jive

work better together™

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

Use the Admin Console to manage system settings, permissions, content (documents, discussions, and blogs), and people.

- To open the Admin Console from your Jive Community, click your avatar in the top right of the page and choose **Admin Console** from the menu.

Setting Up the Community

You have several options for customizing the look and feel of your community.

The first time you log in to the end user interface as an administrator, you'll be prompted to get the site going. All of the settings you make here are things you can change later.

Configuring the Application with the Setup Tool

After you've installed the application, finish setting it up using the setup tool. From the tool, 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 setup tool, 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.

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:

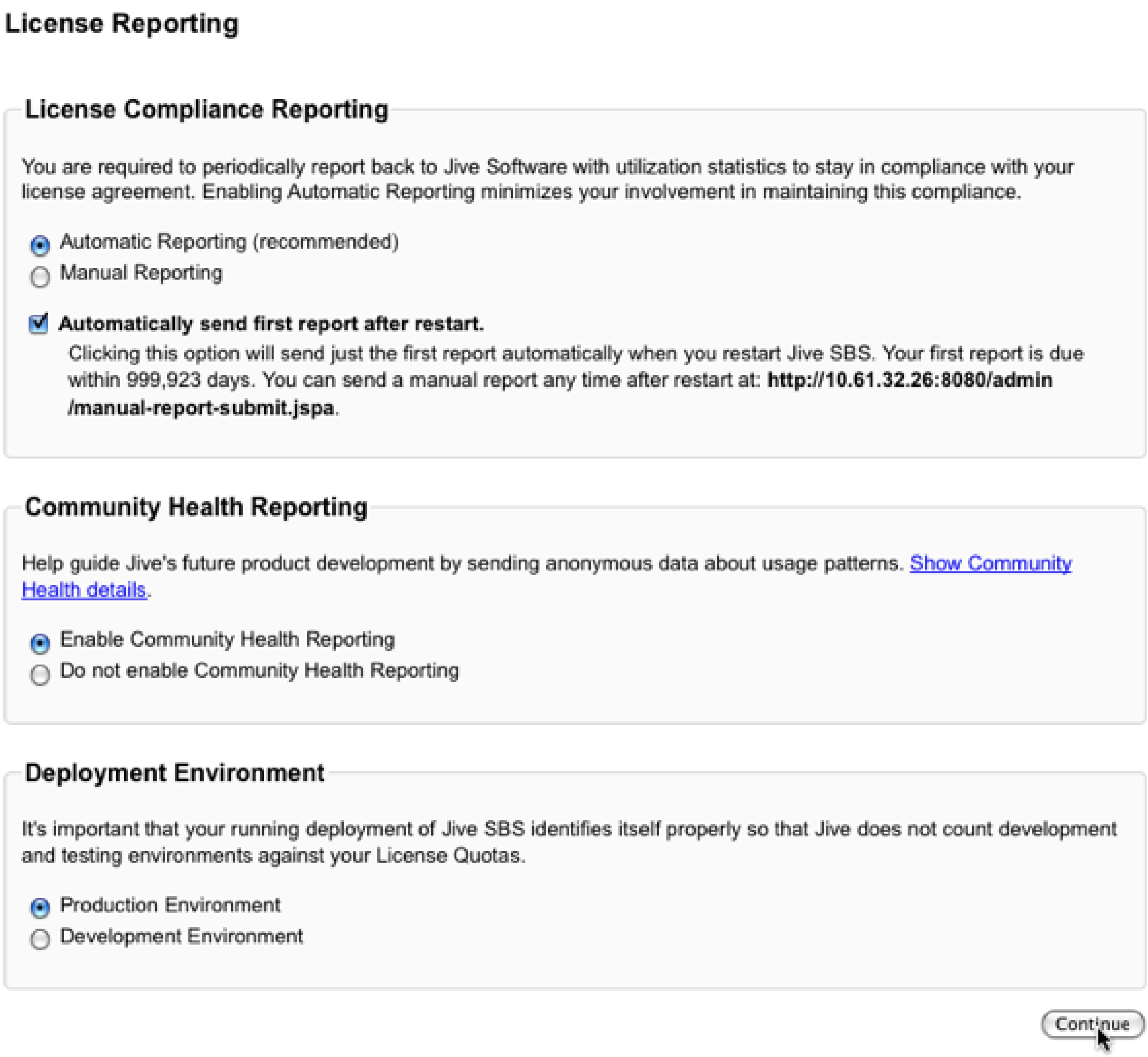
1. Stop the web application and httpd services by running **jive stop webapp** followed by **jive stop httpd**.
2. Edit /usr/local/jive/applications/sbs/home/jive_startup.xml so that the <setup> element has the value "false" (meaning "setup has not been run").
3. Start the web application and httpd services by running **jive start webapp** followed by **jive start httpd**.
4. Point your browser to the Jive community Admin Console URL. By default, using the built-in application server, this URL is: `http://<webapp_hostname>:8080/admin`.
5. 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.

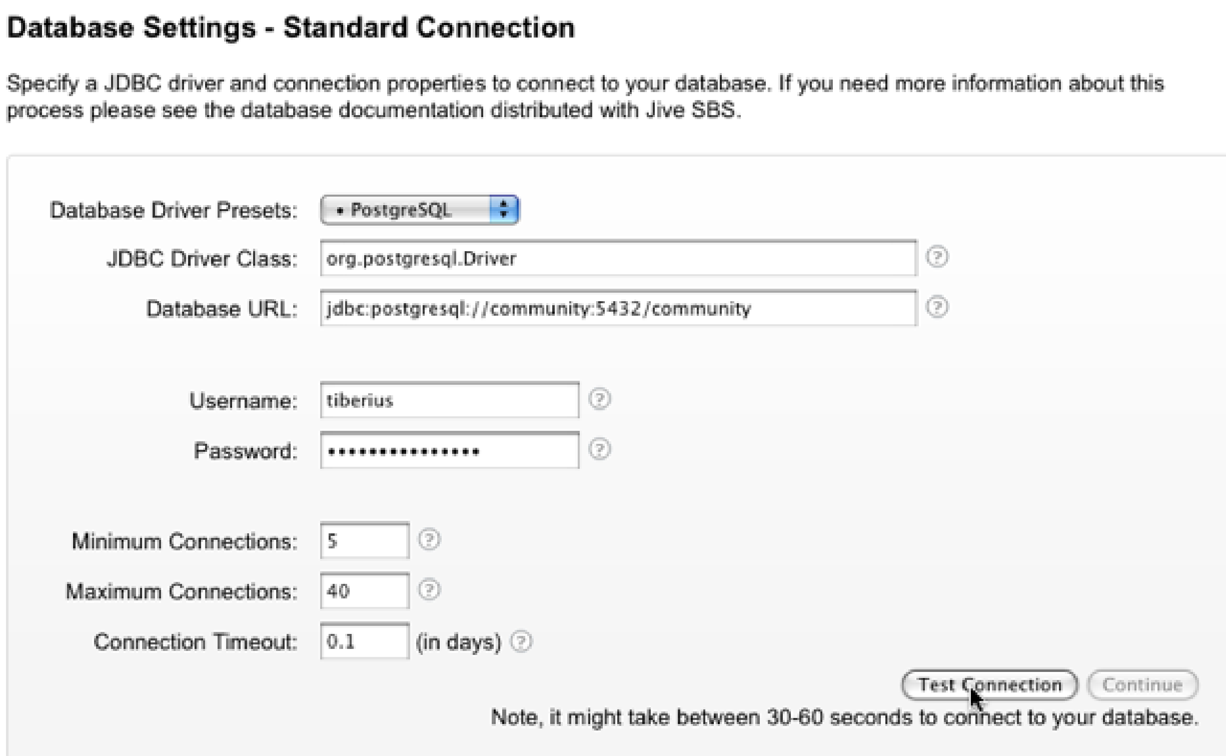
On the License Reporting page, choose whether to have your report sent automatically or to send it manually. Given that periodically sending a license report is required, having it sent automatically might save you the trouble of having to remember to send it. On this page, you also opt in or out of 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.

