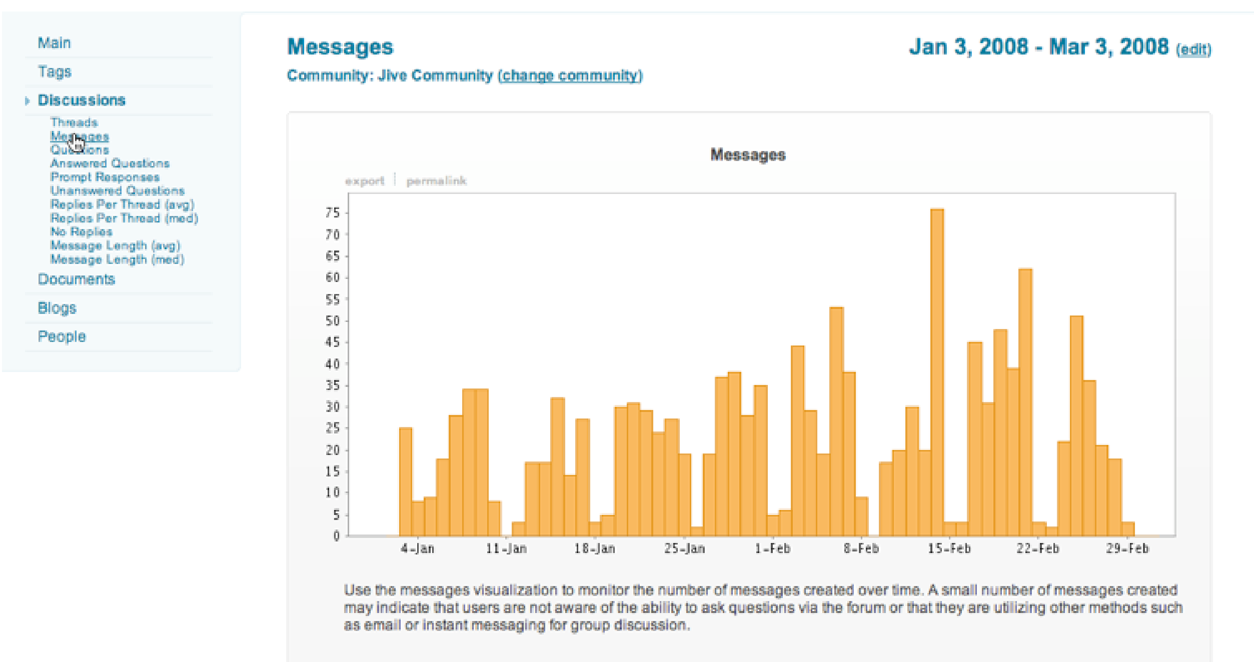
Content

The **content** report lists detail about each piece of content of the type you specify. The report includes the following columns:

- Content_Name
- Author_ID
- Author_User_Name
- Container_Name
- Content_Type
- View_Count
- Unique_Viewer_Count

Tracking Usage Graphically

Jive provides charts that illustrates how people are using the application. You can check these reports periodically to get a high-level view of how content is being used, such as whether discussion posts are replied to, questions answered, and so on.



Fastpath: Admin Console: Reporting > Reports

Integrating Web Analytics

You can connect your community with a third-party web analytics application such as Google Analytics or WebTrends.

Fastpath: Admin Console: Reporting > Settings > Third-Party Integration

In the admin console, go to **Reporting** > **Settings** > **Third-Party Integration**and enable third-party integration. Then, paste the third-party provider's script into the text box and click **Save Settings**. The script will be automatically inserted by the application at the bottom of its pages. The script isn't typically displayed to users, nor are the analytics results displayed in the admin console (you'll get them from your analytics provider).

Here are two examples of third-party scripts that you might enter into the third-party script text box:

```
<script src="www.google-analytics.com—urchin.js <http://www.google-
analytics.com/urchin.js>"
    type="text/javascript">
</script>
```

or

```
<script type="text/javascript">
    _uacct = "AB-123456-1"; urchinTracker();
</script>
```

Connecting Communities with Bridges

You can connect Jive communities with a bridge. Over this bridge, people can see activity taking place in a community that's separate from the one they're currently using. For each user, visibility into another community will rely on their having a user account in both communities. Bridged communities use Web services to communicate with one another.

Note: This is an optional feature available as a module. For more about modules, see *Adding Features with Modules*.

One Way or Two?

Administrators from communities at both ends of a bridge decide whether the bridge should support content visibility one way or both. An administrator managing or configuring an internal community (one designed to serve a closed audience, such as a company's employees) might see value in requesting a bridge to an external community (such as a support site for the company). Content from the external community visible to employees internally could offer an easy way for employees to see external content from customers. But going the other way--internal content visible to external community members--is often not as valuable.

When setting up a bridge, administrators from both ends will make a decision about whether, and how much, content should be visible from their own community to the other. Bridge settings at both ends provide the ability to enable or disable these features.

Bridged Features

With bridged communities, users of the local community can:

- See a list of the bridged communities.
- Log in to a bridged community from the local community.
- Add widgets that present information about activity in the bridged community.
- Receive results from the bridged community as part of their searches.

Setting Up a Bridge

A community uses web services to retrieve information from other bridged communities, presenting much of the same information in the local community that people can get by going to the bridged community directly.

Fastpath: Admin Console: System > Settings > Bridges

When you set up the bridge, you're not just making the connection possible. You're also setting how people who are using the community will see the connected community. So as you set up the bridge, when entering values to help identify the bridged community, be sure to enter values that make sense from a user's perspective. When you add a bridge in one community, you're sending a request to the other community that an administrator there will need to approve.

To create a bridge from the current Jive community to another:

1. Ensure that bridges web services are enabled for registered users on the community you're connecting to. For more information, see *Setting Access for Web Service Clients*.
2. In the admin console, go to **System** > **Settings** > **Bridges** and click **Add bridge**.
3. In the **Bridge URL** box, enter the URL for the community you're bridging to. This should be the community's root URL, which points to the community's home page.
4. For login credentials, enter the username and password that should be used to connect to the bridged community. These credentials should correspond to a valid user account on the community you're bridging to, and are used only to make the request. When the connection is approved, a shared user account is created and used for authenticating between instances.
5. Click **Lookup**. The local community will attempt to connect to the instance you're bridging to. After it succeeds, you'll be prompted to finish configuring.
6. In the **Bridge name** box, enter the name that users should see when they are browsing content retrieved from the bridged community. If the bridged community's name is a long one, it's a good idea to use a short version of it here.
7. For **Bridge elements**, select the features that should be available across bridged communities.
8. If you have an icon that represents the bridged community, browse for its image file. For example, you might want to use the bridged community's *favicon*.
9. When you're finished, click **Save**.

An administrator from the bridged community must approve the bridge request using that community's admin console. To review the bridge request:

1. In the admin console, go to **System** > **Settings** > **Bridges** and locate the pending bridge request.
2. When reviewing the bridge request, you can:
   - Approve the bridge request by clicking **Approve** in the corner of the bridge's settings box.
   - Reject the request by clicking **Reject**.
   - View information about the requesting community (such as its URL) and select features that should be served (that is, reciprocated) to the requesting community by clicking **View/edit details**.

Note: If you have trouble searching across the bridge, double-check the OpenSearch engine associated with it. In the admin console, you can do a test search using OpenSearch engines.

Disabling or Deleting a Bridge

You can disable or delete a bridge so that the bridged community's content is no longer visible in the current community. Disable or delete the bridge on the Bridges page of the admin console.

Fastpath: Admin Console: System > Settings > Bridges

To disable or delete a bridge:

1. In the admin console, go to **System** > **Settings** > **Bridges** and locate the bridge you want to disable or delete.
2. In the corner of the bridge's settings box, click **Disable**.
3. To delete the bridge, after you've disabled it, click **Delete this bridge**.

Managing Customizations

Enhance the application's features with plugins, themes, and other extensions.

Adding and Editing Themes

With themes, you can customize the way Jive looks, adding your own logo and brand information. You can also change the composition of pages, rearrange them, and add and remove features.

Fastpath: Admin Console: System > Settings > Themes

- For simple changes to the UI, such as colors and logo, see *Making Simple UI Changes*.
- To add sophisticated view logic in your header and footer, see *Customizing the UI with the Theme Resource Kit*.
- To use a custom FreeMarker or Soy Template, upload it by going to **Admin Console: System** > **Settings** > **Themes** and clicking **Browse**. Select your theme(s) zip file and upload it (the zip must contain theme.xml which specifies the theme name). Next, assign a theme for the entire site (Global Theme Map). You can stop there or continue to assign themes for different URLs in the community (Custom Theme Maps). This enables a single Jive instance to display multiple skins throughout the application. You can edit themes at any time and apply theme maps without a server restart.

Note: You can also export an uploaded theme to a zip file by clicking its blue down arrow under the Actions list.

Substituting Phrases in the UI

You can give other names to things users see in the user interface. For example, you can rename "Documents" and "Discussions" to "Articles" and "Conversations." Using the admin console, you can make the substitutions in a simple way for the most common terms.

Note: Keep in mind that because your phrase substitutions are part of your theme, they will be overridden if you change your site's theme. When you upgrade, they will be overwritten and you'll have to recreate them.

Fastpath: Admin Console: System > Settings > Phrase Substitutions

Note: This topic describes how to make simple phrase substitutions. For more advanced use of the feature, including more about themes, see the *developer documentation*.

How It Works

All of your substitutions are made at run time. That is, the application keeps track of what word or phrase you want displayed, then inserts your phrase for the default phrase when someone views a page that includes the phrase. The default phrases themselves come from internationalization (i18n) properties files used for localization. Also, your substitutions are associated with a theme. That means that you can make your substitutions globally or by mapping the change to a particular part of the user interface.

Behind the scenes, your substitutions are remembered as "substitution rules" that use regular expressions. The rules give you a way to fine tune the substitutions to meet your needs.

Making Simple Substitutions

You can substitute common phrases that are predefined. The simple substitution mechanism is designed to account for upper- and lower-case versions of the phrases. However, there are some aspects of the change it doesn't account for, for example, a change to an article that would precede the word. Substituting "article" for "document" would leave awkward constructions in English, such as "Create a article or upload a file" (where you'd want "Create *an* article or upload a file"). If you're curious about the outcome of the change you're making, click View Rules to see the rules page, where you can get a preview (you'll need to save your changes first).

Note: You should always test your changes on an instance of the application that people aren't currently using. That way, you can work things out before the changes impact the work of users.

To define simple rules:

1. In the admin console go to the Phrase Substitutions page. There you can choose the theme that the substitution should be a part of and a locale in which the substitution should occur. Beneath these selections you'll see a list of the phrases you can make substitutions for.
2. If the phrase you want to change is listed on the far left side, enter your alternatives for singular and plural versions of the phrase.
3. Click **Save** to make the substitution (you don't need to restart the application or server for the change to take affect).
4. After you save the rule, you can View Rules to go to the Phrase Substitutions page and see what's going on behind the scenes by viewing the details of the substitution rule you're creating.

You won't see the substitution in effect until you assign the theme you select to a part of the user interface. One easy way to verify your work is to assign the theme to the UI application-wide.

Use the following steps to assign the theme to the end user UI globally:

1. On the Phrase Substitutions page, note the name of the theme you've selected. By default, this is "custom".
2. In the admin console, go to **System** > **Settings** > **Themes**.
3. Under Global Theme Map, select your theme (such as "custom") from the dropdown, then click **Set Global Theme**.

After your theme is applied as the global theme, you can continue making and testing changes to your phrase subsitutions.

Adding and Removing Plugins

If your community has any plugins installed, you can view a list of them on the admin console's Installed Plugins page (**Admin Console: System** > **Plugins** > **Installed Plugins**). If you don't have any yet, Jive Software offers a few to get you started. The Add Plugin page lists plugins that are available free from Jive Software. It also provides a place to add plugins for which you have a JAR file.

Fastpath: Admin Console: System > Plugins > Installed Plugins

Fastpath: Admin Console: System > Plugins > Add Plugin

Whenever you add or remove a plugin, you'll need to restart the application server.

Note: In previous versions you could deploy a plugin by copying its JAR file to your plugins directory. That's not supported in this version.

Adding and Removing Widgets

Jive includes widgets users can customize pages with. As an administrator, you can control which widgets are available to users.

Fastpath: Admin Console: System > Settings > Widgets

You can delete widgets by clicking the **Remove** button. For a list of the widgets included with the application, along with descriptions, see *Designing Pages with Widgets*.

You can also add new widgets. At the bottom of the page, under Add a new widget, enter the fully-qualified class name of the class for the widget you're adding, then click **Add Widget**. The JAR containing the widget you're adding must be on the application's classpath.

Configuring OpenSocial Gadget Support

You can configure the application to include gadgets that people can use when customizing home and overview pages. OpenSocial gadgets are mini applications written using the *OpenSocial* API, which is used by many social web applications. Like widgets, gadgets provide a way to embed functionality -- newsfeeds, games, maps, and so on -- in web pages. You can add any gadget developed using the OpenSocial API, which means that gadgets can come from anywhere. You'll find a *directory of gadgets* at the Google web site.

Important: OpenSocial gadget integration is a beta feature. Commercial gadgets are not currently supported. Please proceed with caution, verifying that any gadget you create or install follows the OpenSocial API only.

You enable people to use gadgets by adding the gadgets, then selecting the application contexts in which they will be available for people. For example, after you add a gadget you can specify that it should be available on users' personalized homepage and social group overviews, but not on the main application homepage, space overviews, project overviews, or overviews displayed by custom containers you might have added to the application.

Note: Gadgets can refer to resources such as images and other page from within their code. Depending on how the reference is made by the code and on the browser's security settings, this can cause Internet Explorer (version 6) to display warning messages. The message will warn of "both secure and nonsecure content" on the page.

Adding an OpenSocial Gadget

You add a gadget using the OpenSocial Gadgets page in the admin console. When you add a gadget, the application retrieves the XML file at the other end of the URL you specify. The application interprets the XML and renders it for display in the user's browser.

Note: The gadget URL must be 250 characters or less.

Fastpath: Admin Console: System > Settings > OpenSocial Gadgets

1. In the admin console, on the **OpenSocial Gadgets** page, under **Enter the URL of a gadget to add it**, enter the URL to the gadget XML file, then click **Add Gadget**.
2. Next to the gadget you added, select check boxes for the application contexts in which the gadget should be available and clear check boxes for contexts in which it shouldn't.

Working with Feeds

Like many Web sites and applications, the Jive application provides the ability for users to subscribe to a content digest by using a feed. By subscribing to a feed and using a *feed reader (also known as an aggregator)*, users can discover what has changed in the application without having to visit the application. Feeds provide data about content in a format that a feed reader can use.

Enabling Feeds

Feeds are enabled by default. However, in the internal communities version, basic authentication is required by default. Using the admin console, you can turn feeds on or off, specify which format should be available, and whether users (via their feed readers) should be required to send a username and password with feed requests (using basic authentication).

Fastpath: Admin Console: System > Settings > Feeds

Note: For users to use the links available in feeds, you'll need to be sure you've set the jiveURL property. This tells the application the public Web path to your installation. This is necessary to support links to it from content listed in the feed reader. You typically set the jiveURL when you're setting up. After setting up, you can set or change the URL in the admin console by setting the jiveURL system property at System > Management > System Properties.

Feeds Available

Jive offers feeds in three formats: *RSS (Really Simple Syndication)*, *Atom*, and *JSON (Javascript Object Notation)*. Each of these carries the feed data in a different way. You can retrieve feed results by using the URLs listed here.

Where noted, these URLs support the following variable parts:

- tag_name — The tag that's been applied to the blog post. In the user interface, tags are listed at the bottom of the post.
- user_name — The user's login name.
- communityid — You can find this number at the end of the URL after you click View Feeds in the All Content page. In the admin console, the ID number is shown at Space/Communities > Settings > Space Settings.
- document_id — A unique identifier for a document. You'll find the ID at the end of the URL when you're viewing a document in the application.
- post_id — A unique identifier for a blog post.
- blog_name – A blog's name. For a user blog, this is typically the user's name.
- search_string — For feeds based on searches, this is the URL search parameter created when the user searches. Here's an example with the typical full set of search parameters included. In this case, the search term is "macro".

  ```
  q=macro&resultTypes=BLOG_POST&resultTypes=DOCUMENT&resultTypes=MESSAGE&resultTypes=CO
   &peopleEnabled=true&dateRange=all&communityID=2000&numResults=15&rankBy=10001
  ```

  The example search string includes the following parameters:

  - resultTypes — The kinds of content to search.
  - peopleEnabled — Whether to search people's profiles.
  - dateRange — When the content was added. Acceptable values are: yesterday, last7days, last30days, last90days, thisyear, and lastyear.
  - communityID — The ID number for the space.
  - numResults — The number of results to display.
  - rankBy — How results should be sorted. Acceptable values are: rating, relevance, subject, likes and date. For example, you'd specify rankBy=rating

You can also include the following parameters in your feed URL:

- full — Whether to include the full content in the results. Include full=false as a parameter when you want to return just a summary in feed results.
- numItems — The number of results to return. For example, you could include numItems=25 to return 25 results. The default is 10.

In addition, if your community requires basic authentication (a username and password), you might need to prepend the feed URL with the username and password parameters. Here's an example:

```
https://<username>:<password>@<domain>/community/feeds/documents
```

If you don't want to enable basic authentication but still need to send a username and password, you can use the following form (note that this is less secure):

```
https://<domain>/community/feeds/documents?
username=<username>&password=<password>
```

Feeds System Wide

Feed Subject	URL Syntax
All content	https://<domain>/community/feeds/allcontent
Documents	https://<domain>/community/feeds/documents
Discussion messages	https://<domain>/community/feeds/messages
Discussion threads	https://<domain>/community/feeds/threads
Popular discussion threads	https://<domain>/community/feeds/popularthreads
Unanswered threads	https://<domain>/community/feeds/unansweredthreads
Recent blog posts	https://<domain>/blogs/feeds/posts
New blogs	https://<domain>/blogs/feeds/blogs
Blog tags	https://<domain>/blogs/feeds/tags/<tag_name>
Recent blog comments	https://<domain>/blogs/feeds/comments
Blog author	https://<domain>/blogs/feeds/users/<user_name>
Tags	https://<domain>/community/feeds/tags/<tag_name>
Search	https://<domain>/community/feeds/search?<search_string>
Announcements	https://<domain>/community/feeds/announcements
Polls	https://<domain>/community/feeds/polls
Statistics	https://<domain>/community/feeds/stats

Feeds Per Space

Feed URLs for a particular space are similar to the system-wide feed URLs. The difference is the space-specific feed URLs are appended with the community ID number. In the admin console, the ID number is shown on **Admin Console: Space** > **Settings** > **Space Settings**.