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.

Use these settings to connect to your Search service. You have the option of either connecting to Jive's Cloud Search service or installing and connecting to an On Premise Search service.

Setting	Options	Description
On-Premise Search		
	On-Premise Search Service Host	Enter the host name that Jive can use to connect to the Search service. For On-Premise Search, this is the host name for the node where you installed Search. Default is **`localhost`**. Refer to system requirements for information on Search node size.

Setting	Options	Description
	On-Premise Search Service Port	Enter the tcp port that Jive can use to connect to the Search service. Default is **`30000`**.
Cloud Search		
	Search Endpoint	For Cloud Search, select the public cloud search end point in your area. For connection information, see Connecting to Jive-Hosted Services.

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 by using the following commands from a command prompt as the jive user on the target computer:

```
[root@targethost ~]# sudo su - jiver
[1016][jive@targethost:~]$ jive restart webapp
sbs restarted successfully.
```

Setting Up Your Profile

One of the first things you'll want to do as the community manager or administrator is to set up your user profile. By adding profile information, you create a great example for other new users.

Fastpath: End User Interface > **Your Avatar or Name (in the upper right corner)** > **Edit Profile**

- Add a 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 items you're associated with, such as content you create. Keep in mind that some images look better than others at a small size.
- Add information about yourself. People will be able to find yours and others' profiles when they search for keywords, so it's a good idea to use words in your biography and expertise sections that people might search for.

Theming Your Community

Using the theming interface, you can customize your community with your organization's unique colors and logo, or use a predefined theme included with Jive, such as Bamboo or Winter. You can also export and import themes.

Fastpath: End User Interface > **Your Avatar** > **Themes**

Your community manager and users with Customize Site permissions can use the out-of-the-box theming feature. These users will see the Themes option under their user menu in the upper right corner of the end user interface.

Optimizing Themes for Mobile Browsers

When planning your community theme, keep in mind that some theming options are not viewable on the smaller screen of a mobile browser. You can select **Basic** theming for optimal mobile browsing.

Use these tips to help your community fully support mobile browsing:

- Set the theming option to **Basic** and test on a narrow screen. You can do this on your desktop browser by making the browser smaller. Make sure the theme looks good.
- Header logos are not supported, so we suggest you upload your logo into the Branding header and Navigation area for the theme. See the steps below for help with this.

Here's how to add a logo that's compatible with a narrow-screen view:

1. Click **Your avatar** > **Themes**.
2. Once you're in the theming interface, click the blue dot to the left and directly under the header.
3. Select **Branding header** > **Logo or text**.
4. Click **Image**.
5. Click **Choose File** and navigate to and then double-click the logo you'd like to upload.
6. Click **Save Theme** > **Save and Publish**.

Using Jive in a Mobile Browser

Jive delivers an awesome community experience to smaller screens, too. The mobile browser features simple navigation with large buttons that are better suited for touch screens. You won't see options that are too complex or take up too much real estate on a mobile device.

To visit your community from a mobile browser, just enter your community's URL into the built-in browser of your device and log in. Note that you can see the same narrow interface on the desktop version by making your desktop browser smaller.

Here's what you can do from the mobile browser (and for a quick visual tour of the interface, check this out):

Read and interact with your streams and Inbox	Just like in the desktop version, you can cruise through and interact with your streams, and read and respond to your Inbox items.
Create most content types	Create all sorts of content from your mobile device, for example, ideas, blog posts, documents, and so on.
Search and filter	Tap the magnifying glass, enter your search term, and then click the down-arrow to filter by Content, People, or Places, and/or the time period of the last modification.
Access and use places like a pro	Follow, join, or leave places from the mobile browser. You can also see a place's activity, content, people, and any subspaces, projects, and custom pages the place may have. To sort the content in a place, just click **Content** and then an icon: documents, discussions, blogs, or polls. If you're looking for the tiles on a group's activity page, be sure to scroll all the way down to see them.

Note: Some content and functionality only make sense in the wider desktop view, so you won't see some things cluttering up the smaller space. Also, iPads will always benefit from the full functionality of a wide-screen view.

Known Issues

- The mobile browser does not work on Blackberry devices.
- Older Android browsers struggle with content creation. You can resolve this by upgrading your Android operating system and using Chrome to browse your community.

Which Kind of Theme Should I Use?

Understand the differences and upgrade risks between the out-of-the-box Theming Tool and custom themes you create with Soy or Freemarker.

Note: Jive Software strongly recommends using the out-of-the-box Theming Tool whenever possible due to upgrade risks when using Soy or Freemarker themes.