Feed Subject	URL Syntax
All content	https://<domain>/community/feeds/allcontent?communityid=<community_id>
Documents	https://<domain>/community/feeds/documents?communityid=<community_id>
Discussion messages	https://<domain>/community/feeds/messages?communityid=<community_id>
Discussion threads	https://<domain>/community/feeds/threads?communityid=<community_id>
Popular discussion threads	https://<domain>/community/feeds/popularthreads?communityid=<community_id>
Unanswered threads	https://<domain>/community/feeds/unansweredthreads?communityid=<community_id>

Feed Subject	URL Syntax
Recent blog posts	https://<domain>/blogs/feeds/posts?communityid=<community_id>
Tag	https://<domain>/community/feeds/tags/<tag_name>?communityid=<community_id>
Announcements	https://<domain>/community/feeds/announcements?communityid=<community_id>
Polls	https://<domain>/community/feeds/polls?communityid=<community_id>
Statistics	https://<domain>/community/feeds/stats?communityid=<community_id>

Feeds Per Blog

Feed Subject	URL Syntax
Recent posts	https://<domain>/blogs/<blog_name>/feeds/posts
Blog tags	https://<domain>/blogs/feeds/tags/<tag_name>
Recent comments	https://<domain>/blogs/<blog_name>/feeds/comments
Comments on a post	https://<domain>/blogs/<blog_name>/feeds/comments?blogPost=<post_id>

Feeds Per Document

Feed URLs for documents include the document ID. You'll find the ID at the end of the URL when you're viewing a Jive document.

Feed Subject	URL Syntax
Comments	https://<domain>/community/feeds/document-comments/<document_id>
Version history	https://<domain>/community/feeds/document-history/<document_id>

Feeds Per Person

Feed Subject	URL Syntax
Discussion messages	https://<domain>/community/feeds/messages?rssUsername=<user_name>
Documents	https://<domain>/community/feeds/documents?rssUsername=<user_name>
Blog posts	https://<domain>/blogs/feeds/users/<user_name>
Updates	https://<domain>/people/<user_name>/feeds/updates

Setting Access for Web Service Clients

Jive exposes much of its functionality as web services. Through a web service client, other applications can interact with Jive. In order for this to happen, you'll need to first enable one or more of the web service styles that Jive supports. To set up mobile access for Jive, see the Jive Mobile documentation.

Fastpath: Admin Console: System > Settings > Web Services

Settings

You can enable client access for the following kinds of web services:

- **Core API** web services provide access to APIs using REST services. See the *developer documentation* for more information on using REST services. Core API web services are enabled by default. If you disable this, you will disable users' access to the Jive Apps Market and Jive Mobile functionality.
- **Bridging** web services access lets other Jive communities create bridges to the current one. Note that you must enable bridging here for the bridging feature to work. (For more on bridging, see *Connecting Communities with Bridges*.)
- **OpenClient v3** is an alternative REST API for providing client access to Jive data. This feature is for customers upgrading to Jive 5.0 who need to support existing web service clients. Note that as of Jive 5.0, this API is deprecated and will be removed in the next major release.
- **Legacy Web Services** provide access for clients using *Simple Object Access Protocol (SOAP)* and *Representational State Transfer (REST)* for core functionality. Note that as of Jive 5.0, this feature is deprecated and will be removed in the next major release.

You can set who will be able to access the community via web services. To restrict access to specific groups, for example, click Specific Groups, then type the names of user groups in the box provided, using commas to separate the group names. (For more on user accounts and groups, see *Managing User Accounts and User Groups*.)

Select Force SSL to require that all web services clients use Secure Sockets Layer (SSL) when connecting with your community. Note that the Force SSL setting governs access from bridge web services.

Note: Although requests from the Jive Desktop Office add-in can be filtered based on request URL (as described in *Configuration Support for External Client Access*), it can't be disabled or enabled from the admin console.

Configuring a Binary Storage Provider

By default, Jive stores binary content (attachments on blog posts, discussions, uploaded documents, images, profile pictures, and avatars) in the application database, but we recommend migrating binary content to a different binary storage provider. Storing binary content data in a location outside the database is more efficient and scalable. For production Jive systems, we recommend using a shared file system for storing all binary content. Documents created in the content editor are not binary content and are stored in the application database.

Preparing to Migrate to a Shared File System Location

You need to migrate your binary storage provider if:

- You want to use a file system provider instead of the JDBC provider enabled by default.
- You want to use the provider you're currently using, but change how you're using it. For example, you might want to use a different file system location for the file system provider.

Before you migrate to a different provider, be sure you do the following:

- Back up your current storage provider's backing store.
- Run a successful migration on a backup of this system.
- Do not run the migration tool during a busy period.
- Make sure the file system location is always available to the application.
- Estimate the the amount of space you'll need for shared storage.

Keep the following things in mind as you go through the migration process:

- During the migration, any new binary content will be stored in both the current and the new storage provider. Once the migration has completed successfully the system will switch over to the new provider.
- If any errors occur during migration the system will revert back to the current storage provider settings to allow the system to continue to function normally. Errors will be logged (see *Getting Application Logs* for more on logs). When you've addressed the errors, start over with migration.
- Keep in mind that binary content caching is disabled during migration. This might cause increased load on both the current storage provider as well as the application in general.

- Allow at least a couple of hours for binary storage migration unless you have a trivial amount of content, for example, if you're just starting a community.
- When configuring a file system provider, you'll specify a namespace. The namespace helps ensure that data is isolated for the application instance it belongs to. So, for example, if you had multiple instances (such as an internal and an external instance), you could use the same storage server while giving the storage provider for each instance a different namespace.

Migrating to a Shared File System for Binary Storage

Fastpath: Admin Console: System > Settings > Storage Provider

To migrate to a shared filesystem:

1. Prepare a single unit of shared NFS or block-level storage on your SAN/NAS, and mount it from each of your web application nodes using the same mount point on each node (for example, `/opt/jiveBinStore`).
2. From the Storage Provider page in the Admin Console, click **Migrate to another Storage Provider**.
3. Select **FileStorageProvider** in the **Registered Providers** field.
4. Click **Continue**.
5. Enter a namespace that will correspond to binary data for this application instance.
6. Enter the path to the local directory that you mapped to a mountable location in Step 1.
7. Click **Continue**.
8. Read the notes and confirm that the settings shown are the values you specified.
9. To delete binary content from the current source storage after migration, select the **Delete binary content** check box.
10. Click **Start Migration** to begin the process.
11. When the migration is complete, restart the application.
12. Disable local file caching:
    a. Navigate to **Admin Console**: **System** > **Settings** > **Storage Provider**
    b. Click **Edit** under Caching.
    c. Select **No** in the Cache Enable field.
    d. Click **Save**.

Jdbc Storage Providers

You can also migrate content to Jdbc storage providers (a DBMS).

To migrate to a different provider:

1. In the Admin Console go to the **Storage Provider** page.
2. Click **Migrate to another storage provider**.
3. In the Registered Providers field, select **JdbcStorageProvider**.

About Using a Database for Binary Storage

When you use another database for binary content storage, you specify a JNDI name corresponding to the database. During migration to the new provider, the application will create the database tables needed.

In a cluster, the JNDI name must be the same on each node where you configure an instance to use the provider.

Filtering Web Robots

You can use the Web Robots settings to ensure better community performance when you're experiencing heavy traffic from bots and spiders hitting your site.

Fastpath: Admin Console: System > Settings > Web Robots

If you find that web robots constitute a large part of site traffic, you can limit the amount of extra information overhead caused by these visits by setting rules to identify bots based on the User-Agent values found in the HTTP header. The rules you set here will determine how page views are reported and analyzed. Because bots change constantly, you may need to modify or add rules from time to time.

When you create rules, you can specify a literal substring, or you can use a fully-anchored regular expression for pattern matching. Use the *Java grammar for regular expressions*.

All the strings defined in this list will be used to filter out bots: you must remove any strings you don't want to match. To restore the pre-defined list, click **Reset to Defaults**.

Fine-Tuning with System Properties

System properties are name/value pairs that configure particular aspects of Jive. Many of these are tied to other settings in the admin console, so that changing the value in the console will change the value of the corresponding system property. For more on the properties and their effects, see *System Property Reference*.

Fastpath: Admin Console: System > Management > System Properties

Caution: Changes to some system properties have dramatic effects on the system — a wrong value can break the application. Generally speaking, you should leave system properties unchanged unless you're asked to change it by Jive's support team. You might also change a system property value if the change is part of a larger effort to customize the application. Names and values for system properties and extended properties are case-sensitive.

System Properties Reference

System properties configure application-wide settings. Some of the settings correspond to configuration elements in the admin console user interface.

To make changes to system properties, in the admin console go to **System** > **Management** > **System Properties**. Keep in mind that both property names and values are case-sensitive.

Note: Changing system property values can have a dramatic effect on how the application works. Some settings and values can even severely debilitate the application. You should only make changes to system settings under the guidance of Jive's support or professional services teams.

The following is a list of system properties that are set by default when you install Jive.

Property	Description
blog.searchComments.enabled	`true` to enable return of comments on search; false to disable it (default: true).
bridge.connection.proxy.host	Specify the host name of the proxy server so Jive can bring information from the internet into the community for bridging. Make sure the proxy server does not require a username and password because its not supported by the client used for bridging.
bridge.connection.proxy.port	Specify the port for the proxy server.
browse.main.docs.show.space.browser	`true` to have the Documents page use the original space browsing UI.
browse.main.threads.show.space.browser	`true` to have the Discussions page use the original space browsing UI.
checkmail.host	Email server name used for verifying mail settings provided in the System - Settings - Email Server screen in the admin console.

Property	Description
checkmail.port	Email server port used for verifying mail settings provided in the System - Settings - Email Server screen in the admin console (default: 110)
checkmail.protocol	Email protocol used for verifying mail settings provided in the System - Settings - Email Server screen in the admin console (default: pop3)
communityThreadCount.updateInterval.seconds	The interval, in seconds, between updates to the count of discussions displayed in the community -- such as on the "Discussions" tab of a social group. Default is 5 seconds.
converters.openoffice.skipodf	`true` to skip the ODF converter and use OpenOffice to convert directly to PDF.
document.searchComments.enabled	`true` to enable return of comments on search; false to disable it (default: true).
documentmanager.correctdeletedusers.completed	Determines if the CorrectDeletedUsersTask should run, which finds all the documents in the system and check to make sure that the original author of the document hasn't been deleted. If the author has been deleted, then this task sets the author to "guest" (id: -1)
feeds.protected	Determines whether or not feeds are protected by Basic Authentication.
GroupManager.className	Qualified class name for the default GroupManager implementation. Modify this property to identify a custom GroupManager implementation to associate users with various groups on the system.
http.proxyHost	Specify the host name of the proxy server so Jive can bring information from the internet into the community for certain features, such as RSS, bookmarks, and bridging.
http.proxyPort	Specify the port for the proxy server.
http.proxyUsername	Specify the username for your proxy server, if required.
http.proxyPassword	Specify the password for your proxy server, if required.
i18n.allowedLanguages	Not currently used
i18n.defaultLanguage	Not currently used
ip.header.max.depth	Specifies how many email jumps are secure from the X_FORWARDED_FOR email header. This is designed to reduce the possibility of a fake header when the header is set by a proxy. With this set, the application takes the IP at the position given to get to a known trustworthy address. For example, if the value of X_FORWARDED_FOR is "127.0.0.5, 10.61.8.223, 10.61.201.116, 10.61.3.9" (there are four IPs in the list) and ip.header.max.depth is set to 2, then the remote address will be interpreted as 10.61.201.116. If this property is not set, or is set to 0, the application takes the head of the list of addresses (the 0 position).
jive.auth.disallowGuest	Determines whether or not non-authenticated users are not allowed. When this property is set to true, any non-authenticated user will be redirected to the login page for all requests.
jive.bodyConversionTask.completed	Determines if the BodyConversionTask should run, which goes through all messages, documents, blog posts, comments, and announcements and converts their bodies to the new xml storage format, backing up the previous content if any changes were made.
jive.container.category.tagcloudmax	The maximum number of tags shown in a tag cloud when filtering content by categories and tags. This is an integer that defaults to 30. A very high number might impair performance or cause UI problems.

Property	Description
jive.devMode	Set to true to ensure that images, attachments, and binary documents are not cached. Also turns off page compression when set to false in conjunction with the jive.compressionFilter.enabled property being set to false.
jive.digest.enabled	`false` to disable the email digest feature. The feature is designed to send email to users with a summary of their activity in the community.
jive.digest.email.sendHour	Hour of the day at which digest emails are sent to users who have requested them in their preferences. The value should be a simple integer indicating the hours of the day. Examples are "10" for 10 a.m., "14" for 2 p.m., and "23" for 11 p.m. Default is 9.
jive.dv.service.connection.verification	`true` to have the application server test its connection with the document conversion machine before using the connection. You might want to set this to `false` if you're unable to open TCP port 7 (which is used for the test) on the conversion machine.
jive.featuredcontent.enabled	`false` to disable the featured content feature. The feature is enabled by default.
jive.featuredcontent.objecttype.<type>	`false` to disable featuring for the specified kind of content. Append the objecttype value of the content you want to disable. For example, to disable documents set it this way: `jive.featuredcontent.objecttype.102 = false`. All types are enabled by default.
jive.freemarker.templateUpdateDelay	Set to 1 to tell the application to look for changes to theme files. When you're editing theme FTL files outside of the admin console, use this property and value to ensure that your changes are picked up as you make them. (Because it can slow performance, be sure to remove this property for your production instance.)
jiveInstanceId	The universally unique instance of the application cluster, used to distinguish each server node in a clustered server configuration.
jive.pageCached.enabled	Freemarker pages are cached by default in versions 2.0 and greater (default = true even if not set in the admin console). Set this property to false to turn off caching for development purposes, which will allow theme changes to be reflected immediately in the UI without restarting the server. Page caching should be enabled for production instances however, to increase performance.
jive.pdf.paper.size	Specifies the default paper size for PDF files generated from content. The following values are supported: ANSI_A, ANSI_B, ANSI_C, ANSI_D, ANSI_E, ISO_A0, ISO_A1, ISO_A2, ISO_A3, ISO_A4, ISO_A5, ISO_A6, ISO_A7, ISO_A8, ISO_A9, ISO_A10, ISO_B0, ISO_B1, ISO_B2, ISO_B3, ISO_B4, ISO_B5, ISO_B6, ISO_B7, ISO_B8, ISO_B9, ISO_B10, ISO_C0, ISO_C1, ISO_C2, ISO_C3, ISO_C4, ISO_C5, ISO_C6, ISO_C7, ISO_C8, ISO_C9, ISO_C10, JIS_0, JIS_1, JIS_2, JIS_3, JIS_4, JIS_5, JIS_6, JIS_7, JIS_8, JIS_9, JIS_10, JIS_11, JIS_12
jive.sync.profile.ldap.login	Determines whether LDAP-provided user profile fields should be refreshed when users log in. Set to false for external communities where LDAP is not commonly used (default: true)
jive.sync.relationships.ldap	true to use LDAP to build the organizational chart and specify reporting relationships.
jiveURL	The base URL of the installation. This must be set in order for the application to work correctly.
jive.user.lastname.firstname.enabled	Determines whether user names are stored as two values -- one each for first and last names. If the value is false, then user names are stored as a single value combining first and last names. This is set during application setup.

Property	Description
jive.usercontainer.document.enabled	`false` to turn off the "Your Documents" feature.
jive.usercontainer.thread.enabled	`false` to turn off the private discussions feature.
jive.xmpp.enabled	Determines whether the XMPP service is enabled.
ldap.adminPassword.key	The private key used to decrypt the LDAP password in the database.
ldap.searchFilter	no longer used
log4j.threshold	The level at which logging messages will be recorded (default: ERROR)
mail.smtp.host	Mail server used for sending notifications and messages to users
mail.smtp.port	Mail server port used for mail notifications
mail.valid.tld.pattern	Identifies the valid TLDs pattern used to validate email addresses. The default pattern is `com|net|org|edu|int|mil|gov|arpa|biz|aero|name|coop|info|pro|museum|mobi|cat|jobs|asia|tel|travel` and accepts email addresses ending in these suffixes, for example `user@email.travel`. This can be changed by adding the new supported TLD to the end of the list. For example, to support `qlat` append **|qlat** to the property to make it `com|net|org|edu|int|mil|gov|arpa|biz|aero|name|coop|info|pro|museum|mobi|cat|jobs|asia|tel|travel|qlat`
officeintegration.enabled	`true` to enable support for a preview view of some documents, including PDFs and those from Microsoft Office; default is `false`.
opensearch.key	Unique ID used for external search engine integration
passwordReset.caseSensitive	`true` to allow case-sensitive lookup of usernames when setting a password; default is true. Set this to `false` to allow for case-insensitive username lookup when resetting a password. When this is set to false, if two username values differ only by case, a password reset may fail with an error message until distinct usernames are created. To avoid this, you need to manually change one of the usernames to make the usernames different for case insensitivity.
polls.voting.private	`true` to exclude poll votes from visible activity. The default value -- `false` -- will allow poll votes to appear among other recent activity.
profile.security.collagues.mgr.enabled	`true` to specify that a person's manager is included in the "Colleagues" option when the person is setting visibility for a profile field. Default is `true`. If you change this property, you must rebuild the user search index for the changes to take effect. See *Configuring Main Search* for more information.
profile.security.collagues.drpts.enabled	`true` to specify that a person's direct reports are included in the "Colleagues" option when the person is setting visibility for a profile field. Default is `true`. If you change this property, you must rebuild the user search index for the changes to take effect. See *Configuring Main Search* for more information.
search.indexCreated	Tracks the last time the search index was created (set by the system)
search.indexVersion	The version of the currently used user index.
skin.default.displayFullNames	Set to true to display the full names of users, or false to use their username.
skin.default.newAccountCreationEnabled	Determines whether users are allowed to register to create a new account (default: true)
system.adminuser.email	The default email address that the system will use when sending email notifications

Property	Description
system.adminuser.fromName	The default "From" name that the system will use when sending email notifications
update.lastCheck	Tracks the last time the system checked for updates to plugins or the server (set by the system). New versions of plugins can be downloaded and installed. However, new server releases should be manually installed.
ur.graph.hier.default.ID	The ID of the default (hierarchical) org chart graph.
ur.graph.mesh.default.ID	The ID of the default (mesh) friends/connections graph.
user.default.displayEmailAddress	Determines whether or not to display a user's email address.
webservices.rest.enabled	Determines whether or not REST-style web services are enabled.
webservices.soap.accessType	The access type for SOAP web services. Possible values include all (for all users), registered (for registered users only), specificUsers (for specifically named users only), and specificGroups (for specifically named groups only).
macros.unproxyobjects	true to render the link -- rather than an error message -- even when the user might not have permission to view the linked content. This is false by default in order to prevent potentially sensitive content (such as the linked document's title) from being seen by those who don't have permission to view the content.
people.search.pagesize	The number of results per page in people search
polls.enabled	Turns on polls, and displays the "Create a poll" link in the Actions sidebar if the user has been given permissions to create polls.
questions.markThreadAsQuestionByDefault	Set to true to mark discussions as questions by default (display the "Mark thread as question" checkbox in new discussions as checked), or set to false to leave it unchecked by default. Often users do not even notice that the checkbox is there, and turning it on by default allows users to give points to other users when they provide a correct or helpful answer.
skin.default.changePasswordEnabled	Determines whether users can change their password. Values(true,false).
skin.default.headerHTML	Replaces the header logo for the entire application with the html entered in this system property.
skin.default.newAccountCreationEnabled	Determines whether users can register their own user accounts. Values(true,false).
skin.default.recentHistoryEnabled	Set to false to hide the History menu on the userbar (defaults to true)
system.console.custom.title	The value that should be used in the page title for the admin console. Typically, this matches the title of your community, such as "Acme Community Admin Console".
webservices.soap.enabled	Whether or not SOAP webservices are enabled (default: false)
webservices.xmlrpc.enabled	Whether or not XML-RPC webservices are enabled (default: false)
webservices.soap.accessType	Sets how users can access webservices possible values are • all - Any users. • registeredUsers - Disallow anonymous access. • specificUsers - Only allow specific users (Use the webservices.soap.allowedUsers property to set). • specificGroups - Only allow specific groups (Use the webservices.soap.allowedGroups property to set). (default: all)

Property	Description
webservices.soap.allowedUsers	Comma separated list of allowed users by username (see property: webservices.soap.accessType)
webservices.soap.allowedGroups	Comma separated list of allowed groups by group name (see property: webservices.soap.accessType)
webservices.soap.forceSSL	If this property is set requests that are not over SSL will fail. (default: false)
webservices.soap.permissionHandler.className	Override this property to customize the inbound Handler for XFire. (default:com.jivesoftware.community.webservices.server.xfire.PermissionHandler)

Managing the Community

This section includes information about creating and managing spaces, assigning permissions, and moderating content.