Out-of-the-box Theming Tool	The application includes an out-of-the-box theming tool available to community managers and users with Customize Site permissions. Those users can see a **Themes** option in their user menu in the upper right corner of the end user interface. This theming tool allows you to quickly customize your site with your organization's unique colors, logo, and fonts, or use a predefined theme included with Jive, such as Bamboo or Winter. You can also export and import themes to back up, share, and transfer themes to other Jive communities using this theming tool. These themes are upgrade-safe for future versions of the application.
Custom Themes in Soy or Freemarker	The application also allows you to develop and deploy your own custom themes using Soy or Freemarker. However, be aware that by deploying Soy and Freemarker themes, you will be modifying the application's underlying page templates. Doing so can make application upgrades extremely time-consuming and resource-intensive. At Jive Software, we have observed that customers who deploy Soy and Freemarker themes often experience difficult upgrades due their custom themes. If you want a custom theme but don't want to develop it yourself, you can have Jive Software's professional services team do it for you. Ask your Jive account representative about this service.

Using a Predefined Theme

Quickly create a professionally-designed community with just a few clicks. Using the **Themes** interface, you can select a predefined theme for your community such as Fall, Winter, or Bamboo. You can also use a predefined theme as a base design, and then make further changes to it.

1. Click on your avatar in the upper right corner and select **Themes**. (Note that only with Manage Community or Customize Site permissions can see the Themes option under their user menu in the upper right corner of the end user interface.)
2. Click **Themes** > **Predefined themes**.
3. Select a theme (Bamboo, Winter, and so on).
4. You can further customize your chosen theme by clicking the blue dots next to each component and making changes. As you make changes, you'll see an instant preview of the updates. You can also click **Full Preview**, for a more thorough look at your changes.
5. When you're finished making changes, be sure to click **Save Theme**. You'll have the option to save the theme, but not publish it (this will save your work so that you can continue making theme changes later without affecting your current community), or, you can save the theme and **Publish** it, which will update your community immediately.

Theming Your Site

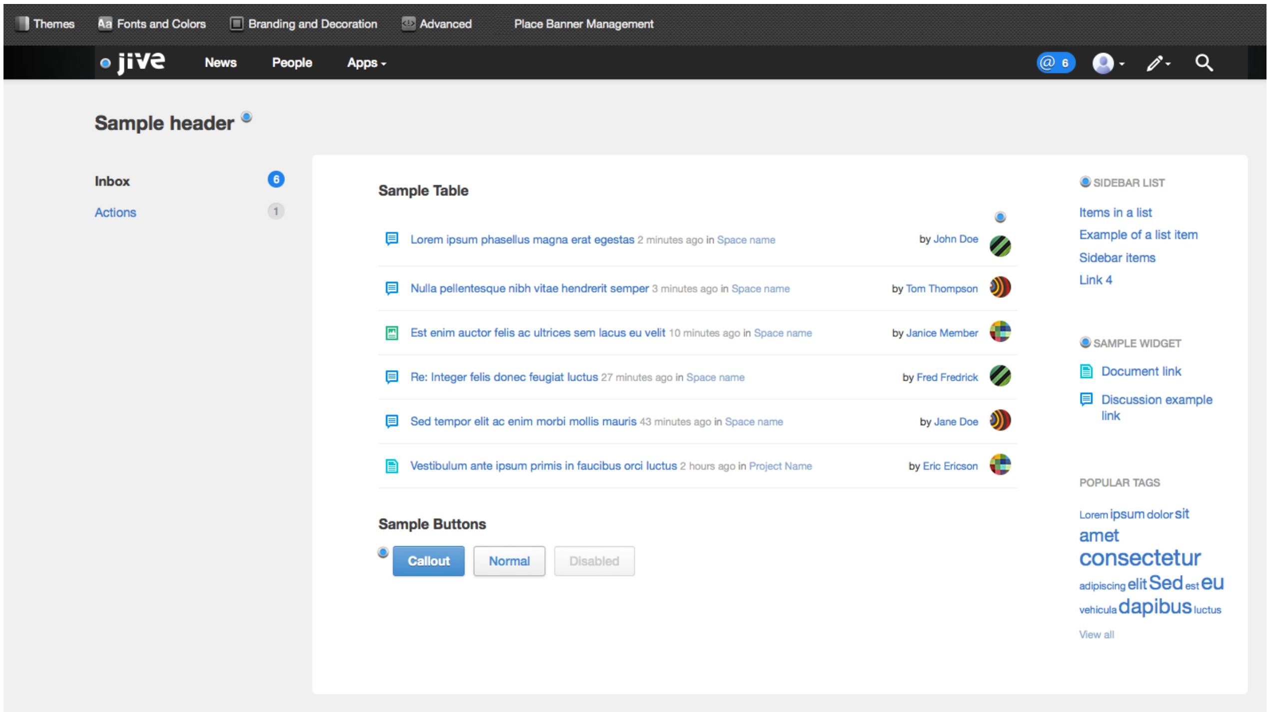
The out-of-the-box theming tool lets you quickly customize the look and feel of your community. You can change the appearance of text, background colors, logo image, and more. These changes will affect all pages in your community.

See the Theming Options Reference on page 17 to review what you can change using out-of-the-box theming.To get started, click on your avatar in the upper-right corner and select **Themes**. (Note that only with Manage Community or Customize Site permissions can see the Themes option under their user menu in the upper right corner of the end user interface.)

Fastpath: End User Interface > **Your Avatar** > **Themes**

Caution: This kind of theming is different from the custom theming you can do with Freemarker or Soy. Jive Software **strongly recommends** using the out-of-the-box theming tool whenever possible due to upgrade risks when using Soy or Freemarker themes. The documentation for custom theme development starts here.

You should see a special theme-editing interface that uses the default theme style (upgraded instances will see their old theme):



To customize your theme:

1. Make changes by clicking the blue dots next to any interface component. You'll see an instant preview of the updates.
2. Select a predefined theme under the Themes tab, such as Bamboo or Winter. You can use these themes as-is or make further changes to them by clicking the blue dots next to any interface component.
3. Change your Header and Navigation Style under the Advanced tab. Options include a thin navigation bar that stays pinned to the top while users scroll pages (Reduced), a more roomy navigation bar and header area combo (Basic), or a fully customizable header or footer (Custom).
4. If you want to create custom navigation buttons in your navigation bar, you'll need to enable Custom Links. Be sure to read Creating Custom Links in the Main Navigation on page 19 for more details.
5. Click **Full Preview** at any time for a more thorough look at your changes.
6. When you're finished making changes, you can save your new theme by clicking **Save Theme**, but not publish it (this will save your work so that you can continue making theme changes later without affecting your current community). After you save a theme, you can export it to another instance by using the import/export feature under the Themes tab. If you **Publish** your saved theme, your community will be updated immediately with the new theme. These changes will affect all pages in your community.

Theming Options Reference

You have a number of options for designing your site using the theming interface. Keep in mind that Advanced out-of-the-box theming, which allows you to use custom CSS in headers and footers, is a more complex and risky procedure.

Table 1: Main Theming Options

Field	Description
Themes	From here you can see all your saved themes, import or export themes to back up, share, and transfer themes to/from other instances (typically, test instances), or select from a list of predefined themes.
Fonts and Colors	Sets the font of all text. You can customize the color of the text for links, hovers, meta text, and so on.
Branding and Decoration	Sets the community's width, favicon, background color and image, and border style. Be aware that if you set your Background Attachment to "Fixed," depending on the image's size and width, browser scrolling may be slow.
Advanced: Header and Navigation Style	You can choose from the following options: **Reduced (default for new instances; upgraded instances retain their existing theme)**: Includes a thin navigation bar, no header, small logo, and limited options for the other configurable items of the user interface. The thin navigation bar stays pinned to the top when a user scrolls any page in the application. You don't need to know any CSS or HTML to use this option. **Basic**: Includes a full navigation bar, header, large logo, and more options than Reduced for the other configurable items of the user interface. **Custom**: Enables you to customize the HTML and CSS of the header (and optionally, the footer). You can even choose to hide the header.
Advanced: Images	You can upload images to your theme to use in custom headers and footers. These images reside in your Jive instance as part of the theme, are accessible from the Internet to anyone who knows the URL, and can be imported and exported with the theme. If a theme is deleted, its associated uploaded images are also deleted, so the best practice when creating themes is only to link to images uploaded to the current theme.
Advanced: Custom Links	You can create custom links on the main navigation bar. You don't need to know any CSS or HTML to use this option.

Field	Description
Advanced: Advanced Theming	In addition, you can create your own custom themes with Freemarker or Soy. However, there are substantial upgrade risks when doing so. Jive Software strongly recommends using only the Customize Your Site theming interface to avoid upgrade risks. The documentation for Freemarker and Soy theme development starts here.

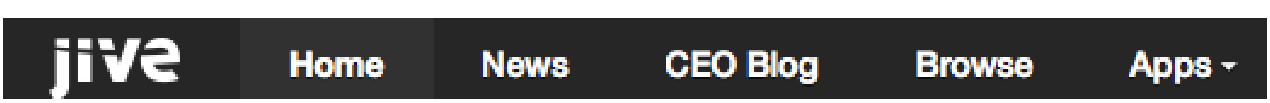
Table 2: More Options ("blue dot" options). These options vary depending on which Header and Navigation Style you select.

Field	Description
Branding Header (Logo)	Sets the community logo and background color and image of this header area.
Branding Header (Logo): Main Navigation	Sets the link colors, and background color and image of the navigation menu. (You can also customize the actual buttons that appear in this navigation menu. Refer to Creating Custom Links in the Main Navigation on page 19 for more information.)
Headline Color and Font (Sample Header)	Sets the background color and font of the headline area. You can also choose to inherit the font from the Branding and Decoration settings.
Secondary Navigation	Styles the Create menu, the search field, and the menu under each user's name or avatar, including the shapes of the avatars shown in the user menu. You can use this setting to remove the search box from the top navigation.
Sidebar List	Sets the text color and font for links in the sidebar. If you don't set this style, it inherits the style of the Sample Widget.
Sample Buttons	Sets the color style of the buttons and various other elements throughout the user interface (e.g., navigation menu highlights).
Sample Widget	Sets the border style, header background, and other elements of widgets.
Search	Sets the display style of the Search box.
User Profile	Sets the text color and the style of the arrow drop-down menu of the User Profile.

Creating Custom Links in the Main Navigation

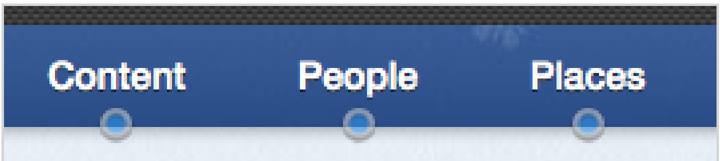
You can customize your main navigation menu so that users can quickly jump to your community's most popular or useful pages, or to external links. You can also delete a navigation button.

Here's an example of a customized navigation menu that includes two custom navigation buttons: CEO Blog and Browse. When a user clicks Browse, they'll see a pull-down menu from which they can select Content, People, or Places.



To create a custom link(s) in the navigation bar:

1. Go to **End User Interface: Your Avatar** > **Themes** > **Advanced** > **Custom Links** and select **Custom Links enabled**. (Note that only with Manage Community or Customize Site permissions can see the Themes option under their user menu in the upper right corner of the end user interface.) You should see blue dots under the main navigation buttons like this:



2. From here, you have several options (for details, see the Custom Links Reference). Generally speaking, you can create navigation buttons that link to pages inside or outside of your community. In addition, you can rename existing pages (for example, change News to 411 or People to Our Users), create dropdown menus of linked pages, rearrange the order of the navigation buttons, or even delete navigation buttons altogether.
3. If you are creating a Single or Multiple custom link (i.e., not a Preset) and your community is set up for multiple languages, be sure to click **Provide other translations** for each navigation button you create and select the languages for which you want to provide a translation. For each new link you configured, you'll see a name and URL field. If you don't provide a translation for a particular language, users who have that language in their browser settings will see the links in the system language set for your community. Because words and phrases can take up more screen space in some languages than in others, you should test your translations to make sure they are displayed correctly.
4. When you're finished customizing your navigation buttons, be sure to click **Full Preview** in the lower left corner to see how your changes look before saving and publishing them.

Main Navigation Options Reference

Here's a handy reference that describes what you can do with custom links in the main navigation bar using the theming interface. You can have a total of four preset and custom links in the navigation bar and drag-and-drop them to change their order on the bar.

Custom Links

Single or multiple custom links are useful for linking to pages inside or outside of your community. Be aware that if you use these custom links, you'll need to provide your own translations if your community is delivered in multiple languages by clicking **Provide other translations** for each link that you add.

Table 3: Custom Links Options

Nav Bar Option	Links to
Single	Use this to customize a single link's title and URL. For example, it might be helpful to your users Users, or change News to 411. Note that if you do this, the URL does not change, just the text c
Multiple	Use this to create a dropdown menu with a unique title. For example, a Supportal button might c

Preset Links

The Preset links are useful for linking to existing preset pages in your community such as Content, People, or Places. When you use any of these Preset options as is, they will be localized automatically for all of the application's supported languages. You could also change the navigation bar label of these Preset options by using the Single link, as described above; but in that case, you would need to provide your own translations by clicking **Provide other translations**.