Making Simple UI Changes

Through a simple user interface, you can change the site-wide logo and colors.

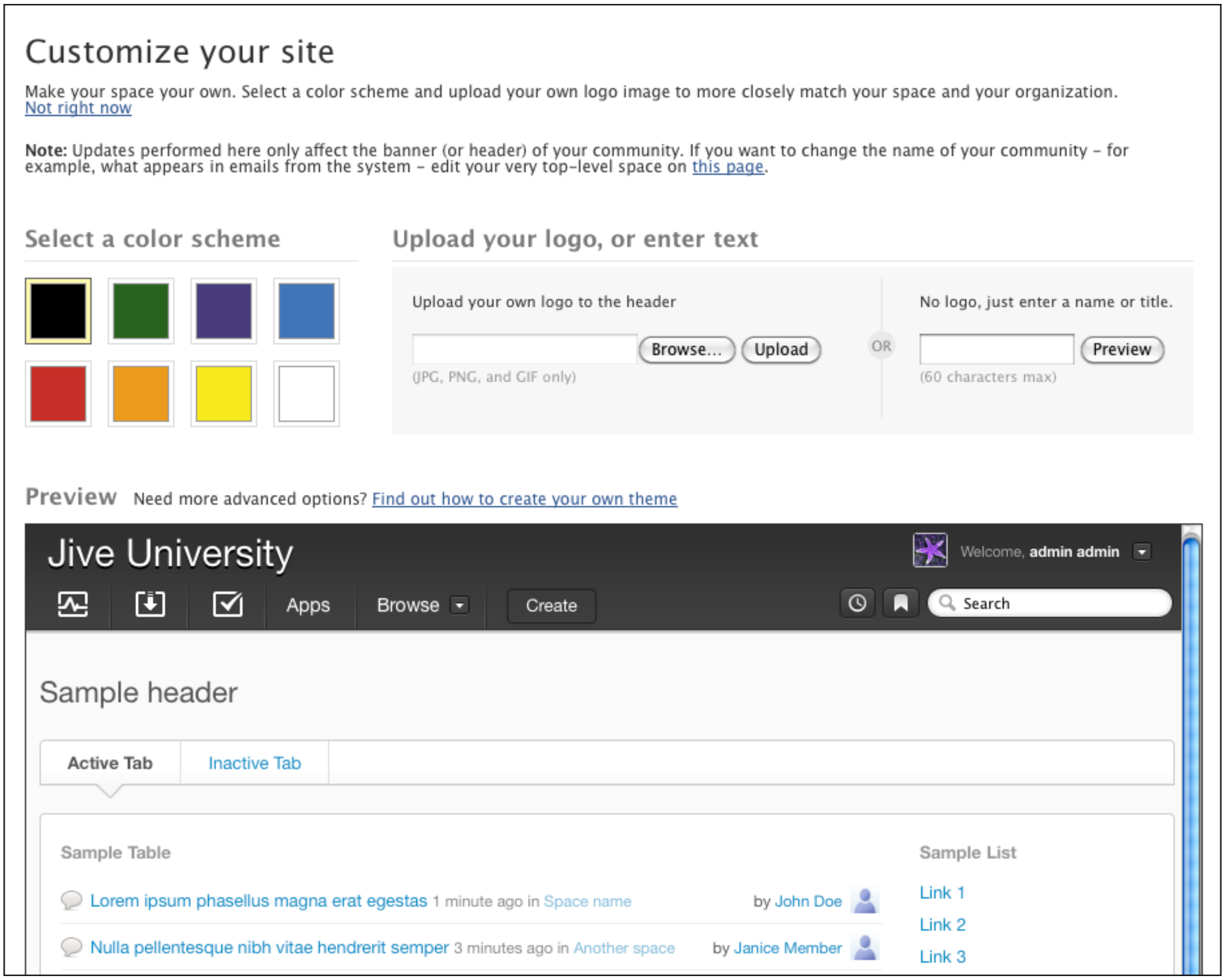
Note: To make the changes described here, you'll need administrator privileges. You'll need to be either a system admin or a space admin for the root space.

The basic changes you can make here are based on predefined schemes. If you're looking for a way to upload your own themes, see *Customizing the UI with the Theme Resource Kit* and *Adding and Editing Themes*.

Choosing Site Colors and Logo

To make Jive a better fit for your community, you may want to change the color scheme and the logo that appear across the site. As an administrator, you can do this easily without logging into the admin console. Jive offers a simple way in the user interface to make basic site-wide customizations.

1. In the end user UI, click the down arrow next to your name and then **Customize Your Site**. You must have administrator privileges to see this option.
2. On the **Customize your site** page, under **Select a color scheme**, click the color you want to use. You'll see the preview section at the bottom of the page update as you click colors.



The UI in the preview is "real," even including a few links that navigate to other parts of the application. You probably want to keep the preview as it is, so try not to click the links.

Also, notice the link, **Find out how to create your own theme**. If you're not able to get the look you want on this page, you can click the link to reach a page with more advanced options. There, you can get started editing source code to create your own theme. For more information see *Customizing the UI with the Theme Resource Kit*.

3. To replace the default logo, either upload a new logo image or enter text to appear in the logo area. If you upload an image, be sure to use a JPG, PNG, or GIF file.

   Using an image with a transparent background will help ensure a cleaner look, with the background color showing through. The background behind the logo is designed to adjust to the size of the image you apply.
4. Click the **Preview** button next to your selection to update the preview section.

   If you enter a name or title instead of a logo image, you can undo the preview by deleting the text from the box and clicking **Preview** again.
5. Click **Publish Design** when you're ready to save your changes. If you don't like your changes, click **Discard Changes**. To reset the site back to the defaults it had when you got it, click **Reset Site to Default**.

Enabling a Custom Community Home Page

If you don't want the What Matters: Activity page to be your community's home page, you can enable a customizable one in the admin console

Fastpath: Admin Console: System > Settings > Home Page

If you want to use a customized home page on your site, you can select **Enable the widgetized community home page**. When this setting isn't enabled, the default page for users is the What Matters: Activity page. (Users can override the default page setting using their individual Preferences setting.)

If you want to choose a different community page as the default for all users, you can use the `skin.default.landingpage` system property to set it to any of the What Matters pages. Check the URL of the target page for the correct value. For example, to set the default page to Communications, set the value to /communications.

Customizing Places

You can customize the places in your community to give your users exactly what they need.

Sharing Exchange Calendars in an HTML Text Widget

Using an Exchange 2010 SP1 or later email server, you can set up a community widget to show users' Exchange calendars, with customizable levels of visible calendar details.

Caution: Calendar sharing uses Exchange Web Services to make HTML and iCal versions of the users' calendars available. Depending on your Exchange topology, this can (and will) publish calendar URLs to the Internet, where they could be viewed by anyone. If you want to prevent this, make sure you have a secure firewall in place.

To get started, set up the following on your Exchange server:

- Create a calendar sharing profile
- Enable the calendar sharing profile for each user for whom you want to have a visible calendar in the community

Note: You cannot share calendars contained in public folders. A shared calendar must be a user mailbox.

Next, follow these steps to publish shared calendars in your community:

1. Ensure that calendar publishing is enabled on your Exchange server. To do this, you can use the following Exchange PowerShell commandlet:

```
Get-OwaVirtualDirectory | ft server, Name,
                        CalendarPublishingEnabled
```

2. Enable calendar publishing with:

```
Set-OWAVirtualDirectory "SERVER\owa
                        (Default Web Site)" –CalendarPublishingEnabled:
$true
```

3. From the Exchange Management Shell, create a new calendar sharing profile and enable anonymous shares:

```
New-SharingPolicy -Name "Calendar Sharing
                        Policy"
```

4. Set the sharing policy on user mailboxes who wish to share their calendars:

```
Set-Mailbox -Identity User.Mailbox -SharingPolicy "Calendar Sharing
                        Policy"
```

5. Tell the target users to share their calendars either via Outlook 2010 or via Outlook Web Access.
6. When the user publishes a shared calendar, gather the full text of the "Link for viewing calendar in a web browser." This link will look something like this:

```
https://YOUR.MAIL.SERVER/owa/calendar/GUID@YOURDOMAIN.PUBLIC/
DIFFERENT_GUID/calendar.html
```

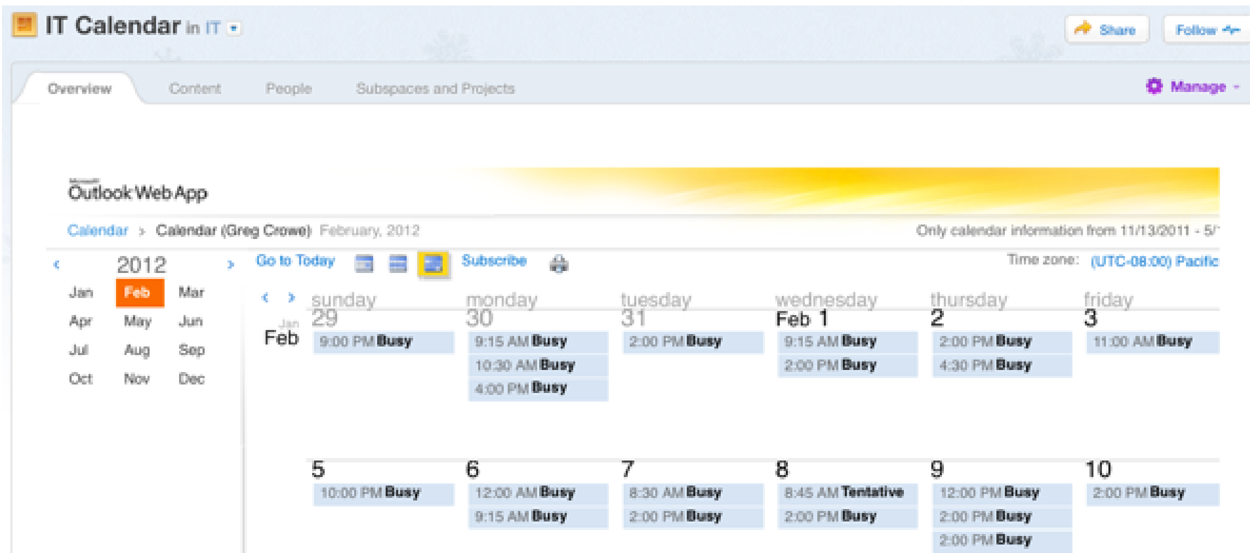
7. In the community place where you want to share calendars, edit the place to include an HTML widget.

8. In the widget, include the link from above. This link must be contained in an iframe tag. Here is an example:

```
<iframe src="https://YOUR.MAIL.SERVER/owa/calendar/GUID@YOURDOMAIN.PUBLIC/
DIFFERENT_GUID/calendar.html" width="1200" height="800"></iframe>
```

9. Save and publish your changes to the place.

Your results in the space will look something like this:



Managing Spaces

A space is a place for content, including documents, discussions, and blogs. A space can also contain projects, polls, tags, and announcements. You can create and configure spaces, setting up defaults for content and managing discussions and documents.

Spaces are typically arranged in a hierarchy that reflects how the community's users are organized. For example, a human resources department might have its own space, with sub-spaces for content related to benefits and recruiting. Spaces provide the context for organizing content, sharing information, collaborating, and generally getting things done.

In This Section

- A space is a place for content such as documents, discussions, and blogs. A space can also contain projects, polls, tags, and announcements.
- You typically structure spaces in a hierarchy, in which some spaces contain other spaces (also known as "sub-spaces"). The hierarchy tends to mirror the organizational context of people using the space.
- You can customize a space's overview page using widgets.
- People with system admin or space admin permissions can create spaces. They can also grant people access to space features related to content or administration features.
- By default, people with system or space admin permissions for a space have those same permissions for spaces inside it (sub-spaces).
- You can assign moderation permissions to one or more users, giving them the ability to approve or reject new content, and edit, delete, and move existing content.
- You can set defaults for discussions and archive discussions.
- You can make discussions available for display on other web sites.

Designing Space Hierarchies

One of the first things you'll do when setting up Jive is create spaces and sub-spaces in hierarchies that reflect your community's functional areas or interests.

A good way to design spaces is to match how your company organizes functional teams and projects. For example, at a high level, spaces could reflect organizational divisions. Sub-spaces are likely to reflect organizational subdivisions, but they could also mirror areas of interest or other more informal boundaries. For example, you might create a top-level Sales space for the sales department, then create sub-spaces such as Channel Sales, Business Development, and Direct Sales. Other criteria by which to define sub-spaces include functional area and topic.

As you define spaces, keep in mind:

- Before adding spaces to the system, you might want to collect information about roles for those who will have special permissions — such as blog authors, moderators, and so on. As you create spaces and sub-spaces using the admin console, you'll be prompted for this information.
- Each space and sub-space can have different sets of permissions, so you can control access and capabilities within a space.
- When defining spaces and sub-spaces, be sure that the divisions and hierarchy are intuitive to people. You might start by looking at how people and teams are organized. You could also create a suggested space/sub-space hierarchy and get user feedback on it.
- Create a general, high-level hierarchy to get started. After people are involved, they'll refine the categorization using tags. As a general rule, larger numbers of spaces and sub-spaces tend to create silos and reduce the power of tagging.
- Define spaces with the role of tags in mind. Spaces organize content, but over time tags will grow to constitute virtual groups to organize content also. As people apply tags to content, for example, a tag such as "personal" might come to mean "a blog post or document that isn't connected with the company's business." In other words, this is probably a better way to categorize "personal" posts than a "Personal" sub-space would be.
- Note that content can't be shared and tagged between discrete spaces -- only within the space in which it's created. Use a space to group multiple concepts or functional areas; use a category to group together discrete concepts within a space.
- For usability reasons, avoid creating a large number of spaces. With a large number of spaces, certain elements in the user interface can become difficult to use. These include lists (including dropdown lists) that display the names of all the spaces.
- Content from a sub-space isn't found when searching the space that contains it, nor is the contained content listed on the All Content page. You can show content for each sub-space with a widget when you customize the space's Overview page. You can also use the Recent Activity widget to show recent activity for all sub-spaces.

Creating and Arranging Spaces

As an administrator, you can create spaces using the end user UI or the admin console. In the admin console, you can also arrange the space hierarchy.

Fastpath: Admin Console: Spaces > Management > Summary

Arranging Spaces

You can view and arrange the list of spaces in the admin console. The space Summary page lists spaces in the full hierarchy and provides a way to create spaces or edit their settings.

On the space Summary page, on the Browse tab, you can drag spaces up and down to reorder the list. Although you can't change where a space is in the hierarchy by dragging it, you can change that with the Move button, as described below.

When you've selected a space in the list, you'll see four buttons: New, Edit, Move, and Delete (you can't move or delete the root space).

- Click **New** to create a new space inside (hierarchically) the space you've currently selected.
- Click **Edit** to edit the space's properties (see *Setting Space Name, Locale, and Allowed Content Types*).
- Click **Move** to start moving the selected space to another place in the hierarchy. There, on the Move Space page, click the name of the space you want the selected space to be inside, then click **Move Space**.
- Click **Delete** to delete the space and all the content inside it. Before the space is deleted, you'll get a warning with notes about what deletion means, along with a summary of the amount of content inside the space you're deleting.

Creating a New Space

You can create a new space from the admin console or the user interface. With either approach, you'll use the same steps to create the space.

1. Start creating the space.
    - In the admin console, go to **Spaces** > **Management** > **Summary**, then click the name of the space that will contain the new space. Click **New**.
    - In the user interface, go to the space that will contain the new space. In the Actions list, click **Create a sub-space**.
2. On the Create New Space page, for a Space Name, enter the space name to appear in the user interface.
3. Enter a description that to appear in the user interface, such as a brief description of what the space is for.
4. For Space Display Name, enter the text that will be used in URLs that access the space.
5. Under Permissions, choose a default access scheme. Each of the options represents a set of permissions that you can also edit later.
6. Under Types of content..., select content types you want the space to support. Space users will be able to see or create only the content type you specify.
7. Click **Create**.

Customizing a Space Overview

You can customize the layout of a space in the user interface. Go to the space's home page and click **Manage** > **Overview page**. From there you can select the layout and drag and drop the widgets you want displayed when users visit your space. Useful widgets to consider are Featured Content, Recent Activity, and Related Projects. When you're finished, click **Publish Layout**.

Tip: If you've seen another space layout you like, you can copy it to your current space by clicking **Copy** and then selecting the space.

To learn more about widgets, see *Designing Pages with Widgets*.

Configuring Spaces

Setting Space Name, Locale, and Allowed Content Types

You can change a space's **name** and **description** if the space's focus changes. You can also change the display name, which is the name used in URLs that link to the space.

Fastpath: Admin Console: Spaces > Settings > Space Settings

For sub-spaces, you can also set which **content types** the space supports. For example, by clearing the Documents check box, you'll remove the Create a document link from the space's Actions list. It also means that users won't be able to select that space when choosing where to put a new document they're creating using the Create menu. Such a change also applies to existing content. So, if users have created documents in the space, and then you clear the Documents check box to remove support for them, existing documents will no longer be viewable in the space (although they'll still exist).

Display name is the text displayed at the end of the space's URL in the browser's address bar. For some people, using the space's URL is a quick way to get to the space. (Note that you can't change the display name for the root space.)

Change the space's **locale** setting to set end user UI characteristics such as language, date format, and so on. Keep in mind that this locale setting applies to one of several locale scopes that can govern UI. For more on how the locale is chosen for display to the user, see *Locale Settings*.

Configuring Discussions for a Space

Within a space, you can configure discussion settings related to threads marked as questions. These settings govern how alerts should be sent for questions that remain unanswered.

Fastpath: Admin Console: Spaces > Settings > Discussion Settings

Note: For application-wide discussion settings, be sure to see *Configuring Discussions Application-Wide*.

Enabling email alerts for open questions. Choose "Enabled" to have an email sent when a thread marked as a question has remained open (unanswered) for the period of time you specify. You might want to enable alerts if you want to make sure that questions get prompt responses. If you enable this, be sure to enter the recipient's email address. With this enabled, email will be sent to the people whose addresses you give in the **Email Addresses** box.

Specify an **open question age** value that makes sense for your community. If it's a very active community, you might want to make this shorter.

Setting a Document Approver in a Space

You can specify someone to approve all documents created in a space before the documents can be published and made visible to other users. With a space approver assigned, users will submit a document for approval before it is published.