Table 4: Preset Links Options

Nav Bar Option	Links to
Content	/content
People	/people
Places	/places
News	/news (note that you'll need to be running version 8.0.1 to be able to rename, remove, and sort
Browse	Creates a dropdown menu that will contain at least one of the following predefined links: Conten

System Links

You can make some modifications to the following system links, including moving them around (in the case of the Create menu), or not showing them at all.

Table 5: System Links Options

Nav Bar Option	Links to
Home	The Home button will show in the main navigation if the Welcome/Home page (**System** > **Home**
Create	The Create menu will show in the main navigation when the Basic header is enabled. Otherwise more detail about the header options, see the Theming Options Reference on page 17.
Apps	Opens up the Apps menu when clicked. The Apps navigation button will only show outside of th

Export a Theme

Using the **Themes** interface, you can back up a copy, share, or transfer your saved themes to another Jive community using the Export a Theme feature.

When you export a theme using the out-of-the-box theming tool, the application creates a zip file containing all of the theme's information, including its customized colors, images, and so on. This zip file includes any images you uploaded using the Advanced theming interface. The theme file is encrypted for security reasons, so you cannot further customize its contents.

1. Click on your avatar in the upper right corner and select **Themes**. (Note that only with Manage Community or Customize Site permissions can see the Themes option under their user menu in the upper right corner of the end user interface.)
2. From the theming page, select **Themes** > **Import/Export**.
3. Choose **Export**, and then select the theme you want to export.
4. Select **Save the file** to save the theme as a zip file.
5. The zipped file will download to your local file system.
6. Now, you can import the zipped theme file to another Jive community using the Import a Theme feature.

Import a Theme

Using the **Themes** interface, you can import a theme so that it is saved in your list of available themes.

When you Import a theme, you are adding it to your list of saved themes. From there, you can click on it to preview the theme in your community. Note that you can import only the zip file that is created when you Export a Theme. This zip file includes any images that were uploaded using the Advanced theming interface.

1. Click on your avatar in the upper right corner and select **Themes**. (Note that only with Manage Community or Customize Site permissions can see the Themes option under their user menu in the upper right corner of the end user interface.)
2. From the theming page, select **Themes** > **Import/Export**.
3. Choose **Import**, and then browse to and select your theme.
4. Click **Add to saved themes**.
5. Now in your list of saved themes, you should see the new theme. Click on it to see a preview of your community with that theme. If you like it, don't forget to click **Save Theme**.

Replacing a Place Template's Default Banner

You can replace the default banner image that appears in a Place Template (such as the Best Practices template) with your own custom image. Or, you can change the background color, text color, and repeating pattern of the default image.

To replace the default banner image with a custom image in a Place Template:

1. In the end user interface, click **Your Avatar** > **Themes** > **Place Banner Management** (you must have community administrator or Home Page/Customize Site permissions to see this option in your user menu).
2. On the Template Mapping tab, click **Edit** on the template you want to change (such as Event Planning).
3. Change the header text and background color or leave them as is.
4. Browse to the custom image you want to add and select it.

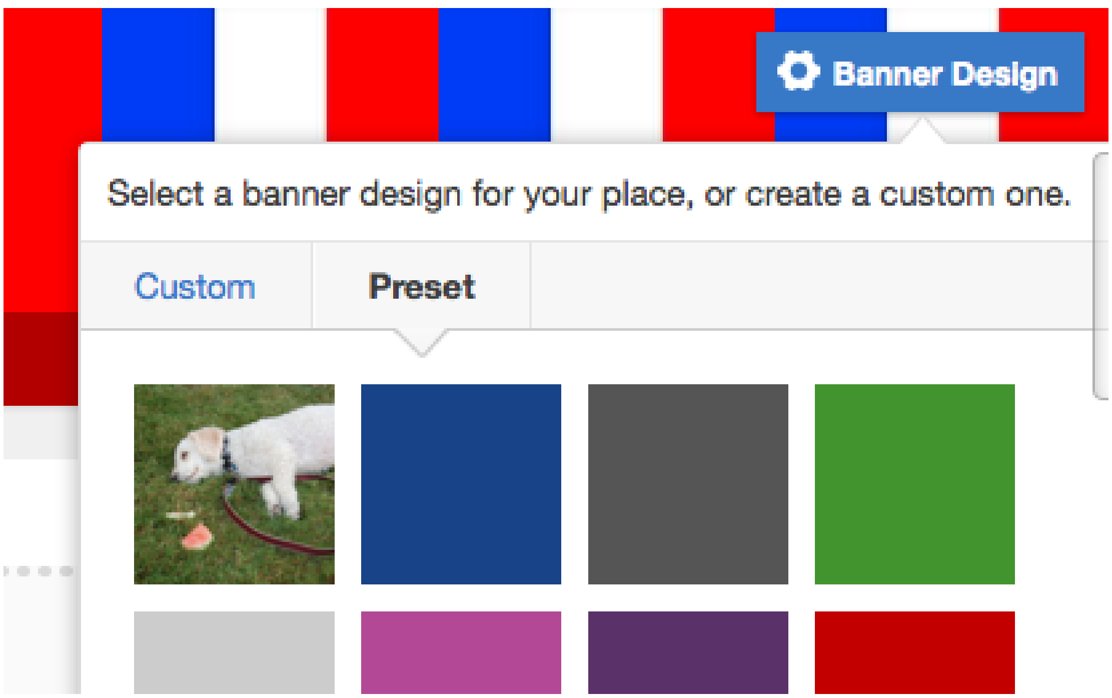
5. Set the background position and pattern for the image.
6. Select **Update existing usages** if you want your change to update existing images. If you do not select this option, the banner in existing instances of the place template will remain unchanged.
7. Click **Save**.

Managing Place Banner Presets

You can add custom images to the existing set of Banner Designs available in places. These are the images place owners see when they are editing the Banner Design of a place. You can also change the order of the default banners, or delete any of them.

Fastpath: End User Interface: Your Avatar > **Themes** > **Place Banner Management** > **Place Banner Presets**

Any changes you make to the Place Banner Presets will affect what place owners see when they edit the Banner Design of their place. In the following example, the community manager has added a custom image of a white dog for place owners to use as a banner:



Note that the place owner can still choose to upload *their own* Custom image for the banner as well.

Adding a New Image to the Place Banner Presets

You can add a custom image to the existing set of Banner Designs available in a Place Template.

1. In the end user interface, click **Your Avatar** > **Themes** > **Place Banner Management** > **Place Banner Presets** > **Add new banner preset**. (Note that only with Manage Community or Customize Site permissions can see the Themes option under their user menu in the upper right corner of the end user interface.)
2. Change the header text and background color or leave them as is.