You specify space approvers in the admin console as a setting for each space. For information on moderation, see *Moderating Content*.

Note: A space approver only approves documents. If you want to control more than documents, use the moderation feature. To learn more about that, see *Moderating Content*.

Fastpath: Admin Console: Spaces > Settings > Document Settings

Setting Space Approvers

To set space approvers, type the approver's application username in the **Add User** box. You can also browse for users with the Select People tool. You can add more than one approver.

How Space Approval Works

Note: If the containing place of the document has moderation enabled, then the approver(s) must approve the content before it will be sent to the moderator's queue.

1. A user creates a document in the space.
2. The user clicks "Send for approval" and the document goes into an approval queue. The document isn't actually *sent* somewhere, but is marked for approval by the application.
3. The approver will know when something needs approval by the alert in their **What Matters: Actions** icon.
4. On the approver's Actions > Notifications page, there is a list of documents waiting to be approved.
5. By clicking on a document, the approver can view the document and then approve or reject it. If they approve it (and if all other approvers approve it), the document will be published. If they reject it, they can enter an explanation and the document will be sent back to the author as a draft.
6. The author can edit and resubmit the document.

Note that a document can also have document-level approvers who've been designated through its Manage Collaboration page. All approvers must approve before a document is published.

Setting Up Abuse Reporting

Fastpath: Admin Console: Spaces > Settings > Abuse Settings

When abuse reporting is enabled, people can use a link on content to report the content as abusive. When someone clicks the link, the content is sent to the moderator's queue so that it can be evaluated; while the content is waiting to be approved, it will still be displayed. Abuse reporting is a system-wide, global setting: if it's enabled, it's on for every piece of public or private content on which abuse can be reported.

Abuse reports for open or member-only social groups go to the system moderator, but to the system administrator for private or secret social groups. Abuse reports are queued in the space moderator's moderation queue. If there's no moderator for that space, the report is queued at the root space level.

To set the threshold after which the offending content should be hidden until it can be reviewed by the administrator, use the **Automatically hide content after** setting. For example, if you set this value to 5 and then five users flag the same piece of content for abuse, the content will be removed from view pending moderation. By default, all content types (such as discussions, blogs, and documents) are handled in the same way when abuse is reported.

Note that the application does not send email notifications to moderators for abuse reports. To keep up with abuse reports, moderators and administrators should check their moderation queue. For more on moderating content in the queue, be sure to see *Reviewing Queued Moderation Requests*.

The following table shows the types of content that can be configured for abuse reporting, who moderates abuse reports, and the order in which Jive notifies the abuse reports moderator(s). When abuse reporting is enabled in a place, the application sends a moderation notification to the first valid moderator it finds. For example, if you set up a moderator for abuse in an open social group, Jive first looks for a global (root space) moderator (because social groups are not attached to any parents); if there is none assigned, it then looks for a full access moderator (typically, system administrators).

Abuse	Announcements	Polls & Poll Comments	Documents & Document Comments (1. If abuse reporting is turned on in the admin console. 2. On a per document basis. 3. Notifications go to the space moderator.)	Discussions & Discussion Replies	Blog Comments	Status & Status Comments	Avatar	Registration	Trackback	Profile Image	Private Messages
Space	⊘	S→G→F	S→G→F	S→G→F	S→G→F	⊘	⊘	⊘	⊘	⊘	⊘
Open & Member Group	⊘	G→F	G→F	G→F	G→F	⊘	⊘	⊘	⊘	⊘	⊘
Private & Secret Group	⊘	F	F	F	F	⊘	⊘	⊘	⊘	⊘	⊘
Your Personal Content	⊘	G→F	Visibility:Open G→F Otherwise X	F	G→F	[1] G→F	⊘	⊘	⊘	⊘	⊘
Root Container	⊘	G→F	⊘	⊘	G→F	⊘	⊘	⊘	⊘	⊘	⊘
Project in a Space or Group	⊘	I	I	I	I	⊘	⊘	⊘	⊘	⊘	⊘

[1] Status and Status Comments are not moderated in v 5.0.2 or earlier

F = Full Access (user is a community/system administrator)
S = Space Moderator
G = Global/Root Space Moderator
I = Inherited from parent space

X = Not moderated
⊘ = Cannot create in that container
→ = Order of moderation notification

For Jive 5.x

Archiving Discussion Threads

You can "clean up" old discussion content by archiving it. When you turn archiving on for discussions in a space, you can specify how old a thread should be before it's archived and whether archived threads are deleted or moved to another space. For example, you could create a space for holding archived threads.

Fastpath: Admin Console: Spaces > Settings > Thread Archive Settings

Exposing Discussions on Another Site

You can expose certain discussions from your Jive community through web pages that aren't part of Jive by using the Community Everywhere feature. For example, if you've got a web site that describes products offered by your company, you might want to expose discussions related to tips for using the products. Visitors to your product page would be able to view a link to discussions in Jive and optionally see recent posts as well as a box for adding a comment.

If you want to encourage people to participate in your Jive community, Community Everywhere can be a useful enticement. In the admin console, you can enable the feature, limit the sites that can use it, even generate the script code needed to add Community Everywhere links to web pages.

For more about Community Everywhere and how to set it up, see *Using Community Everywhere*.

Fastpath: Admin Console: Spaces > Settings > Community Everywhere

Using Community Everywhere

With Community Everywhere, you can embed discussion threads directly into existing news articles, blog posts, or other content that would benefit from comments or discussions.

Instead of forcing users to leave your content to create a comment or view a discussion thread, you use Community Everywhere to enable users to log in or create an account and participate in discussions while on the page that contains your content.

This topic explains community everywhere, describing how you can set it up via the admin console and generate the script you'll use to embed access to discussions into your other content.

Community Everywhere embeds your discussion threads using JavaScript: first you enable Community Everywhere via the admin console, then you generate a unique key for each one of the articles you want to embed discussions on, and, finally, you insert a JavaScript <script> tag into the pages that you want discussions to be shown.

Setting Up Community Everywhere

Before you can use Community Everywhere, you must first enable it via the admin console.

Fastpath: Spaces > Settings > Community Everywhere.

You can optionally choose to limit the sites that embed discussions by entering a comma-delimited list of referrers that should be allowed to embed discussions. Each of the referrer values must begin with http:// or https://. You can also specify a user who will be used as the author of the threads that are generated by your content (note that users of your application will only be able to create replies/messages to threads which are generated automatically by Community Everywhere).

If you choose not to enable the Community Everywhere feature, the feature will display an error message stating that "Comments have been disabled by the system administrator." If a user attempts to use the Community Everywhere feature from a web site that you haven't explicitly allowed in the referrer list, the Community Everywhere feature will display an error message stating that "This site is not authorized to access the Community Everywhere feature."

Script Generator

Once you have enabled the Community Everywhere feature, you use the Script Generator to create URLs that you can embed in your site. There are options for the amount of content you can show:

- **Display "Discuss This" Link**: Choosing this option will result in only a link back to your community to a thread created from this piece of content. If a user posts a reply message, the reply and any other messages will not be displayed with the content.
- **Display "Discuss This" Link and Recent Posts**: Choosing this option will show a link to your community to a thread created from this piece of content and will show the messages (if any) in the thread.
- **Display "Discuss This" Link, Recent Posts, and Comment Box**: Choosing this option will show a link to your community to a thread created from this piece of content, will show the messages (if any) in the thread and will show a comment box giving users the ability to create comments on the piece of content.

The Script Generator gives you four display options for the content generated from the choice you made about the content to display:

- **View Threaded**: Select this option to have messages displayed as threaded (indented hiearchically), rather than flat.

- **Show Discussion Statistics**: Select this option to have Community Everywhere display the total number of replies and the date and time of the last reply. Sample: 2 message(s). Last at: Feb 28, 2007 12:48:36 PM
- **Open Link in New Window**: Select this option to have Community Everywhere force the opening of a new window when the user clicks on the "Discuss This" link.
- **Include Default Style (CSS)**: Select this option to have Community Everywhere include style markup (via CSS) in the list of replies and comment box.

The Script Generator requires you to choose the space/community that you want the thread to be generated in and provides a button that gives you the ability to generate a unique key for each piece of content. After you've settled on all the options, you can copy and paste the text in the **Code** section of the admin console page into the HTML of the content that you want the Community Everywhere feature to be embedded in. See the **Usage** section below for more information.

Finally, the Community Everywhere feature gives you the ability to choose a custom title and description for the thread that is automatically generated by the system. You can do this by including two meta tags in the <head> of your document:

```
<meta name="jiveTitle" content="A discussion about Widget Foo"/>
<meta name="jiveDescription" content="Add your thoughts about the Widget Foo
 article below."/>
```

or by including a snippet of JavaScript code in your document:

```
<script language="JavaScript" type="text/javascript">
    var jiveTitle = "A discussion about Widget Foo";
    var jiveDescription = "Add your thoughts about the Widget Foo article
 below.";
</script>
```

Script Generator

After you have *enabled the Community Everywhere feature*, you use the Script Generator to create URLs that you can embed in your site. There are options for the amount of content you can show:

- **Display "Discuss This" Link**: Choosing this option will result in only a link back to your community to a thread created from this piece of content. If a user posts a reply message, the reply and any other messages will not be displayed with the content.
- **Display "Discuss This" Link and Recent Posts**: Choosing this option will show a link to your community to a thread created from this piece of content and will show the messages (if any) in the thread.
- **Display "Discuss This" Link, Recent Posts, and Comment Box**: Choosing this option will show a link to your community to a thread created from this piece of content, will show the messages (if any) in the thread and will show a comment box giving users the ability to create comments on the piece of content.

The Script Generator gives you four display options for the content generated from the choice you made about the content to display:

- **Number of Posts to show**: Enables you to choose the number of replies that will be displayed alongside your content. The default is to display all the replies. You can choose to limit the number of replies to five, ten, fifteen, twenty or twenty five replies.
- **Show Discussion Statistics**: Select this option to have Community Everywhere display the total number of replies and the date and time of the last reply. Sample: 2 message(s). Last at: Feb 28, 2007 12:48:36 PM
- **Open Link in New Window**: Select this option to have Community Everywhere force the opening of a new window when the user clicks on the "Discuss This" link.
- **Include Default Style (CSS)**: Select this option to have Community Everywhere include style markup (via CSS) in the list of replies and comment box.

The Script Generator requires you to choose the space/community that you want the thread to be generated in and provides a button that gives you the ability to generate a unique key for each piece of content. After you've settled on all the options, you can copy and paste the text in the **Code** section of the admin console page into the HTML of the content that you want the Community Everywhere feature to be embedded in. See the **Usage** section below for more information.

Finally, the Community Everywhere feature gives you the ability to choose a custom title and description for the thread that is automatically generated by the system. You can do this by including two meta tags in the <head> of your document:

```
<meta name="jiveTitle" content="A discussion about Widget Foo"/>
<meta name="jiveDescription" content="Add your thoughts about the Widget Foo
 article below."/>
```

or by including a snippet of JavaScript code in your document:

```
<script language="JavaScript" type="text/javascript">
    var jiveTitle = "A discussion about Widget Foo";
    var jiveDescription = "Add your thoughts about the Widget Foo article
 below.";
</script>
```

Usage

After you've completed the configuration steps in *Setting Up Community Everywhere*, you're ready to embed the Community Everywhere feature into your content. To do so, you will simply cut and paste the <script> tag in the text box into your page. As an example, let's say you had an article about Widget Foo on your site:

```
<p>
    Widget Foo is the greatest tool on the planet. You should buy one now.
</p>
```

And you want to include a discussion form and replies below your content. You would go the admin console, enable Community Everywhere, choose the content and display options you want, and click the "Generate New Key" button. You would then copy and paste the <script> tag into your content so that the end result would look something like this:

```
<p>
    Widget Foo is the greatest tool on the planet. You should buy one now.
</p>

<script language="JavaScript" type="text/javascript"
    src="http://our-community/everywhere/1801?community=2003&key=TGFu9V">
</script>
```

Fine-Tuning with Extended Properties

Extended properties are name/value pairs that configure particular aspects of a space. Many of these are tied to other settings in the admin console, so that changing the value in the console will change the value of the corresponding property. Generally speaking, you should leave properties unchanged unless you're asked to change it by Jive's support team. You might also change a system property value if the change is part of a larger effort to customize Jive.

Fastpath: Admin Console: Spaces > Settings > Extended Properties

Note: Names and values for system properties and extended properties are case-sensitive.

Managing Content in a Space

From the admin console, you can access discussions and documents in a space. A few of these features are also available in the user interface.

Note that settings you make at the root level apply to all social groups. From the document- and discussion-management perspective, you can think of social groups as being contained at the root.

Managing Discussions

Content moderators have the ability to edit and delete discussions, as well as make other changes. You can view a list of the discussions in a space, and edit or delete them. As a space administrator, you're also able to edit or delete discussions when you're viewing them in the community.

For more on moderation, see *Moderating Content*.

Fastpath: Admin Console: Spaces > Management > Discussion Management

Managing Documents

You can view a list of a space's documents and edit, restore, or delete them. If a user deletes a document, you can still see the document from this page of the admin console. You can either restore the document by editing and publishing it, or you can permanently delete it from the community.

Fastpath: Admin Console: Spaces > Management > Document Management

Important Notes:

- A space administrator can edit or delete that space's documents when viewing them in the community.
- Content moderators also have the ability to edit and delete documents, as well as make other changes. For more on moderation, see *Moderating Content*.
- Be aware that as an administrator, you may move a document from one space to another; however, users who need that document may not have document viewing permissions in the new space.

Managing Categories

Categories are words or phrases through which users can add content to predefined groups. As an administrator, you define categories in a way that's specific to a particular place (a space or social group, for example). As you create categories, think about how the place's content should be grouped. You can optionally associate certain tags with the category. If you do, someone who uses those tags with content will see the category's name highlighted. This is a cue to consider assigning the content to the category.

By creating or editing categories, you can help ensure that content is organized in the best way for people using the space.

Fastpath: Admin Console: Spaces > Management > Categories Management

To manage categories:

1. In the admin console, go to **Space** > **Management** > **Categories Management**.
2. To create a new category:
    a. Select a space and then click **Create New Category**.
    b. Enter the new category's name and description.
    c. Enter the tags that should be associated with this category. When people attempt to assign these tags, they'll be prompted to assign the associated category.
    d. Click **Save**.
3. To edit an existing category:
    a. Under Categories, locate the category you want to edit.
    b. Click the category's edit icon.
    c. Edit the category properties as needed.
    d. Click **Save**.

Merging Spaces

You can merge the content from one space into another space. This can be a useful way to remove spaces that are no longer needed *as spaces*, but whose content you still want to keep.

Fastpath: Admin Console: Spaces > Management > Merge Spaces

You'll need to be a space administrator for both spaces to merge content from one to another. Merging content moves all of the content into the destination space, mixing it with content that's already in the destination space. The space you're merging from will be deleted after the merge.

Note: You can't merge the root space into another space.

To merge the content from one space into another space:

1. In the admin console, go to **Spaces** > **Management** > **Summary**.
2. In the list of spaces, click the name of the space you want to merge *from*.
3. Click **Merge Spaces**. The Merge Space page displays a summary of content in the space.
4. Click the name of the space you're merging content *into*. This will begin the merge. The space you're merging from will be deleted during the merge.

Moderating Content

A user assigned as a content moderator can edit, approve, or reject content before the content is published and visible to others.You may want to designate a moderator to review and approve content before it's published if content in a place could become contentious or contain sensitive information. This section describes how moderation works and how to set it up.

What Is Content Moderation?

Content moderators review content before it is published in the community. As a community administrator, you may want to designate a moderator to review and approve content before it's published if content in a place could become contentious or contain sensitive information.

Content You Can Moderate

Community administrators can enable moderation for most content types in spaces, sub-spaces, social groups, blogs, and so on. You can designate one or several content moderators per place. For a complete list of content types and the places where you can enable content moderation, see *Who Moderates What?*

Content You Can't Moderate

Private content cannot be moderated. This includes content created in private groups, secret groups, private discussions, and Your Documents that have visibility limited to the author or specific users.

Other Kinds of Moderation

- **Abuse reporting.** When users report abuse, the reports are sent to a moderator. For more information, see *Setting Up Abuse Reporting*.
- **Document approval.** Document approval is different from content moderation in that document approvers can only approve *documents* in a given space. For information about that, see *Setting a Document Approver in a Space*.
- **New user registrations.** You can moderate new user registrations. For more information, see *Moderating User Registration*.
- **Avatars.** You can moderate user avatars. See *Avatar Settings*.

Moderation Best Practices

Here are some best practices to consider when using moderation:

Develop a Community Usage Policy

Make the usage policy for content and discussions available and easy to find.

Here are some ideas for usage policy statements:

- Don't use profanity.
- Treat others with respect.
- Stay on topic.

Encourage Users to Report Abuse

You can design policies to ward off abusive or inappropriate posts. Early warning can make a big difference by preventing users from having a negative experience. Make the consequences clear for unacceptable behavior. Other community users are more likely to follow the guidelines when you enforce them quickly and publicly, for example, by removing or editing an offensive post. For more information about abuse reporting, see *Setting Up Abuse Reporting*.

Designate More than One Moderator Per Place

Relying on only one moderator can cause a bottleneck if that person becomes unavailable. Consider designating more than one moderator per place. Here's why:

- The moderation queue for a given place is visible only to its moderator(s). It is not visible to moderators of other places.
- Content set for moderation will remain unpublished (and invisible to the community) until it is approved by the moderator.
- Existing moderation requests cannot be routed to another moderation queue (for example, from a sub-space to the root space) after they're in the moderator's queue. They will remain in the queue until they're moderated (i.e., approved or rejected).
- Users added as new moderators in a place won't see existing moderation requests in that place's moderation queue, only moderation requests that are posted after they became a moderator.

Be Aware that Some Content Cannot Be Moderated

You cannot moderate content created in private groups, secret groups, or content that has visibility limited to the author or specific users.

Who Moderates What?

The following table shows the types of content that can be configured for moderation, who moderates them, and the order in which Jive notifies the moderator(s). When moderation is enabled in a place, the application sends a moderation notification to the first valid moderator it finds. For example, if you set up a moderator for announcements in an open social group, Jive first looks for a global (root space) moderator (because social groups are not attached to any parents); if there is none assigned, it then looks for a full access moderator (typically, system administrators).