3. Browse to the custom image you want to add and select it.
4. Set the background position and pattern for the image.
5. Click **Save**.

Place owners will now be able to see this image in their Banner Design options.

Creating a Site Structure

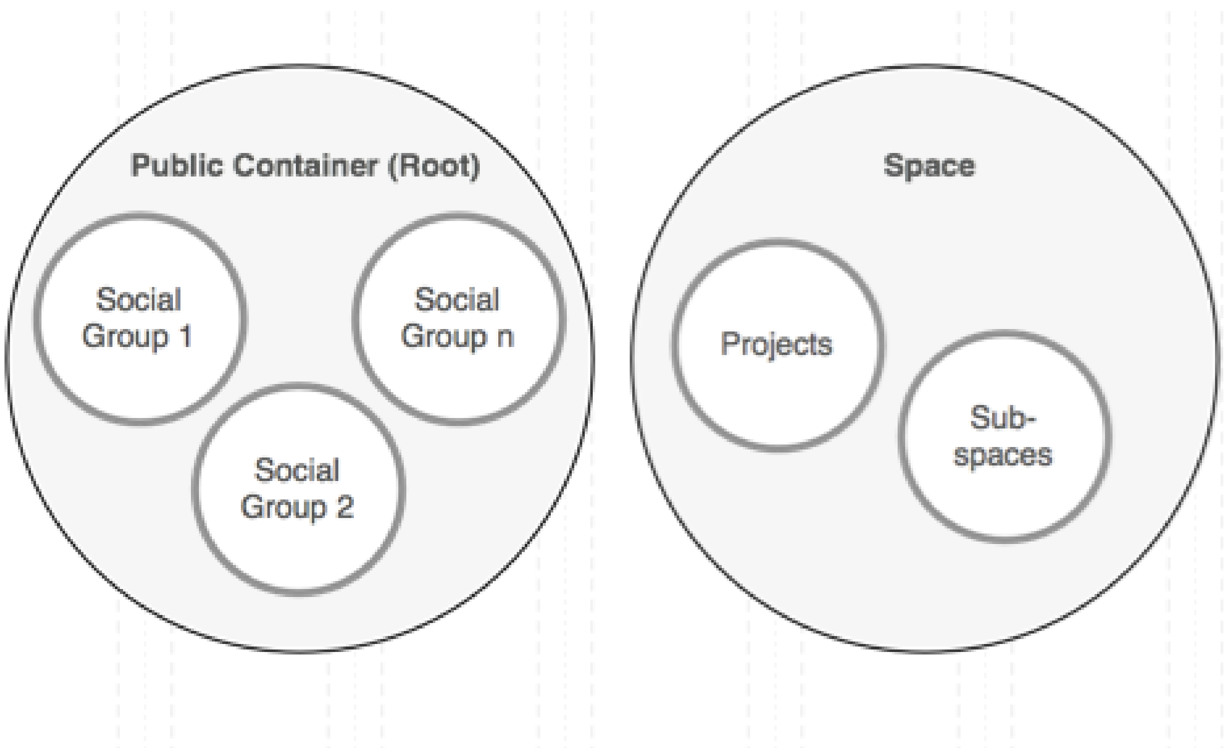
Creating a structure for content is one of the most important things you'll do to get your community started. Because people post content in places in the community, the places you create will help your users intuitively understand where to post (and find) content.

For example, you might organize the spaces to reflect the organization of the company itself (HR, Accounting, Research, and so on).

A couple of things to note about how groups and spaces work:

- Social groups are contained by the root community space, but other than that, they don't have a hierarchical structure. This means that groups cannot be created inside a different space or under another group.
- Spaces contain any associated sub-spaces and projects (if you have them enabled). You may find this ability to create hierarchical spaces and sub-spaces useful depending on your needs.

You can think of it this way:



This becomes important when you're setting up things like moderation and permissions in places because of inheritance relationships. Social groups inherit from the root space, while projects and sub-spaces inherit from their parent space. Inherited settings can be modified, but the settings inherited at the time of creation are used as a starting point.

To get started, sketch out a list of the places you think you'll want, and then pick a few that are most likely to help new users get interested in the community. For example, you could create places that are sure to compel people to read and add content to them, such as Shout Outs for Jobs Well Done, Funny Kitten Gifs, or Planning the Big Party.

To read more about creating spaces, be sure to read Designing Space Hierarchies and Creating a New Space.

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. To change the jiveURL, go to **Admin Console: System** > **Management** > **System Properties** and edit the property `jiveURL`. (If you want to know how to change the root context of your community, be sure to read Changing the Root Context (optional).

Next, be sure to update the following components with the new URL.

Caution: If you change the jiveURL system property from https to http temporarily for the purpose of doing an upgrade, you will need to also change the value of the system property jive.auth.forceSecure to false. This system property causes a redirect of all incoming requests to https.

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

Component:	How to update with the new jiveURL:
Web Application Nodes	Change the `jiveURL` system property (**Admin Console: System** > **Management** > **System Properties**). Then, as the jive user, set the following: • jive set webapp.http_proxy_name <newdomainname> • jive set webapp.http_proxy_port 443 • jive set webapp.http_proxy_scheme https
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` (**Admin Console: System** > **Management** > **System Properties**). 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** > **Native Apps** > **Gateway Access URL**).

Component:	How to update with the new jiveURL:
SSL/Tomcat	Update the new URL in the server.xml file for the Tomcat connector.
Apache	Ensure that any redirects you have configured previously are reconfigured to point to 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).
Emoticons	Update the URL setting for the emoticon post-processing filter (**Admin Console: Spaces** > **Settings** > **Filters and Macros** > **Emoticon Filter** > **Settings**).

Changing the Name of the Root Space

You can change the name and description for the root space from the Admin Console. By default, the root space is named "Jive".

Fastpath: **Admin Console** > **System** > **Settings** > **Space**

Setting the Locale and Time Zone

You can set the default locale, time zone, and character set for your community. The correct locale helps to make people's experience in the community feel more familiar and comfortable.

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. For communities that want to support a broad variety of languages, Jive requires using "UTF-8" (Unicode) as your character encoding.

You can use the Locale settings to determine 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** > **Settings** > **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.
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** > **Settings** > **Locale**).

Note: The server time zone set on the operating system can occasionally override some of the other Locale settings. If you encounter unexpected mixed-language results on your site, try checking the OS language set on the machines where you installed Jive.

Customizing the News Page

Users with Manage Community or Manage News Streams permissions can configure the News page of the community, which features a variety of configurable tiles and subscription streams curated for specific users or groups of users.

What Is News?

News is the central place for you to see what's happening in the community.

The News page features a variety of streams created for you by your community manager, designed to direct you to content, people, and places that pertain directly to you. You'll also see your Connections stream, any custom streams you have created, the Top & Trending stream, and the Most Recent stream, which shows recent activity from all over the community that you have permission to see.

You can pin any of the streams listed on your News page to the News button. Just click **News** and then the pin icon or triangle next to your desired page's name in the left sidebar. Now when you click News from anywhere in the application, you'll be taken right to the page you pinned.

The News page also features a variety of tiles to help you find important people, places, and content quickly. The Trending Content and Trending People tiles are included by default, but may be removed by your community manager.

Here's an overview of what you'll see on the News page. For a quick visual tour of the News interface, click here.

News (top-level view)	The News view aggregates and displays only new content posted in your News and Connections streams. However, unlike your other streams, News will not show content updates and comments in the stream. In addition, content that gets updated or interacted with is not bumped to the top of the News view. So, to repeat, the News view shows *only new things*.

	Because the News view aggregates new posts from your News and Connections streams, content is pulled in and displayed in the News view in the order in which your streams are displayed in the left sidebar. Six items from each stream are pulled in and shown in creation-date order. Duplicated content is removed if it's already being pulled in from a higher-order stream. Content you've read (by clicking-through to it either from your desktop or a mobile version of Jive) will stay in News for three days before going away. Content you haven't yet read will stay for seven days. Because the News streams are designed just for you, you won't see the same content pulled into the News view that others will see.
News streams	These are the streams you see listed above the Connections stream. They are created and managed by your community manager or people with Manage News Streams permissions. Because these streams are designed just for you, you may not see the same News streams or the same content in them that others see. To learn more, be sure to read What Are News Streams? on page 29
Connections stream	This is a built-in stream where you are automatically following some of your colleagues, but you can add to or delete content, people, and places from it. This stream can be a good way to avoid stream proliferation if you just want to check in throughout the day with things that interest you without having to create a lot of custom streams.
Your custom streams	If you've created any custom streams, you'll see those listed below the Connections stream. Custom streams can be a great way to keep up with the content, people, and places that matter most to you in your community. Here are some examples of custom streams you might want to create for yourself. For a quick visual tour of the custom streams interface, click here.

Top & Trending stream	Check out this stream to get a feel for what's happening right now. The Recommended Content and People widgets, as well as the Trending Content and People widgets, show you what's generating a lot of interest around the community. To learn more, take a look at Using Your Recommendations.
Most Recent stream	This stream shows you *all* community updates that you have permission to see as they are posted in real time. Scrolling through this stream can be useful for adding new people and content to your Connections or custom streams.

What Are News Streams?

News streams are configured for you by your community manager and are designed to bring you the latest news from your organization, department, team, or product.

News streams are listed above the Connections stream. Because they are designed just for you, you may not see the same News streams or the same content in them that others see.

For example, everyone in your community may see the "CEO's Blog" stream that shows the latest blog posts from your organization's CEO. However, only people in the Marketing department may have a stream called "Marketing News" that shows activity from the Marketing space.

In addition, you might have a news stream based on your role in the community. For example, let's say everyone has a stream called "What’s New," but what is displayed there will be different depending on your role. So *Customers* might see content pulled from the Special Promotions blog in their What's New stream, but *vendors* might see content pulled from the New Solutions group.

To learn more about streams and how they work, be sure to read What Are Streams?

Tips for Creating News Streams

Before you create a news stream, here are some questions to consider.

Does absolutely *everyone* need this information?	News streams created for Everyone will display on the News page for *all* registered community users. If you work in a large organization, this could include all people across a wide variety of job roles, divisions, and locations. If you're confident the information will be relevant to all of these users, follow the instructions in Creating a News Stream for Everyone.
How much traffic is generated by the place or blog I want to share content from?	Be sure that the place you select for the news stream isn't too noisy for the intended audience.

	For example, if your Sales group sometimes contains social chatter, consider creating a more controlled group or blog that contains only key communications, and use that one for the News stream.
Who, exactly, needs this News stream?	You can define audiences by selecting individual people, by filtering on profile fields, and/or by selecting a user permissions group defined in Jive. The last two choices may require some preparation on your part: to make sure you're using profile fields consistently, and to create any permissions groups you need for targeting an audience. Note that the system-defined groups in Jive (under **People** > **Management** > **User Group Summary**) cannot be used to target audiences. You can use any custom-defined groups shown in this screen. These groups may be created manually or synced from an SSO provider. You may need to work with your community manager to define user groups.
What are some examples of News streams I might create?	For a detailed example of how you might create News streams for your community, be sure to read this article in the Jive Community. You must be a registered community user to see this content.

Creating a News Stream for Everyone

Here's how to create a News stream for all registered users to see.

Users see News streams listed above the Connections stream. You must have Manage News Streams or Manage Community permissions to create, modify, or delete News streams.

For a detailed example of how you might create News streams, be sure to read this article in the Jive Community. You must be a registered community user to see this content.

To create a News stream for everyone in the community:

1. Go to the **News** page and click

   .

   Restriction: You'll only be able to see this icon if you are a community manager or have Manage News Streams permissions.
2. Click **Everyone**.
3. Give the new stream a title, for example, "Executive News" or "CEO Blog." This is the stream name users will see on the News page.

4. Under **Places/Blogs**, enter or select the place or blog you want the stream to pull content from.

   Tip: If you see both a place and the place's blog listed, keep in mind that selecting the blog would post less content in the stream. In other words, selecting a place means *any* new content created there will show up in the stream. Selecting the blog means only blog posts will show up.

5. Under **Audience**, decide whether you want guest users (users who have not registered) to be able to see the stream. This is only relevant if your community is visible to unregistered users.
6. Under **Email Options**, select whether you want the stream's users to receive email or mobile notifications every time new content is posted in the place or blog.

   Tip: Generally speaking, we recommend setting this to **Off**. However, you'll likely want to enable notifications on the most important content that your users cannot miss. Just keep in mind that if notifications get noisy, users may stop reading the content.

7. Click **Save**, then **Publish Layout**.

You can create up to ten news streams, which will display on the News page in the order listed. You can reorder the list by dragging a stream to a new position.

Creating a News Stream for Specific Users

Create a News stream to show a different selection of content to different audiences.