Moderation

	Announcements	Polls	Poll Comments	Documents & Document Comments (1. If the author specifies moderation on comment. 2. On a per document basis. 3. Notifications go to the space moderator.)	Discussions & Discussion Replies	Blogs	Blog Comments	Status & Status Comments	Avatar	Registration	Trackback	Profile Image	Private Messages
Space	S→G→F	S→G→F	⊘	S→G→F	S→G→F	S→G→F	S→G→F	⊘	⊘	⊘	⊘	⊘	⊘
Open & Member Group	G→F	G→F	⊘	G→F	G→F	G→F	G→F	⊘	⊘	⊘	⊘	⊘	⊘
Private & Secret Group	X	X	⊘	X	X	X	X	⊘	⊘	⊘	⊘	⊘	⊘
Your Personal Content	⊘	G→F	⊘	Visibility:Open G→F Otherwise X	X	G→F	G→F,B	[3]G→F	⊘	⊘	⊘	⊘	⊘
Root Container	G→F	G→F	⊘	⊘	⊘	G→F	G→F	G→F	G→F	G→F	G→F	G→F	G→F
Project in a Space or Group	I	I	I	I	I	I	I	⊘	⊘	⊘	⊘	⊘	⊘

1 Notifications for avatar moderation appear in the Admin Console
2 Notifications for registration moderation appear in Actions→Alerts
3 Status and Status Comments are not moderated in v 5.0.2 or earlier

F = Full Access (user is a community/system administrator)
S = Space Moderator
G = Global/Root Space Moderator
B = Blog Author

I = Inherited from parent space
X = Not moderated
⊘ = Cannot create in that container
→ = Order of moderation notification

For Jive 5.x

Common Moderation Scenarios

This table highlights the most common moderation scenarios. These scenarios may differ depending on your settings. Keep in mind that a project inherits the moderation settings of its parent place. Sub-spaces inherit the moderation settings of their parent space. Groups are moderated by the root space moderator.

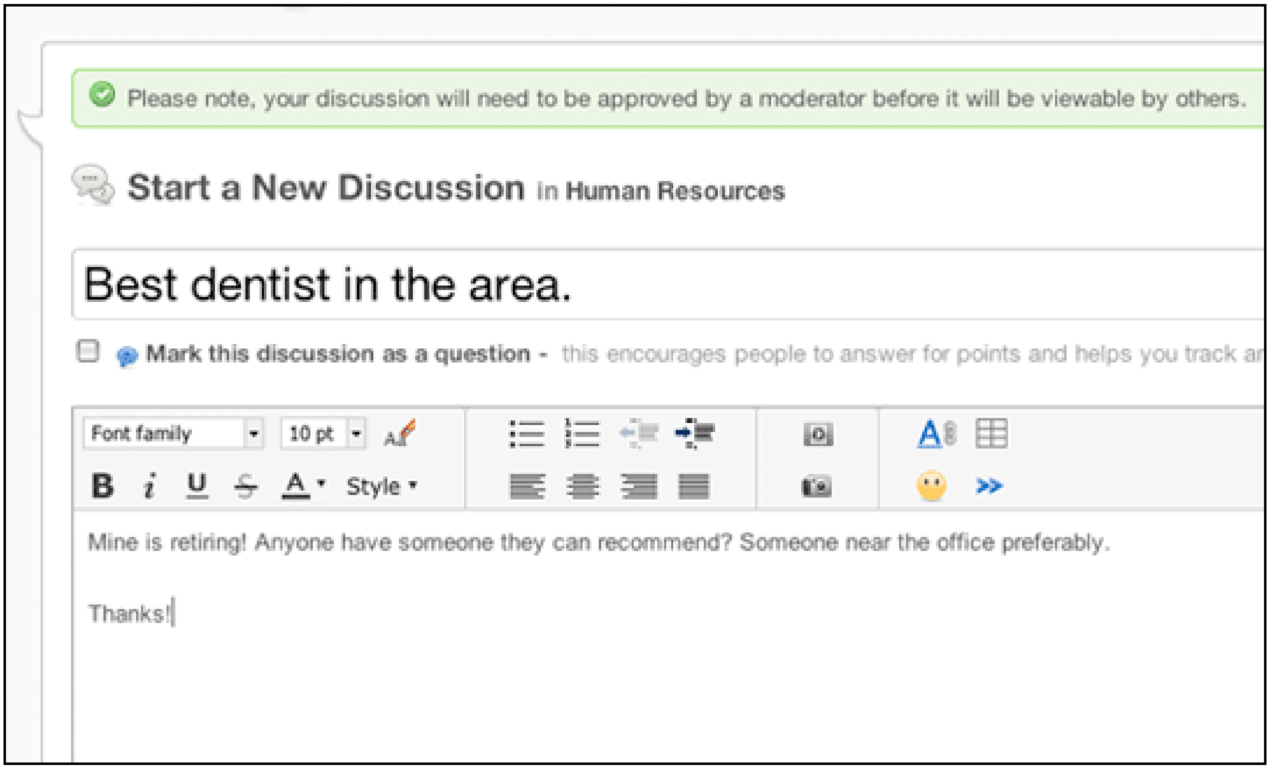
	Space	Social Group	System
Who moderates?	Space Moderator or System Moderator if no Space Moderator is defined	System Moderator (Abuse reports for open or member-only social groups go to the System Moderator, but to the System Admin for private or secret social groups. Private or secret social groups cannot have content moderation.)	System Admin
Where is the moderation notification received?	What Matters: Actions, under the Moderation tab	What Matters: Actions, under the Moderation tab	What Matters: Actions, under the Moderation tab. Exception: Notifications for avatar moderation appear in the Admin Console
Where is the content author notified when their content is approved?	What Matters: Actions, under the Notifications tab	What Matters: Actions, under the Notifications tab	What Matters: Actions, under the Notifications tab
Where is the content author notified when their content is rejected?	What Matters: Actions, under the Notifications tab	What Matters: Actions, under the Notifications tab	What Matters: Actions, under the Notifications tab
Where does moderation take place? (Front end or the Admin Console?)	Front end	Front end	Front end, except moderation of avatars takes place in the Admin Console

Reviewing Moderation Requests

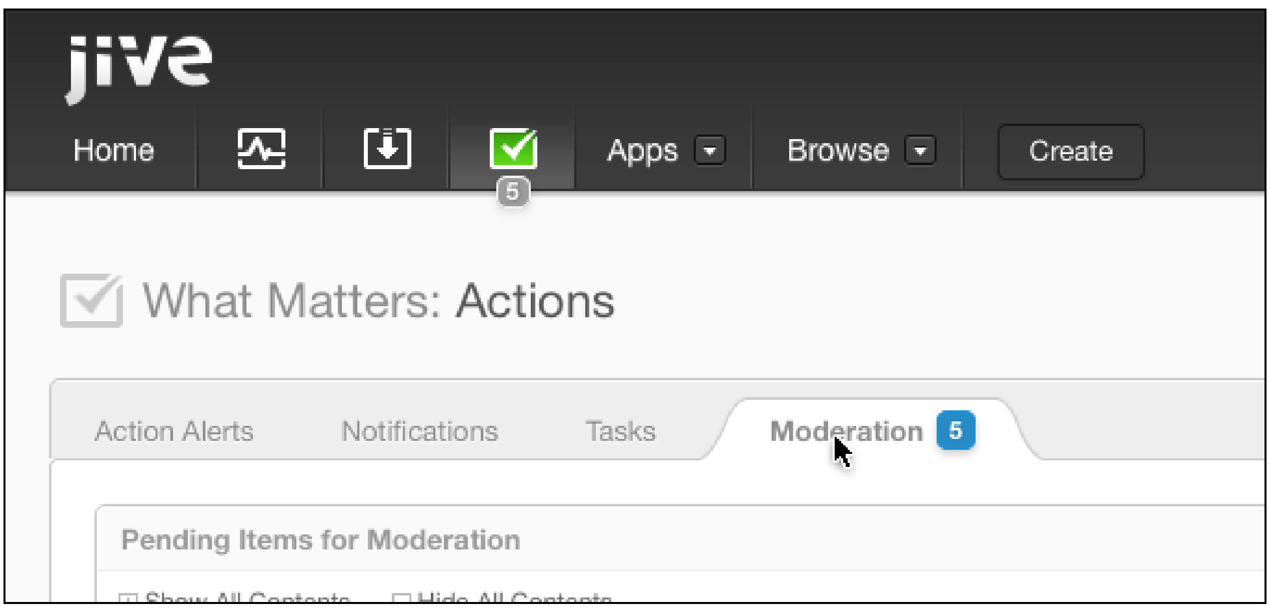
If you are a moderator, you'll have access to a list of requests for moderation. A request for content moderation will be sent to your moderation queue for approval before the content is published for others to see in the place. (Your community administrator sets up moderators for places. For more about that, see *Setting Up Moderation*).

For example, when discussion posts are enabled for moderation in a place, the author will see a message indicating that the post must be approved before it is published. The author can still access the submitted content by going to **Browse** > **Content** > **Drafts**, where they can continue to make changes and resubmit. When an author revises a draft that has already been submitted for moderation, the moderator must moderate each saved version individually.

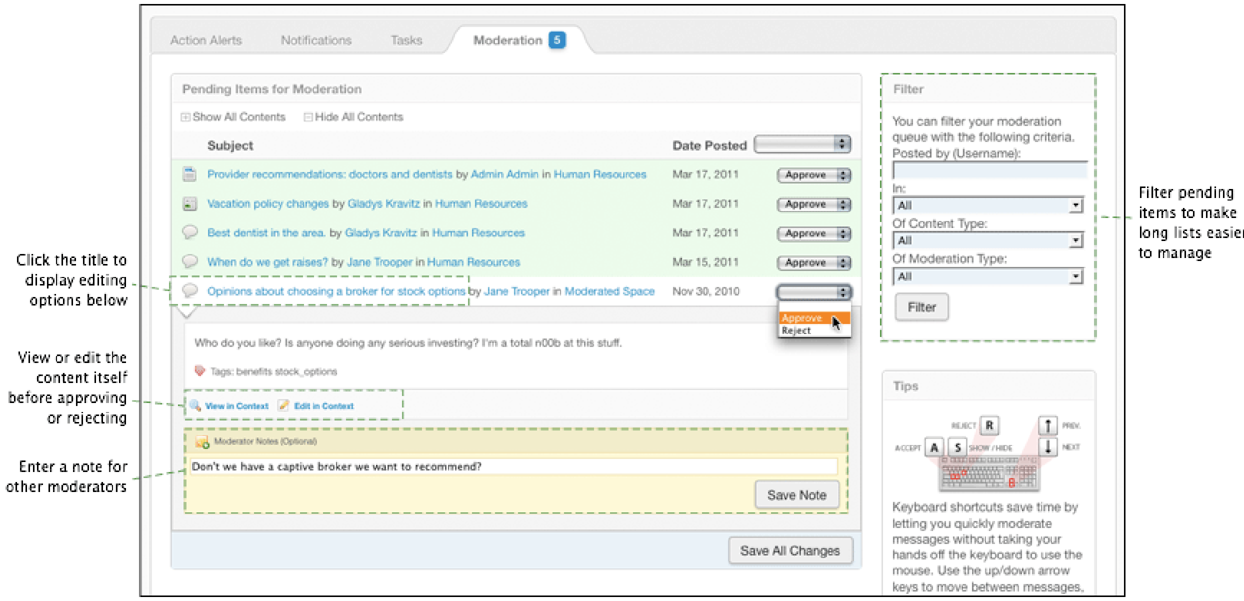
Here is what the author will see when submitting content for moderation:



After the author submits the post, you'll see an alert on your Actions icon. Go to **Actions** > **Moderation** to view the content.



If you have more than one item awaiting moderation, you'll see a list on the **Actions** > **Moderation** tab. For example, you might see content that's been reported as abusive, as well as content that's been submitted for moderation, depending on the moderation features set up by the community administrator. The following example shows a variety of items awaiting moderation:



Notice that at the right side of the page, you can filter the content listed. Filtering can be helpful when you've got a very long list. To moderate, simply take a look at each item and make a decision to:

- **Approve the content.** This will publish the content in the community.
- **Edit the content.** You'll be taken to the content editor to make changes.
- **Reject the content.** This will make the content invisible to users. Other moderators will still be able to view it. If you reject content, its author will be notified via email. You can edit the template content of this email -- see *Managing Email Templates* for more information. When you reject a discussion reply, the individual reply is hidden, but its parent and children remain visible.
- **Leave a message.** This message is for other moderators; it is not displayed to regular users. For example, you might explain to another moderator why you think the content should be approved or rejected. Moderator notes are not preserved after the content has left the moderation queue (because, for example, the content was approved).

Setting Up Content Moderation

How you set up moderation depends on the content type(s) and place(s) you want to moderate.

Caution: Private content cannot be moderated. This includes content created in private groups, secret groups, private discussions, and Your Documents that have visibility limited to the author or specific users.

Setting Up Moderation in a Space, Project, or Group

Note: A sub-space inherits the moderation settings of its parent space. A project inherits the moderation settings of its parent space or group. If you try to change the moderation settings of a sub-space or project, you will break the moderation settings of its parent. Social groups are moderated by the root space moderator.

1. Go to **Admin Console: Spaces** > **Settings** > **Moderation Settings**.
2. Click **Change space** and select the space in which you want to enable moderation.
3. Select the content type(s) you want to moderate in the space, for example, announcements, polls, documents, blog posts, and so on. You can choose one, several, or all. (All content types will go to the moderator(s) you designate. In other words, you can't have Joey moderate documents and Dee Dee moderate blog posts in the same space).
4. Click **Save changes**.
5. Go to **Permissions** > **Space Permissions**, and select the same space.
6. Click **Create a user override**, select the user(s) you want to be moderator(s), and then click **Set exception**. Select **User can manage space** > **Moderate**. You could also set a whole group as the moderators by clicking **Add group**, selecting the group, setting the permission level to **Moderate**, and then **Add Group**.

Setting Up Blog Moderation

You can set up blog *post* moderation by following the instructions above in "Setting Up Moderation in a Space, Project, or Group" and selecting the content type "blog posts" from the **Admin Console: Spaces** > **Settings** > **Moderation Settings** page. All system, social group, and personal blog posts are moderated from the root space; space and sub-space blog posts will go to the parent space moderator. A project in a space or group inherits the moderation settings of its parent.

Blog *comment* moderation is set up by the blog's author for every kind of blog (system-level, space, project, group, and personal blogs). Blog owners set up moderation for a blog's comments on the blog's **Blog Management** > **Options** page. System administrators can also moderate blog comments for system, social group, and personal blogs from the admin console **Blogs** > **Management** > **Comments** page.

Setting Up Document Comment Moderation

Document comments can be moderated. This includes comments for all documents created in all places and Your Documents. The author enables moderation when creating or editing a document, and selecting **Collaboration Options** > **Comment Policy** > **Moderated (Non-Authors comments will require approval)**. To understand who will moderate the document's comments, refer to the chart in *Who Moderates What*.

Moderation of Your Documents

If a user sets the visibility of a document saved in Your Documents to **Open to anyone**, and the root space has moderation enabled, the document will be moderated by the root space moderator.

Moderation: Frequently Asked Questions

Answers to frequently asked questions about moderation.

Can I moderate the creation of social groups?

There is no specific setting to set up moderation for the creation of social groups. However, you can implement a workaround by limiting the permissions of group creation to one group. Users would then have to request the creation of a new social group from the group with permission.

How is social group moderation different from space moderation?

Social groups are contained by the root space, so if you enable moderation in them, moderation requests are sent to the root space moderator's queue.

How does moderation inheritance work?

A sub-space inherits the moderation settings of its parent space. A project inherits the moderation settings of its parent space or group. If you try to change the moderation settings of a sub-space or project, you will break the moderation settings of its parent. Social groups are moderated by the root space moderator.

Who can moderate document comments?

To understand who will moderate a document's comments, refer to the chart in *Who Moderates What*. A document's author enables comment moderation on a document when creating or editing a document (the author would select **Collaboration Options** > **Comment Policy** > **Moderated**). Note that administrators cannot set batch moderation for all document comments; it must be set by the author each time a document is created or edited.

Who can moderate blog comments?

The blog's owner can enable comment moderation from the blog's home page by clicking **Manage** > **Options** > **Comments** > **Hold comments for approval**. Community administrators can also moderate blog comments from the admin console (**Blogs** > **Management** > **Comments**).

How do I moderate any item containing a specific word?

We recommend setting up a keyword interceptor. For information, see *Configuring Interceptors*.

If a space has moderation enabled, but no moderators are specified, who would get moderation notifications?

The community administrator, who has full access permissions. See the chart in *Who Moderates What* to understand how the application notifies moderators.

How are moderators notified that they have content pending moderation?

The alerts displayed on the What Matters: Actions icon show the number of unacknowledged action alerts, including moderation requests. Moderation requests are shown on the Moderation tab. To understand the process flow of moderation, see *Reviewing Queued Moderation Requests*.

I set a document to be editable only by me. Can a moderator edit this document?

Yes. Moderation is determined by place. So, if you create a document in a space, project, or group with moderation enabled, the moderator can edit any and all documents submitted for publication in that place.

Why did a document I saved under Your Documents get moderated?

Your community administrator has enabled moderation for documents created under Your Documents that have visibility set to **Open to anyone**. If you had set visibility to only certain users or only yourself, the document would not have been moderated.

What happens if I move moderated content?

If you need to move content between a place that's moderated and one that's not, or vice versa, be aware of the following:

- If you move content from a social group to a space and both are moderated, posts still awaiting moderation will be moderated as group content. New posts will be moderated as space content.
- If you move content from a moderated place to an unmoderated one, posts that were already awaiting moderation will remain in moderator queues, but the content will appear to community users as if it were already approved.

Managing Permissions

A system admin can grant permissions to users for access to content and administrative features.

When assigning permissions, you follow these basic steps:

1. *Create user groups* that capture how you want to grant access to the community's features. Each user group you create can represent a different category of people, from a permissions perspective. You might have user groups for administrators, managers, moderators, bloggers, people in the HR department, people in the Products department, and so on. You create user groups based on how you want to structure access to your community's features.
2. *Add user groups* to the different areas in the Admin Console: administration, spaces, social groups, blogs, and home page. For each group you add, assign permissions that capture that group's access.
3. Assign permissions in one of the following ways:

    - **Assign a permission level.** For *administrative permissions* and in *spaces*, you can use permission levels to assign bundled access permissions. You can also create your own space permission level.
    - ***Assign one or more access permissions*.** For blogs, social groups, and the rest, you work in a more a la carte way, assigning access by choosing from a list of usually fine-grained options.

- ***Create a user override for special cases*.** For example, you might want all but one or two people in a particular user group to have the permissions you assigned to the group. For those one or two, you can create a user override that assigns specific exceptions.

Permission Areas

Permission areas represent a mix of roles, places, and content types. Each permission area exposes its own set of permissions that are based on what you can do in the area. When you add user groups to an area, you assign access from among the permissions that the area offers. The pernission areas include:

- **Administrative** -- administrative and moderation permissions through which people have access to system-wide settings. Most of these provide access to the Admin Console. With the exception of the Full Access permission level, these don't provide access to content.
- **Space** -- per-space permissions for administering or moderating the space, as well as for working with content there.
- **Blog** -- permissions related to global blogs (such as system and personal blogs) to view and create blogs, comment on global blog posts, and so on.
- **Social group** -- permissions to view and create social groups, as well as work with attachments and images in content there.
- **Home page** -- permissions to create and interact with content that can appear on the communities home page and in the user container, including announcements, polls, and videos, and updates.
- **Mobile** -- permission to access the community from a mobile device, such as an iPhone.

For two of the areas -- administrative and space permissions -- the permissions are bundled into permission levels to make managing permissions for the area easier. In both of these areas, communities tend to set permissions along a similar set of themes. The permission levels are designed to reflect those themes.

Note: You can't break out the bundled permissions in the administrative area as you can with space permissions.

Keep in mind that there are a few exceptions in the permissions model. For example, the "blogs" area applies only to global blogs, such as system blogs and personal blogs (neither of which belong, strictly speaking to a place). This leaves out blogs in spaces, social groups, and projects, whose permissions are managed in different ways as described in *Managing Blog Permissions*.

Defining User Groups

Define a set of user groups that reflect the kinds of access you'll be granting. These groups can be defined in an external user identity system (such as an LDAP system) or in the application database. These groups provide a convenient, built-in way to manage a people's access to application features.

System-Defined User Groups: Everyone and All Registered Users

The application includes two groups that are defined by the system: Everyone and All Registered Users. These are a good place to start when managing permissions that are in effect across the community. After you've figured out how permissions should be applied for these broad groups, you can start assigning permissions based to user groups you create.

Note: Configuring permissions on the Everyone group is reserved for administrators of public communities. Administrators of internal communities, which are typically not licensed to permit public access to content, are not allowed to modify permissions on the Everyone group.

- **Everyone** includes anyone who visits the site, including anonymous users. Think hard about what you want people to be able to do anonymously, but weigh that against the need to engage people to encourage them to participate. (Note that users who merely view content are not counted among the number of users your license provides for.)
- **All Registered Users** includes people who have entered registration information and logged in for access. Use this group when you want to ensure certain kinds of access go only to people who have an account on the system.

Your User Groups

Your user groups will reflect your community's organizational groups. They could be relatively few, with separate groups for those who manage, moderate, and administer the community. They could also be many, with groups representing departments of a company, people with specific privileges (such as blogging), virtual teams within the organization, and so on.

For more on creating and managing groups, see *Managing User Groups*.

Setting Permissions

You can set permissions in the Admin Console on each permissions page.

1. On the page, under **Groups with access**, assign permissions to user groups:
   - To assign permissions to a user group not yet added:
     1. Click **Add group**.
     2. Enter the name of the user group to add.
     3. Click the **Select Permissions** button.
     4. In the dialog box, select the permissions you want to apply for the user group.
   - To edit permissions for a user group already added:
     1. Locate the group in the list.
     2. Next to its name, click **edit permissions**.
     3. In the dialog box, select the permissions you want to apply for the user group.
2. Click the **Set Permissions** button.

Creating User Overrides

For those cases, when there are exceptions to the rules you've defined, you can create user overrides. User overrides provide a user-by-user way to express those exceptions. You might be further limiting the user's access, but you could also be broadening it, such as to lend an administrative flavor to the user's access.

Create a user override to grant a particular set of permissions to an individual. You might need to create an override if:

- A person requires a particular set of permissions for an area, but isn't (and shouldn't be) a member of a group to which you've already assigned permissions for the area.
- A person is a member of a group to which you've assigned permissions for an area, but they require a different set of permissions than they've received as a member of the group -- in other words, they're an exception to the rule. For example, you might want to separately define their permissions in order to enhance or limit their access in the area.

Use the following steps to create a user override on the permissions page you're editing:

1. Under **User Overrides**, click **Create a user override**.
2. In the box, start typing the name of the user for whom you want to set the override. Click the popup that displays the user's name.
3. Click the **Set override** button to view the permissions you can set.
4. In the permissions dialog for the person you selected, select and clear check boxes as needed. In the end you want the list of checked items to reflect the permissions the person should have. Note that you merely clear a check box to remove a permission -- there's no need to explicitly revoke the permission.
5. Click **Set Permissions** to save the override you've created.

Managing System Administration Permissions

System Administration permissions give designated users the ability to keep the application running. Assign these permissions to delegate behind-the-scenes work. A user with system administration permissions can:

- Make configuration changes to the system

- Manage spaces
- Manage user accounts and user groups

Fastpath: Admin Console: Permissions > System Administration Permissions

About System Administration Permission Levels

System Administration permission levels represent sets of permissions designed to support specific types of administrative work in the application.

Note: You can only use the following standard permission levels for system administration permissions.

Permission	Description
Full Access	Gives control over every facet of the system. This level should only be assigned to users who are cleared to administer the system from a technical standpoint. It also gives access to view and administer all content in the system. **Full access supersedes all other permissions at the space level and beyond. In other words, with full access, a person can do anything in the application whether or not they're explicitly granted permission to do it.**
Manage System	Similar to Full Access, the Manage System permission level grants control over all technical aspects of the Admin Console. However, unlike Full Access, it does not automatically grant access to all community content. If your system has content in spaces that should be kept confidential, grant this permission to technical administrators instead of Full Access.
Moderate Content	Provides the ability to moderate social group content as well as perform global moderation duties across all spaces. Does not provide Admin Console access. When this level is granted to a group, all moderated content will pass through their queue before it appears in the community. For more about moderation, see *Moderating Content*.
Manage Users	Grants access to manage the users of this application. For more on managing users, see *Managing User Accounts and User Groups*.
Manage Groups	Grants access to create and manage user groups, such as for assigning permissions. For more on groups, see *Managing User Accounts and User Groups*.

How Permission Levels Affect Your Access

Administrative permission levels determine access to the Admin Console. For example, a user who has been assigned the "Manage Users" level wouldn't typically need access to system-related areas of the console other than those for managing user accounts.

The following tables lists sections of the console, showing what users at different permission levels can see. If all pages in a section are the same, then you'll only see the section.

Table 1. Overview Section

Console Page	Full Access	Manage System	Manage Space*	Manage Users	Manage All User Groups	Manage Particular User Groups**
Overview	✔	✔	✔	✔	✔	✔

Table 2. System Section

Admin Console Page	Full Access	Manage System	Manage Space*	Manage Users	Manage All User Groups	Manage Particular User Groups**
Management (all pages)	✔	✔	🛇	🛇	🛇	🛇
Settings (all pages)	✔	✔	🛇	🛇	🛇	🛇
Plugins (all pages)	✔	✔	🛇	🛇	🛇	🛇

Table 3. Spaces Section

Console Page	Full Access	Manage System	Manage Space*	Manage Users	Manage All User Groups	Manage Particular User Groups**
Management (all pages)	✔	🛇	✔	🛇	🛇	🛇
Settings						
Space Settings	✔	🛇	✔	🛇	🛇	🛇
Discussion Settings	✔	🛇	✔	🛇	🛇	🛇
Document Settings	✔	🛇	✔	🛇	🛇	🛇
Moderation Settings	✔	🛇	✔	🛇	🛇	🛇
Abuse Settings	✔	🛇	✔	🛇	🛇	🛇
Community Everywhere	✔	🛇	✔	🛇	🛇	🛇
Thread Archive Settings	✔	🛇	✔	🛇	🛇	🛇
Extended Properties	✔	🛇	✔	🛇	🛇	🛇
Filters and Macros	✔	🛇	✔	🛇	🛇	🛇
Gateway Settings	✔	🛇	🛇	🛇	🛇	🛇
Interceptors	✔	🛇	🛇	🛇	🛇	🛇

Table 4. Blogs Section

Console Page	Full Access	Manage System	Manage Space*	Manage Users	Manage All User Groups	Manage Particular User Groups**
Management (all pages)	✔	✔	🛇	🛇	🛇	🛇
Settings (all pages)	✔	✔	🛇	🛇	🛇	🛇

Table 5. People Section

Console Page	Full Access	Manage System	Manage Space*	Manage Users	Manage All User Groups	Manage Particular User Groups**
Management						
User Search	✔	✔	⊘	✔	✔	✔
Create User	✔	✔	⊘	✔	⊘	⊘
Group Summary	✔	✔	⊘	⊘	✔	✔
Create Group	✔	✔	⊘	⊘	✔	⊘
User Relationships	✔	✔	⊘	✔	⊘	⊘
Settings						
Avatar Settings	✔	✔	⊘	⊘	⊘	⊘
Ban Settings	✔	✔	⊘	⊘	⊘	⊘
Password Reset	✔	✔	⊘	⊘	⊘	⊘
Forgot Username	✔	✔	⊘	⊘	⊘	⊘
Login Security	✔	✔	⊘	⊘	⊘	⊘
Profile Settings	✔	✔	⊘	✔	⊘	⊘
Registration Settings	✔	✔	⊘	⊘	⊘	⊘
Status Level Settings	✔	✔	⊘	⊘	⊘	⊘
User Data Synchronization Settings	✔	✔	⊘	⊘	⊘	⊘
User Relationship Settings	✔	✔	⊘	⊘	⊘	⊘
Profile Image Moderation	✔	✔	⊘	⊘	⊘	⊘
Delegated Authentication	✔	✔	⊘	⊘	⊘	⊘
Terms and Conditions	✔	✔	⊘	⊘	⊘	⊘
User Status Settings	✔	✔	⊘	⊘	⊘	⊘
Single Sign On	✔	✔	⊘	⊘	⊘	⊘

Table 6. Permissions Section

Console Page	Full Access	Manage System	Manage Space*	Manage Users	Manage All User Groups	Manage Particular User Groups**
System Administration	✔	✔	⊘	⊘	⊘	⊘
Space Permissions	✔	✔	✔	⊘	⊘	⊘
Space Permission Levels	✔	✔	✔	⊘	⊘	⊘
Blog Permissions	✔	✔	⊘	⊘	⊘	⊘
Home Page Permissions	✔	✔	⊘	⊘	⊘	⊘
Mobile Module Permissions	✔	✔	⊘	⊘	⊘	⊘

Table 7. Reporting Section

Dashboard						
Tags	✔	✔	✔	✔	✔	⊘
Third-Party Integration	✔	✔	⊘	⊘	⊘	⊘

Setting Administrative Permissions

You can set administrative permissions on the System Administration Permissions page in the Admin Console.

Fastpath: Admin Console: Permissions > System Administration

1. In the Admin Console, go to the **System Administration Permissions** page.
2. To assign permissions to a user group not yet listed:
    a. Click **Add group**.
    b. Enter the name of the user group to add.
    c. Click the **Select Permissions** button.
    d. In the **System Administration Permissions for <user_group>** dialog box, select check boxes for the permission levels you want to apply for the user group.
3. To edit permissions for a user group already listed:
    a. Locate the group in the list.
    b. Next to its permission level, click **edit permissions**.
    c. In the **System Administration Permissions for <user_group>** dialog box, select check boxes for the permission levels you want to apply for the user group.
4. Click the **Set Permissions** button.

Managing Space Permissions

Spaces are places where users can create content such as documents, discussions, and blog posts just like in social groups, but whether you can create content or manage spaces is controlled by permissions. Permissions for social groups are controlled by adding a user to a user group or creating user override for them.

You can assign space permissions to control whether users can manage the space and how they can access content types within the space. Generally speaking, you assign permissions to user groups, and then create exceptions as needed by overriding permissions for particular users.

Note: Before assigning permissions, be sure you're familiar with permission levels and how to customize them. For more information, see *Managing Space Permission Levels*.

At a high level, setting space permissions typically includes these steps:

1. Create user groups that capture how you want to grant access to the community's features.
2. Set default space permissions. These should represent the access you'll most commonly want to provide for new spaces in the community.
3. As you add spaces, decide how to handle setting permissions for each. When someone creates a space, their options typically are:
    - Inherit from the parent space
    - Start with the parent space's permissions, then customize
    - Start with the default space's permissions, then customize
    - Start from scratch (no permissions assigned), then customize

Note: Permissions in spaces are inherited by projects and space created inside them. Social groups, on the other hand, are independent of spaces and projects. For more, see *Managing Social Group Permissions*.

How a New Space Inherits Permissions

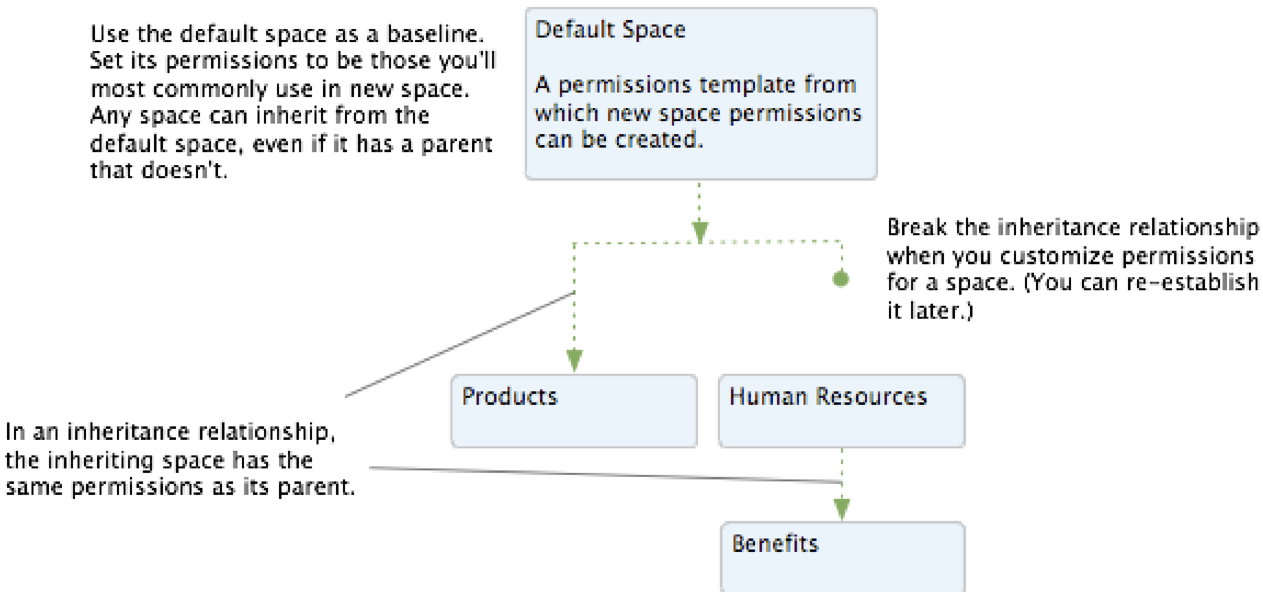
To make managing space permissions easier, an inheritance model provides a way to avoid (when you can) setting specific minute permissions for each new space. Spaces can inherit permissions from their parent or merely use those permissions as a starting point.

As you might expect, the inheritance relationship means that changes to the inherited space's permissions are automatically also changes to permissions in inheriting spaces. A *default space* is provided as a starting place for new spaces regardless of where they are in the hierarchy. While not actually a space in other respects -- it can't contain content -- the default space is useful as a permissions template.

Note: The Admin Console will provide cues about inheritance for a particular space, such as by noting how many spaces inherit permissions from it.

Here are a few important inheritance characteristics to keep in mind when working with the permissions model:

- You can customize the default space permissions to represent a permission set that will be commonly used when creating new spaces. And new space can use these, if only as a starting point.
- A space can inherit its parent space's permissions, a relationship that must be broken before the sub-space's permissions can be customized. For spaces at the top level, the default space is the parent space.
- At any point after a space is created, you can re-establish an inheritance relationship between it and its parent space. When you do, you remove any customizations you've made to permissions in the sub-space (and, of course, in space's that inherit from the sub-space).
- A new space can begin with its parent space's permissions as a starting point only. When it does, those permissions aren't inherited, instead providing a basis for customization.
- A new space can begin with the default space's permissions as a starting point, regardless of where the new space is in the hierarchy.
- A new space can begin with no permissions set, a blank slate that you customize.



Using and Customizing the Default Space

The default space contains all of the community spaces and it is designed to be a community-wide template for setting permissions in new spaces. When new spaces are created, their permissions can be based on the default space's, if only as a starting point to customize.

Customizing Default Space Permissions

You can customize the default space, setting commonly-used permissions that will make sense for new spaces to have.

Fastpath: Admin Console: Permissions > Space Permissions

1. In the Admin Console, on the **Space Permissions** page, click **Edit default space permissions**.
2. Configure the permissions for user groups or individual users in the default space.

Setting Permissions for Spaces

You set permissions for a space by adding a user group, then assigning a permission level to the group. Users in that group will have the permissions in the level you assigned. You can edit space permissions in the Admin Console.

Fastpath: Admin Console: Permissions > Space Permissions

To set permissions for a space:

1. In the Admin Console, go to the **Space Permissions** page.
2. Under **View and edit a space's permissions**, type or browse for the name of the space you want to set permission for.
3. On the page describing permissions for the space, assign permissions to user groups.
4. To assign permissions to a group not yet listed:
    a) Click **Add group**.
    b) Enter the name of the group to add.
    c) Select a permission level from the dropdown.
    d) Click the **Add Group** button.
5. To edit permissions for a group already listed:
    a) Locate the group in the list.
    b) Next to its permission level, click **edit**.
    c) Select a permission level from the dropdown.
    d) Click **Save**.

Creating User Overrides for Spaces

Create a user override to grant a particular set of permissions to an individual. You might need to create an override if:

- A person requires a particular set of permissions for an area, but isn't (and shouldn't be) a member of a group to which you've already assigned permissions for the area.
- A person is a member of a group to which you've assigned permissions for an area, but they require a different set of permissions than they've received as a member of the group -- in other words, they're an exception to the rule. For example, you might want to separately define their permissions in order to enhance or limit their access in the area.

Use the following steps to create a user override on the permissions page you're editing:

1. Under **User Overrides**, click **Create a user override**.
2. In the box, start typing the name of the user for whom you want to set the override. Click the popup that displays the user's name.
3. Click the **Set exception** button to view the permissions you can set.
4. In the Set Exception dialog, select the access and content type permissions.
5. Click **Save**.

What are Space Permission Levels?

Permission levels are specific permissions for content types and administrative roles grouped into one. The application includes several standard permission levels, and you can create your own custom ones. When you assign permissions to groups for access to a space, you should assign levels, and then customize as needed with overrides for particular users.

When working with space permissions, you can assign access to the space as a whole, or assign access to particular kinds of content in the space by creating a Custom permission level.

Standard permission levels	Capture how users can access space features at a high level, each bundling fine-grained access to content or administrative roles along a particular theme. The application comes with several predefined levels designed to reflect common roles, including a space

	administrator, a moderator, a user who can only view content, and so on. See the section on standard permission levels for more on included levels. You can also create your own levels.
Custom permission levels and User Overrides	Bundle fine-grained access to a particular content type. You use content-based permissions when creating your own permission level or overriding permissions for a certain user. For example, you might create a custom level in which people can create new discussion posts, but only comment on documents (rather than create them).

Note: Permissions in spaces are inherited by projects created inside them. Social groups, on the other hand, are independent of spaces and projects. For more, see *Managing Social Group Permissions*.

Standard Space Permission Levels

The application includes several default space permission levels. Designed to meet common permissions needs, these are worth a look if you're starting from scratch (or even revising what you've got). As described below, you can also add your own levels.

Note: To see the list of space levels in the Admin Console, go to the **Permissions** > **Space Permissions Levels** and then click the **Standard Levels** tab.

The following table lists the standard space permission levels, along with a summary of the access granted by each. See the table later in this section for details on specific permissions granted by each.

Table 17: Levels Described

Space Permission Level	Access Granted
Administer	Design the space layout, read and write for all content types, delete (but NOT edit) comments, assign permissions to users and user groups, delete the space.
Moderate	Read and write all content types, edit other people's content.
Create	Read and write all content types.
Contribute	Comment on commentable content types, as well as reply to discussion threads.
View	View content.
Discuss	Read/write discussions, contribute on all other content types.
No Access	Only applicable when creating a user override. Use this to prevent access to the space and no entitlements are set.

The following table lists each default space permission level, along with the specific permissions granted by each. As described in the section below, when you create a permission level, you can choose from among these.

Table 18: Access Granted for Each Level

Space Permission Level	View	Create	Reply	Comm	Attach file	Insert image	Rate	Vote	Create Projec	Create Annou	Edit Comm	Delete Comm	Moderate
Administer	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	No
Moderate	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Space Permission Level	View	Create	Reply	Comm	Attach file	Insert image	Rate	Vote	Create Projec	Create Annou	Edit Comm	Delete Comm	Moderate
Create	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	No	No	No
Contribute	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	No	No	No	No	No
View	Yes	No	No	No	No	No	No	No	No	No	No	No	No
Discuss	Yes	Yes	Yes	Yes	No	No	Yes	Yes	No	No	No	No	No

Custom Permission Levels and User Overrides for Spaces

When you create a custom permission level or a user override, you're in effect designing exceptions to existing rules. Those exceptions could replace permission levels included by default, permission levels you've created, or one-off overrides for particular users. For example, you might want to create a custom permission level for a group of people who should be the only ones to post to a space's blog. Or you might create a user override for a particular user who will be a space's administrator, managing its permissions, creating spaces beneath it, and so on.

When you create this kind of customization, your options are divided into three categories (described in detail below):

No access	Available for a user override only, this option lets you simply exclude a particular user from access to the space. This is designed as a user-by-user approach. To prevent access for a group of people instead, ensure that those people aren't included in groups that *do* have access. For example, to restrict access to a space that contains sensitive information, create a user group that contains people who should have access, taking care to leave out those people who shouldn't have it.
Access space	Available in custom permission levels and user overrides, this category provides fine-grained control with which you assign permissions specific to each content type. Want to create a permission level that grants access to create discussion threads but only view documents? This is what you want.
Manage space	Available in custom permission levels and user overrides, this category provides a way to create administrative roles for the space. Each space should have an administrator, even if that role is inherited from a parent space. But typically, the roles available in this category will go to very few people.

The following sections give details on the options available for each of the categories.

No Access

The user has no access to the space and won't be able to see content from it. Pretty straightforward.

Access Space

Use this category to craft custom content-specific access in the space. When you select this category while customizing, you have access to a list of the content types, each with a list of the access levels available for it. Choose an access level for each content type.

The following table lists the access levels that each content type permission level includes, along with the specific permissions each allows.

Table 19: Access Granted for Each Content Type Permission Level

Content Type Permission	View	Create	Reply	Comment	Attach file	Insert image	Rate	Vote
Create	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Create (for discussions)	Yes	Yes	Yes	Yes	No	No	Yes	Yes
Contribute	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes
View	Yes	No	No	No	No	No	No	No
Advanced	See the specifics below.							

The **Advanced** access level for each content type provides even finer-grained control of permissions for a content type. After you select **Advanced**, select check boxes for the permissions you want the customization to allow.

The following table lists what's available in the **Advanced** level for each content type.

Table 20: Access Settings Available for Each Content Type

Content Type	View	Create	Reply	Comment/ Reply	Attach file	Insert image	Rate	Vote
Document	Yes	Yes	No	Yes	Yes	Yes	Yes	No
Discussion	Yes	Yes	Yes	No	Yes	Yes	No	No
Blog Post	Yes	Yes	No	Yes	Yes	Yes	No	No
Poll	Yes	Yes	No	Yes	No	No	No	Yes
Video	Yes	Yes	No	Yes	No	No	Yes	No

The following are also available as "on or off" options.

Option	Access Granted
Create Project	Create a project in the space.
Create Announcement	Create an announcement in the space.

Manage Space

Use this category to assign administrative roles that are specific to the space. The following table describes the two access levels that are available.

Option	Access Granted
Full Control	Customize the space overview page, edit space details, delete any space content, create subspaces, manage permissions for that space, delete the space, create a category, and manage the space blog.
Moderate	Moderate and edit all content in the space. Selecting this option enables the moderation queue for all content in the space.

Full Control -- Someone with full control has access to administrative features for the space, along with any sub-spaces beneath it. A space administrator can create sub-spaces, set content defaults, and set permissions for the space. They can see content that is in a moderator's queue but hasn't been approved yet. They can even designate other space administrators.

Moderate -- Granting moderator permission gives someone two areas of access:

- A content moderator has access to certain links for handling content after it's published. Through these they can manage content by editing, moving, and deleting it as the need arises. For example, a content moderator might lock a discussion thread that is no longer useful or move a document to another space. These abilities are inherited by sub-spaces of the space in which the permission is granted.
- A content moderator can approve or reject content before it's published. When moderation is on for the context in which the content was created (such as the space, social group, or even globally), the content moderator for that context will be able to accept or reject the content in a moderation queue. Setting this up involves not only assigning content moderation permission, but also turning on moderation for those kinds of content you want moderated. This ability is not inherited in sub-spaces; the moderator can approve or reject content only in the context where they've been assigned permission.

Note that as a failsafe to ensure that moderated requests always have a place to go, new requests are routed in the following order:

1. If content would be moderated at the sub-space level but there's no moderator there, it goes to the system moderator's queue.
2. If content would be moderated at the system level but there's no moderator there, it goes to the system administrator's queue.

This applies to new requests only. For example, if a request is in the queue when moderators are removed, the requests will remain in the queue until someone approves or rejects them there. Existing requests won't be routed to the next queue up. If there's only one moderator and that person is deleted from the system, then requests currently in the queue will be orphaned even after a new moderator is assigned to that area. If moderation permissions are merely revoked (or un-granted) for someone, then that person will still have access to the requests currently in the queue but won't be able to approve or reject them.

Keep in mind that in order to have moderators approve and reject content in a moderation queue, moderation will need to be enabled for specific content types in the console at Spaces > Settings > Moderation Settings. For more on these, see *Choosing Content to Moderate*.

Creating a Custom Space Permission Level

You can create a custom space permission level that you can subsequently use when assigning permissions space by space. You might want to do this, for example, if you think you're going to be using a custom set of permissions in more than one space. If you'll use the customization only once, you might instead want to create a customization that you don't save as a custom level for use in other spaces.

Fastpath: Admin Console: Permissions > Space Permission Levels

To create a custom space permission level:

1. In the Admin Console, go to the **Space Permission Levels** page.
2. On the **Custom Levels** tab, click **Create new permission level**.
3. On the **Create a Custom Permission Level** dialog box, enter a name and description for the permission level. These will help other administrators know the new level's purpose.
4. Under **Access and administration,** select a category for the level, then choose from among the options in the category.
5. Click **Save**.

Managing Blog Permissions

This topic describes the permission settings for global blogs -- that is, blogs that aren't associated with a particular place, such as a space. These include system blogs (which tend to represent the community as a whole) and personal blogs (which represent a particular community member).

Managing permissions for other kinds of blogs varies depending on what kind of place the blog lives in. The following table gives a brief description of each:

Table 21: Permissions Management for Non-Global Blogs

Blog Location	Permissions Management
Space	You manage permissions for blogs in a space when you manage permissions for the space. For more on space permissions, see *Managing Space Permissions*.
Social group	Access for blogs in social groups are always completely open. That is, if the social group's creator chose to allow a blog for the group, then anyone who's a member of the group can do all of the things there that are allowable for blogs (viewing, posting, and so on). For more information on social group permissions, see *Managing Social Group Permissions*.
Project	Blogs in projects inherit blog permissions from the place the project is in. In other words, a blog for a project in a space inherits blog permissions from the space. For more on space permissions, see *Managing Space Permissions*.

Note: You configure settings and membership for global blogs by using the Blogs tab of the Admin Console. For more information, see *Managing Blogs*.

About Global Blog Permission Levels

Blog permission levels enable people to read and edit global blogs.

Note: You can only use the following standard permission levels for global blog permissions.

Permission	Access Granted
View blog	View and read all public blog posts.
Create blog	Create/manage a personal blog, and author blog posts in it.
Comment	Leave comments on public blog posts.
Create attachment	Attach files to blog posts (Note: Requires the "Create Blog" permission to be effective).
Insert images	Insert images into blog posts (Note: Requires the "Create Blog" permission to be effective).

Setting Global Blog Permissions

You can set global blog permissions in the Admin Console on the Blog Permissions page.

Fastpath: Admin Console: Permissions > Blog Permissions

1. On the page, under **Groups with access**, assign permissions to user groups:
   - To assign permissions to a user group not yet added:
     1. Click **Add group**.
     2. Enter the name of the user group to add.
     3. Click the **Select Permissions** button.
     4. In the dialog box, select the permissions you want to apply for the user group.
   - To edit permissions for a user group already added:
     1. Locate the group in the list.
     2. Next to its name, click **edit permissions**.
     3. In the dialog box, select the permissions you want to apply for the user group.
2. Click the **Set Permissions** button.

Creating User Overrides for Blogs

Create a user override to grant a particular set of permissions to an individual. You might need to create an override if:

- A person requires a particular set of permissions for an area, but isn't (and shouldn't be) a member of a group to which you've already assigned permissions for the area.
- A person is a member of a group to which you've assigned permissions for an area, but they require a different set of permissions than they've received as a member of the group -- in other words, they're an exception to the rule. For example, you might want to separately define their permissions in order to enhance or limit their access in the area.

Use the following steps to create a user override on the permissions page you're editing:

1. Under **User Overrides**, click **Create a user override**.
2. In the box, start typing the name of the user for whom you want to set the override. Click the popup that displays the user's name.
3. Click the **Set override** button to view the permissions you can set.
4. In the permissions dialog for the person you selected, select and clear check boxes as needed. In the end you want the list of checked items to reflect the permissions the person should have. Note that you merely clear a check box to remove a permission -- there's no need to explicitly revoke the permission.
5. Click **Set Permissions** to save the override you've created.

Managing Social Group Permissions

Social groups are places where users can create content such as documents, discussions, and blog posts just like in spaces, but whether you can view, create or manage social groups is controlled by permissions. When you manage the permissions, you are managing what users and user groups can do to social groups and to content within them. For example, you may allow a user to create groups, insert images to content and create attachments to content.

Note: Projects created inside social groups use the same content types as the social group they belong to. For example, If your group only allows users to create blogs or discussions, a project under that group would only allow you to create blogs or discussions as well.

When you manage social group permissions, you decide how users and/or user groups can interact with social groups. They can do any combination of view and create groups, create attachments to content, and insert images. The group owner controls which content types are available for social groups when they create the group, or later when they manage it. For example, groups can have any combination of blogs, discussions, documents, and more.

About Social Group Permission Levels

Social group permission levels are designed essentially as a way to manage whether people can see or create social groups. A user with access to create a social group can set the group's level of access and which content types are allowed in the group.

Permissions for each content type in a social group, however, are not configurable. They're essentially unlimited (read, create, comment, attach file, etc.) Projects created inside a social group inherit these permissions.

Note: Be sure to select "View social group" when granting access to create groups. Without that permission, users won't be able to see aspects of the UI through which they can create groups.

The following table lists the permission levels provided for social groups.

Permission	Access Granted
View social group	See the group feature in the UI and read all visible social groups. This is a general visibility option for groups. In other words, it must be selected in order for uses to choose "Group" from the New menu in the end user UI.
Create group (public)	Create a new a public or members only social group.

Permission	Access Granted
Create group (private)	Create a new private or secret social group.
Create attachment	Add an attachment to content in social groups.
Insert images	Add an image to content in social groups.
Manage social group	Allows users to manage social groups.

Setting Social Group Permissions

You can set social group permissions in the Admin Console on the Social Group Permissions page.

Fastpath: Admin Console: Permissions > Social Group Permissions

1. On the page, under **Groups with access**, assign permissions to user groups:
   - To assign permissions to a user group not yet added:
     1. Click **Add group**.
     2. Enter the name of the user group to add.
     3. Click the **Select Permissions** button.
     4. In the dialog box, select the permissions you want to apply for the user group.
   - To edit permissions for a user group already added:
     1. Locate the group in the list.
     2. Next to its name, click **edit permissions**.
     3. In the dialog box, select the permissions you want to apply for the user group.
2. Click the **Set Permissions** button.

Creating User Overrides for Social Groups

Create a user override to grant a particular set of permissions to an individual. You might need to create an override if:

- A person requires a particular set of permissions for an area, but isn't (and shouldn't be) a member of a group to which you've already assigned permissions for the area.
- A person is a member of a group to which you've assigned permissions for an area, but they require a different set of permissions than they've received as a member of the group -- in other words, they're an exception to the rule. For example, you might want to separately define their permissions in order to enhance or limit their access in the area.

Use the following steps to create a user override on the permissions page you're editing:

1. Under **User Overrides**, click **Create a user override**.
2. In the box, start typing the name of the user for whom you want to set the override. Click the popup that displays the user's name.
3. Click the **Set override** button to view the permissions you can set.
4. In the permissions dialog for the person you selected, select and clear check boxes as needed. In the end you want the list of checked items to reflect the permissions the person should have. Note that you merely clear a check box to remove a permission -- there's no need to explicitly revoke the permission.
5. Click **Set Permissions** to save the override you've created.

Managing Home Page Permissions

Home page permissions enable you to manage global permissions for features such as polls and announcements on the community's home page, as well as manage permissions that fine tune the video and update features. The global permissions are not limited by any container.

The community's home page includes global permissions for actions like managing announcements, which is typically seen by everyone at one time or another. Often it's the place people stop first to get a snapshot of what's going on. Because it's so central, it's a great place to put things that should be visible to everyone. In other words, when setting permissions for the home page, keep in mind that you might want to offer some kinds of access to people who have an active role in the community as a whole, and some kinds more broadly. For example, a community manager could be given permission to create announcements. Other kinds of access, such as vote in polls or rating videos, might keep the community more active if they're more broadly granted. See About Home Page Permission Levels for the list of levels you can grant.

The video and update features include global permissions for actions like commenting on updates or videos. These permissions can be enabled or disabled for groups of users. You can customize permissions for groups of users in Home Page Permissions page of the admin console. See About Home Page Permission Levels for the list of levels you can grant.

About Home Page Permissions

Home page permissions enable global permissions for features that affect the application on a global level. These permissions enable people to create and interact with content that's displayed on the community's main page, or fine tune what users can do with updates in their personal containers and videos that they upload into the projects, spaces, or groups they belong to.

Note: You can only use the following standard permission levels for home page permissions.

Permission	Access Granted
Create announcement	Create announcements that appear on the main (and personalized) homepage.
Create poll	Create polls at the system level.
Vote in polls	Vote in polls created at the system level.
Create video	Create and upload videos in their personal containers.
Rate videos	Rate the videos that they can access.
Comment on videos	Comment on the videos that they can access.
Create and Repost updates	Create their own updates and repost someone else's update.
Like updates	Like someone's updates, which affects their status points.
Comment on updates	Comment on other users' updates.
View updates	Allows users to view updates that others post.
Insert update images	Add images to their update as an attachment.
Insert comment images	Add images to comments on updates.

Setting Home Page Permissions

You can set home page permissions in the Admin Console on the Home Page Permissions page.

Fastpath: Admin Console: Permissions > Home Page Permissions

1. On the page, under **Groups with access**, assign permissions to user groups:
    - To assign permissions to a user group not yet added:

    1. Click **Add group**.
    2. Enter the name of the user group to add.
    3. Click the **Select Permissions** button.
    4. In the dialog box, select the permissions you want to apply for the user group.
  - To edit permissions for a user group already added:
    1. Locate the group in the list.
    2. Next to its name, click **edit permissions**.
    3. In the dialog box, select the permissions you want to apply for the user group.
2. Click the **Set Permissions** button.

Creating User Overrides for Home Page

Create a user override to grant a particular set of permissions to an individual. You might need to create an override if:

- A person requires a particular set of permissions for an area, but isn't (and shouldn't be) a member of a group to which you've already assigned permissions for the area.
- A person is a member of a group to which you've assigned permissions for an area, but they require a different set of permissions than they've received as a member of the group -- in other words, they're an exception to the rule. For example, you might want to separately define their permissions in order to enhance or limit their access in the area.

Use the following steps to create a user override on the permissions page you're editing:

1. Under **User Overrides**, click **Create a user override**.
2. In the box, start typing the name of the user for whom you want to set the override. Click the popup that displays the user's name.
3. Click the **Set override** button to view the permissions you can set.
4. In the permissions dialog for the person you selected, select and clear check boxes as needed. In the end you want the list of checked items to reflect the permissions the person should have. Note that you merely clear a check box to remove a permission -- there's no need to explicitly revoke the permission.
5. Click **Set Permissions** to save the override you've created.

Managing User Accounts and User Groups

If you're a system admin, user admin, or group admin, you can use the admin console to add, remove, and edit accounts for users and groups.

Note that this guide does *not* describe how to set permissions for users and groups. You can set permissions if you're a system or space admin, but not a user or group admin. For more on setting permissions, see *Managing Administrative Permissions*.

About User Accounts and User Groups

User accounts represent people who have access to the application. User groups collect user accounts in order to make it easier to manage access to the application's features.

User Accounts and User Groups

A **user account** represents a person using the application. Each user account has associated content, including the person's profile. For all users, you can use the console to change their user name and password, view and delete the content they've created, and view and edit their profile information. You can also disable a user, such as when they're no longer involved, but you want to hang on to their content.

For more, see *Managing User Accounts*.

A **user group** collects user accounts, typically in order to make it easier to grant all of the collected users certain permissions. For example, you might create a group of human resources workers so that you can give them (and only them) permission to view potentially sensitive information about employees in a "Benefits" space. A user group is made up of members, who typically aren't aware they're in the group, and admins, who have admin console access through which they can manage user group settings and membership.

For more, see *Managing User Groups*.

External User Identity Systems

The work you do with user accounts and user groups will depend heavily on whether the application is connected to an external user identity management system. Generally speaking, when you add user accounts and user groups using the admin console, you're adding that data to the same database used to store content. This isn't typically the case if the application is connected to an external user identity system such as **LDAP or Active Directory**. In that case, much of the information about users will be coming from -- and managed within -- the external system.

By default, even if your community uses an LDAP or Active Directory database (or some custom solution), the users you add through the admin console will be added to the application's database and not the external system. It is also possible that user accounts will be managed by the external system, but the groups they're members of will be created and managed locally in the application database. How user group are managed is defined when the external system is connected to the application.

For information on connecting an external LDAP or Active Directory system, see the *LDAP and Active Directory Guide*.

User Registration

You can configure the application so that users can register on their own. When you enable user-created accounts, people can register by entering basic required registration information (such as a username and password), along with user profile information. They can also invite other people to join the community.

For information on configuring registration, see the *Configuring User Registration*.

Managing User Groups

A user group makes managing permissions easier by gathering users into one group. For example, you might create a user group called "hr_users" and add user accounts for people in the human resources department. The existence of user groups isn't visible in the application's user interface.

User groups are made up of members and admins. Unless they have access to the admin console, members typically aren't aware that they're in a user group. The account simply defines (at least partly) their access to the application's features. Group admins have access to the area of the admin console through which they can manage settings and membership for a group they're administering. By default, they get to this feature by directing their browser to a URL as described in *Starting the Admin Console*. Unless they have other types of admin access, they'll only be able to access account management pages for the account they're administering.

Be sure to see *Managing User Accounts and User Groups* for overview information on how accounts work.

Note that if your community uses an external database (such as LDAP or Active Directory) to manage user identities, you won't by default be able to use the admin console to edit information managed there. Also, it's possible for your community to use an external data store for user account information, but not for user groups (which you can instead create and manage with the admin console). For more information about using LDAP or Active Directory with Jive, take a look at the) *LDAP and Active Directory Guide*.

Fastpath: Admin Console: People > Management > Group Summary

Fastpath: Admin Console: People > Management > Create Group

Adding User Groups

You add user groups by creating and naming a group, then adding user accounts for each of the group's members. You also add one or more user accounts for those who'll be administrators for the account.

1. In the admin console, go to **People** > **Management** > **Create Group**.
2. Enter a group name. Choose something that will help you know at a glance what the group is for and who's in it. Add a description if you like. Create **Create Group**.
3. Use the Add Members links to add user accounts for people who should be members of the new group. For more information see Managing Group Membership.
4. Use the Add Admins links to add user accounts for people who will have permission to administer the account. For more information see Managing Group Membership.

Try defining user groups before launching the community. For example, you can group users according to employee job function or department. User and Group permissions can be assigned on a space or sub-space basis.

Note: If your user account and user group information is stored externally (such as in LDAP or Active Directory), new user groups you create will be managed in the admin console and stored in the local application database instead.

Tip: You can create user groups for testing, then add user accounts to the groups later.

Managing Group Membership

To edit the membership list for an existing user group

1. In the admin console, go to **People** > **Management** > **Group Summary**.
2. Click **Edit** next to the group from which you want to add or delete members.
3. Click **Edit** next to Admins or Members dependng on which you want to add or edit.
4. Add members to the group by typing their name in the Add Member box, then clicking the Add button. If you don't know the name, click User Picker to browse or search a list of users, then select the check box for the user you want to add. Unless they have access to the admin console, users won't know which user groups they're a part of.
5. Add administrators in the same way you add members. User group administrators have access to the portions of the admin console where they can manage settings and membership for the group they're administering.
6. Click **Update**.

Editing Group Settings and Properties

Group settings are simple, including the group's name and description, along with group properties. You can edit a group's settings in the admin console by going to the Group Summary page, then clicking the group's name.

Group properties are simple name-value pairs that programmers can use to work with the group in their code. Group properties are often used as a way to keep track of extra information about the group. For example, if groups are defined based on company departments, each could have a departmentID property whose value is the department's internal billing ID. A group can have multiple properties. When you're working with properties, remember that entering the name and value for an existing property will update that property's value to the one you entered.

Managing User Accounts

A user account represents a person using the application. Everything about a person's activity in the application is associated with their user account. From User Summary page, you can view user profile information, their activity (such as content they've posted), change their password, and disable/delete their account by clicking the appropriate links at the top of the page.

Fastpath: Admin Console: **People** > **Management** > **User Search** > **Edit User**

Be sure to see *Managing User Accounts and User Groups* for overview information on how accounts work.

If your community uses an external user identity system (such as LDAP or Active Directory) to manage user data, you won't by default be able to use the admin console to edit information managed there. Console fields corresponding to data in the external system will be disabled, and you won't be able to delete users from the admin console. (Typically, the external system stores profile information about the user, while information about their activity in the application is stored in the application database.)

For more information about using LDAP or Active Directory with Jive, take a look at the) *LDAP and Active Directory Guide*.

User Account Summary

The User Search page in the admin console shows all information for each user when you click **Edit**. Here you can get information and perform actions on the account. To get to this page, in the admin console go to the user Search page, then browse or search for the user's account. Click the user's name to view their user summary page.

Fastpath: Admin Console: People > Management > User Search

Profile Information

Among the user properties you'll see information that's part of the user's profile. Much of this is the same information that the rest of the community sees when they view the user's profile in the end user UI.

Password

You can change the password for a user account. Note that an administrator can configure the application to enable people to request their own password reset. If that feature is disabled, then you can reset the password from the User Summary page.

Note: The application doesn't send an email to the person whose password you changed when it's changed this way.

Enabled

You can disable a user account, removing their access but keep their content in the system. For more information, see Deleting and Disabling User Accounts.

User Activity in the Community

You can view lists of the documents, discussion messages, and blog posts that a person has contributed or worked on. The User Properties lists will display quantities for each, and you can view a list of the items themselves by clicking the name of the kind of item you want to view.

Visiblity Settings

You can choose whether or not a person's name and email address are visible to others in the community.

An administrator can configure the application so that a person can set the visibility of their own name and email address. If that's the case, then the user will be able to change the setting independently of the setting you make in the admin console. In other words, if you change it, they can change it back.

Group Membership

If the user account is a member of user groups, links to those accounts will be displayed among the user properties.

User groups are a way to collect user accounts to more easily manage user access and permissions. For more information about them, see *Managing Group Accounts*

Email Notifications

The User Properties list displays the number of email notifications the person is signed up for. To see a list of the notifications, click the number.

Avatars

If a person has uploaded their own avatars, their User Summary page will display the images they've uploaded. You can delete avatar images from this page.

For more on managing avatars, see *Avatar Settings*

User Properties

User properties are simple name-value pairs that programmers can use to work with the user account in their code. User properties are often used as a way to keep track of extra information about the user account. A user can have multiple properties. When you're working with properties, remember that entering the name and value for an existing property will update that property's value to the one you entered.

Creating User Accounts

When you need to create user accounts, you do so on the admin console's Create User page. By default, if your community uses LDAP or Active Directory to manage users, new user accounts you create from the admin console will go into the local application database (where content is stored). You will be able to edit user account properties for LDAP-managed users if your LDAP provider allows it (by default, it isn't allowed).

1. Navigate to Admin Console:**People** > **Management** > **Create User**.
2. On the Create User page, enter basic information, including user name, "friendly" name, email address, and password. You can also request to send the new user a welcome email. (For more on the template a welcome email is created from, see *Editing Email Notification Templates*.)

   Note: A user name may not contain any of the following characters: **, / ? & #**

3. To create this new account and edit its properties now, click the **Create User**. In general, you should edit properties for the user account while you're creating it. That's because the new account doesn't yet have permission to do anything in the community. For more about the user account properties, see .
4. To create this account and move on to creating another (without editing account properties), click the Create & Create Another User button.

Deleting and Disabling User Accounts

You can disable or delete a user account when you want to remove the person's presence from the community. You can disable or delete from the User Search page, where user accounts are listed.

Note: An administrator can also ban someone if you merely want to prevent their having access to the community. For more information about banning, see *Banning People*.

Disabling a user account removes their access but keeps their content in the system. When you disable someone's account, Jive will replace their former avatar with a blank avatar; the word "Disabled" will appear on their profile. The person will no longer be able to log in or receive notifications, but their content will remain viewable in the application.

Deleting a person's user account also deletes the content they've contributed. This is a permanent action that, depending on the user's amount of activity, can have an impact on content throughout the community. If you're not sure whether you want to delete the account, consider banning or disabling the user instead.

When you delete a user account, you begin the deletion by clicking the link. However, the actual deletion might take a few minutes to finish, depending on how much content is associated with the account.

Caution: Deleting someone's account is permanent. You'll be deleting everything about the user's presence in the system. This includes in some cases content that was created by other people (such as replies to the deleted user's posts). Be sure to read the warnings on the Delete User page!

To delete or disable a user account:

1. Navigate to Admin Console:**People** > **Management** > **User Search**.
2. Find the user acount you want to delete in the list and click **Delete** or **Disable** icon.

Moderating User Registration

If you've set up the application to allow people to register on their own, you can moderate those new registrations. (A system administrator enables both user registration and moderation for new registration requests.)

Fastpath: End User UI: Actions > Moderation

When someone registers (usually by filling out the registration form defined by the system administrator), you'll get a chance to approve or decline their request. In the end user UI, click **Actions** > **Moderation**. On the Pending Approvals tab, view the list of requests. You can click the person's name to view a profile page with the information they entered. Click **Approve** or **Decline** for each request. If you decline, you can enter your reason before finishing.

Synchronizing with User Authentication Systems

You can set up the application to synchronize data between its database and your external user identity system such as LDAP or Active Directory. This feature helps you ensure that the local application database contains only data related to users who are in your external user identity provider. Configure this feature in the admin console.

After you enter values to configure this feature, you can click the **Run Synchronization Task Now** button to go ahead and synchronize.

Fastpath: Admin Console: People > Settings > User Data Synchronization Settings

You can use the following table to complete the User Data Synchronization Settings page. Some fields are not visible until you select a previous field.

Setting	Description
Scheduled sync task enabled?	Synchronize with the user identity system nightly.
Synchronize user relationships?	Include user relationships in the data that's synchronized. For more on relationships, see Configuring User Relationships.
Managing LDAP attribute name	Visible when **Synchronize user relationships** is selected. The name of the LDAP attribute that provides information about user relationships.
Synchronize profile photo?	Include profile photos among the data that's synchronized. For more about profiles, see Defining User Profile Templates. You might want to let people maintain their profile photos independently.
User photo LDAP attribute name	Visible when **User photo LDAP attribute name** is selected. The name of the LDAP attribute specifying the user photo.
Last modified LDAP attribute name	The LDAP attribute on a user record which typically holds a timestamp of when the user's record was last modified. A common attribute name is "whenChanged".
Synchronize user profiles on login?	Synchronize a user's profile information when the log in.

Setting	Description
Disable non-administrative user accounts not found in source during synchronization?	Disable an account in Jive when the account is not fount in the user identity system. This is useful to help ensure that the enabled accounts in Jive are only those that are also in your system of record.
Disabled user LDAP attribute name	Visible when **Disable non-administrative user accounts...** is selected. The name of the LDAP attribute that indicates whether a user account is disabled.
Disabled user LDAP attribute value (regular expressions allowed)	Visible when **Disable non-administrative user accounts...** is selected. The value of the "disabled" attribute when it indicates that the user account is disabled.

Defining User Relationships

You can define relationships between people. The relationships you define are optionally visible in people's profiles. Using these relationships, people can stay on top of what certain people in the community are doing, including their changes to content, status messages, and so on.

Fastpath: Admin Console: People > Management > User Relationships

Although they're simple to use, user relationships require a little thought to manage well. Be sure to read the overview on user relationships, *How User Relationships Work*.

On the admin console's User Relationship Management page, you can view existing relationships and create or retire (break) relationships. Here, a "relationship graph" is the kind of relationship you're creating or retiring.

Viewing and Breaking Relationships

The page lists existing relationships. You can browse and filter the list to locate the one you want to break.

1. In the admin console, go to the User Relationship Management page.
2. View the list of relationships at the bottom of the page. You can filter the list to display only the relationships that include a particular person. To do so, enter that person's username in the Filter by Username box, then click the Filter button.
3. To break a relationship, locate the relationship you want to break, then click its Retire button.

Creating Relationships

The relationship graph dropdown will list the kinds of relationships your community supports.

1. Navigate to Admin Console: **People** > **Management** > **User Relationships**
2. Select the kind of relationship you want to add from the Relationship Graph dropdown list.
3. Enter the usernames of the people in the new relationship. If you can't remember the username, click **User Picker** to browse and search a list of users, selecting the check box next to the one you want.
4. Click **Add** to create the relationship.

Note: If your community draws data about people from an external data source such as LDAP or Active Directory server, then organizational relationships might already be defined.

How User Relationships Work

A user relationship connects two people in the community, allowing them to see one another's community activity.

Fastpath: Admin Console: People > Settings > User Relationship Settings

People can be part of two kinds of relationships, as described below. An administrator can enable one or both kinds of relationships. An administrator can also enable whether people using the community are able to create their own relationships, as well as whether approval should be required from the second person when the first requests a relationship.

- **Organizational chart** relationships, such as a relationship in which one person reports to another. Depending on how relationships are configured, it can be possible for people in the community to create their own relationships in either direction -- as reporting or reported to.

  Depending on how your community is configured, organizational relationships might be defined in an external user identity system such as LDAP or Active Directory, and merely displayed in the application. If so, these relationships typically can't be edited in the admin console or by people using the community.
- **Friend** or **connection** relationships, where two people are connected outside a hierarchical context. Your community will support *either* friend or connection relationships depending on whether user relationships have been configured to be bidirectional (friends) or unidirectional (connections/follows).

  In addition to determining how you manage such relationships in the admin console, the directionality setting determines the labels and commands people see in the application's end user interface. For example, one person can "friend" another to create a bidirectional friend relationship in which they're friends of one another. In contrast, a person can "follow" another to create a unidirectional connection relationship in which the followed person's activity is seen by the first person, but the followed person needn't reciprocate.

Direction	Description	Example
Unidirectional (follow)	A unidirectional relationship is one in which one person declares a relationship with another person, but the other person isn't invited to reciprocate (although they can separately create a similar relationship with the first person). Unidirectional relationships might be suited to situations where a reciprocal (bidirectional) relationship would be inappropriate or burdensome for the second person.	Someone working in a particular area is interested in keeping up with the work of another person who is doing research in that area. The first person clicks a link to "follow" the researcher. The researcher has no particular interest in following the person following them, so they needn't be prompted to follow the first person. If approval is required, the researcher receives the request and decides whether to approve it and let the first person follow them; otherwise, the unidirectional relationship is created automatically.
Bidirectional (friend)	In a bidirectional relationship, one person's relationship declaration creates (or at least invites) a relationship that goes the other way. Bidirectional relationships might be useful for communities in which people's personal relationships are less hierarchical, or are less specialized.	Someone with a particular interest notices that another person has similar or complementary interests. The first person clicks a link to "add as a friend" the second person. If approval is required, the second person receives the request and decides whether to approve it and become a friend of the first person; otherwise, the bidirectional relationship is created automatically.

Configuring User Profiles

Letting Users Control Their Own Settings

You can let people control how their profile information is displayed in the community, as well as provide them with other customizations, or you can set this information for them. For example, you can enable users to change who sees their name and email address, or you can just select the group who sees their name and email address. You can also enable or disable profile images. For information on customizing the user's profile, see *Defining User Profile Templates*.

Fastpath: Admin Console: People > Settings > Profile Settings

Setting	Description
Allow Profile Images	Set to "Yes" to allow people to display an image (such as of themselves) on their user profile.
Show Full Name by Default	Set to "Yes" to have a person's full name displayed on their profile, as opposed to merely their username. In some communities, such as some that are visible to the public, people would prefer not to have their full name displayed. In the Name Visibility field, you can allow users to customize the visibility of their name.
Name Visibility	Select **Users may edit the visibility for their name** to let users set whether their name should be visible to others in the community. You can also set who sees the name by default.
Email Visibility	Select **Users may edit the visibility for their email address** to let people set whether their email address should be visible to others in the community. You can also set who sees the email by default.
Profile Image Visibility	Select **Users may edit the visibility for their profile image(s)** to let users set who can view their profile image. You can also set who sees the profile image by default.
Creation Date Visibility	Select **Users may edit the visibility for their creation date** to let users set who can view their profile creation date (Users may see a "Member Since" date). You can also set who sees the creation date by default.
Last Login Date Visibility	Select **Users may edit the visibility for their last login date** to let users set who can view their last login date. You can also set who sees the last login date by default.
LinkedIn Profile Visibility	Select **LinkedIn Profile Visibility** to surface the LinkedIn widget in each user's profile page. Users who agree to surface their public LinkedIn profile in the Jive profile can see the profiles of other LinkedIn users when they browse profile pages. To complete this setup, provide an API key and a company ID (available from Jive Support). These two keys are required to establish connectivity to the LinkedIn servers.

Defining User Profile Templates

User profiles are like other content in that they can be found on searches. Because of this, information that people give about themselves — including interests and areas of expertise — can be a great source of information for people looking to have a question answered. A *person's profile* can include biographical and professional information, along with links to content they've contributed.

Fastpath: Admin Console: People > Settings > Profile Settings

On the Profile Settings page, you'll find three sections: Settings, Default Profile Fields, and Custom Profile Fields The Settings section enables you to fine-tune certain profile settings, including who can see essential fields by default. You can also set whether to show the user's full name, or allow profile images or personalized home pages. For more information on configuring these settings, see *Letting Users Control Their Own Settings*.

Changing Profile Fields

In the Default Profile Fields section, you can define the exact profile template you want to provide users so they can complete their profile. The application includes several commonly used fields by default, and you can add customized fields as well. Keep in mind that if you allow people to register themselves, you can define a form with a subset of these customized fields for a person to complete when they register.

To edit an existing field, click **Edit**. See the Editing Fields section for information on how to edit a field's properties. To create a custom field, click **New Field**. See the Customizing Fields section for information on adding new profile fields.

Default Profile Fields

Name	Type	Properties	Mapping
Title	Text Field	Edit	N/A
Department	Text Field	Edit	N/A
Address	Address	Edit	N/A
Phone Number	Phone Number	Edit	N/A
Home Phone Number	Phone Number	Edit	N/A
Mobile Phone Number	Phone Number	Edit	N/A
Hire Date	Date/Time	Edit	N/A
Biography	Large Text Field	Edit	N/A
Expertise	Large Text Field	Edit	N/A
Alternate Email	Email	Edit	N/A
Home Address	Address	Edit	N/A
Location	Text Field	Edit	N/A

Custom Profile Fields

New Field

Name	Type	Properties	Options	Mapping	Order	
Office Address	Address	Edit	N/A	N/A		
						Delete

Editing Fields

Click a field's Edit link to edit the field's properties. When you edit a profile field, you're defining its behavior in the system -- who can see it, whether it's editable, and so on.

Be sure to consider whether or how a field should be visible. For example, in some communities people might not want their phone number widely visible.

Note: Only visible fields are available when searching or browsing.

Give some thought to how people will be using profiles -- to introduce themselves or to find other people, for example -- then select or clear attributes accordingly. For example, making too many fields required could have the effect of discouraging people from completing them. The following list describes the attributes you can assign the profile field.

- Required -- People won't be able to save a profile when they leave a required field empty.
- Filterable -- When a field is filterable, people can type or select values of the field to make a list of people shorter. For example, someone viewing a long list of people in the community could make the list shorter by filtering on the hire date, specifying that the date be no earlier than last year.
- Searchable -- A searchable field is seen by the search engine.
- Editable -- People can edit their editable profile fields.
- Externally managed -- An externally managed field is associated with an external user directory, such as LDAP. Select this to include this field among those that can be synchronized with the external system. You'll need to separately set up synchronization. For more information, see *Synchronizing with User Authentication Systems*.

Customizing Fields

The Custom Profile Fields section is where you can create customized fields for user profiles. When you add two or more custom fields, you can adjust the order by clicking the up or down arrows in the Order column.

1. Click **New Field** to create a new profile field.
2. Select the field type. You can choose from date, text, number, or many more types to help provide the best user experience for this field's information.
3. Click **Continue**.
4. Enter the field name. This is a label that identifies the field content, and it may be different than what the user sees in their profile.
5. Enter the Language Display Name, and click **Add Translation** for each language you want to provide translations for. This is what the user sees in their profile field.
6. Select the relationship to user for field visibility. This indicates how the releationships between users determines who can see this field. Set this field considerately because some sensitive information should have limited visibility. You can also set the default and enable user's to edit their own profile field's visibility. For example, some people may be more comfortable publishing their phone number than others.

   Note: Only visible fields are available when searching or browsing.

7. Select one or more of the following attributes for the field:

   - Required -- People won't be able to save a profile when they leave a required field empty.
   - Filterable -- When a field is filterable, people can type or select values of the field to make a list of people shorter. For example, someone viewing a long list of people in the community could make the list shorter by filtering on the hire date, specifying that the date be no earlier than last year.
   - Searchable -- A searchable field is seen by the search engine.
   - Editable -- People can edit their editable profile fields.
8. Click **Finish**.