You must have Manage News Streams or Manage Community permissions to create, modify, or delete News streams.

To create a News stream so that specific users will see content relevant to them:

1. Go to the **News** page and click

   .

   Restriction: You'll only be able to see this icon if you are a community manager or have Manage News Streams permissions.

2. Click **Specific Users**.
3. Give the new stream a title, for example "Management Ideas" or "My Team News." This is the stream name users will see on the News page.

   Tip: Make the stream title work for every rule you are going to create for this stream. For example, you could create a heading called "Management Ideas" and then create different rules that direct new content from Finance groups to the Finance managers, blog posts from the Technical Managers group to Engineering managers, and so on. You could then add a stream rule targeting content from Human Resources management groups to all these management groups, because those management ideas can apply to any manager.

4. Select **Create Stream Rule**.
5. Under **Places/Blogs**, enter or select the place or blog you want the stream to pull content from.

> **Tip:** If you see both a place and the place's blog listed, keep in mind that selecting the blog would post less content in the stream. In other words, selecting a place means *any* new content created there will show up in the stream. Selecting the blog means only blog posts will show up.

6. Under **Audience**, enter the users and group of users who will be able to view the stream. You can also enter profile field values.

   > **Note:** For more information on filtering based on a profile field, be sure to read this article in the Jive Community. You must be a registered community user to see this content.

   You also have the option to select **Create profile filter** so that you can filter your audience based on a combination of profile fields.
7. Click **Save**.
8. Under **Email Options**, select whether you want the stream's users to receive email notifications every time new content is posted in the place or blog.

   > **Tip:** Generally speaking, we recommend setting this to **Off**. However, you'll likely want to enable notifications on the most important content that your users cannot miss. Just keep in mind that if notifications get noisy, users may stop reading the content.
9. Click **Save**.
10. Click **Publish Layout**.

You can create up to ten news streams, which will display on the News page in the order listed. You can reorder the list by dragging a stream to a new position.

> For a detailed example of how you might create News streams, be sure to read this article in the Jive Community. You must be a registered community user to see this content.

News Page Tile Reference

Here's a complete list of the tiles available on the News page.

> To learn more about using tiles, be sure to read Using Tiles.

Table 6: Your Tiles

Tile	Description	Dependencies
Your Custom Tile Name	Any custom tiles you have created will be listed here.	You must first Create New Tile to see the Your Tiles option under Categories.

Table 7: Content Tiles

Tile	Description	Dependencies
Document Viewer	Shows a full preview of a document you choose to display.	Content added manually.

Tile	Description	Dependencies
Helpful Links	Build a list of key items for quick reference. Links can be internal to your community or external URLs.	Content added manually.
Key Content and Places	Displays a list of content and places that you can edit and manage yourself.	Content added manually.
Featured Video	Shows a manually selected video from an external, non-community source.	Content added manually.
Image Gallery	Create a slideshow with images and captions.	Content added manually.
Tagged Content	Displays content that matches specific tags.	Relies on content being tagged.
Expandable Sections	Shows links to community content under collapsible headings.	Content added manually.
Latest Blog Posts	Shows the newest blog posts in your community. (You won't see this tile if your community manager has disabled blogs in your community.)	Content added manually.
Carousel	Link a rotating image carousel to key destinations.	Content added manually.
Trending Content	Shows content that's attracting views and interactions. This tile appears by default on the News page. You can remove it by clicking the garbage can icon.	Relies on an algorithm.
Ask a Question	Find a previously asked or answered question, or ask a new one.	Content added manually.

Table 8: People Tiles

Tile	Description	Dependencies
Featured People	Build a list of important people for your place.	Content added manually.
Trending People	Displays the avatars of people trending in the community. This tile appears by default on the News page. You can remove it by clicking the garbage can icon.	Relies on an algorithm.

Table 9: Places Tiles

Tile	Description	Dependencies
Similar Places	Shows places with the same tags.	Relies on content being tagged.
Key Content and Places	Displays a list of content and places that you can edit and manage yourself.	Content added manually.

Table 10: Other Tiles

Tile	Description	Dependencies
Key Dates	Show selected dates for your team.	Content added manually.
Featured People	Build a list of important people for your place.	Content added manually.
Key Content and Places	Displays a list of content and places that you can edit and manage yourself.	Content added manually.
Featured Video	Shows a manually selected video from an external, non-community source.	Content added manually.
Image Gallery	Create a slideshow with images and captions.	Content added manually.
Carousel	Link a rotating image carousel to key destinations.	Content added manually.
Featured Video (internal)	Display a video from your community.	Content added manually.

Configuring News FAQ

Here are some frequently asked questions and answers about configuring the News page and News streams.

Who can create and modify the News page and News streams?	People with Manage News Streams permissions have the rights to modify the News page and create, modify, or delete News streams, including those set up by other people with Manage News Streams permissions. People with Manage Community permissions already have these rights. Community managers can give someone Manage News Streams permissions, by going to **People** > **Permissions** > **System Administration** and

	creating a user override to assign the user Manage News Streams permissions.
Can I add a secret place to a News stream?	Yes, if you are an owner or member of the secret place. Be aware when adding a secret place to a News stream that other users with Manage News Streams or Manage Community permissions will be able to see this stream greyed-out when configuring News. They will not be able to modify or delete a News stream that has a secret place to which they are not an owner or member.
Is there a limit to the number of News streams the community can have?	There can be up to 10 News streams configured in your community. (This does not include each user's ability to create up to 10 custom streams of their own; so in theory, a user could see 10 News streams and 10 of their own custom streams listed in the left sidebar).
How many rules can I have per news stream?	You can have 100 rules in a news stream. Within each rule, audiences and places are essentially unlimited.
Can I change the name of the News button on the navigation bar?	Yes. Just use the Single custom links feature in the theming interface. To learn more, be sure to read Main Navigation Options Reference on page 20.

News Streams Administration

News is a newly added set of features that is enabled by default in new communities. The News page functions as a central news page for your community. It is enabled by default. In the next release, News will be enabled for all communities, and you won't be able to turn it off.

News is deeply integrated into your community's architecture, so turning it on and off has significant effects on how users navigate around the community. With News enabled, users will see News in the main navigation. By default, it is the landing page for users when they log in. But the News feature is also linked to a large number of navigation changes that determine how end users find and interact with content. You shouldn't turn News off in a working community, because you'll risk confusing your users.

For more information about setting up News, see Customizing the News Page on page 27.

Customizing the Home Page

You can customize the Home page of your community if you have Manage Community permission. You also have the option to delete the Home button from your community in the Admin Console.

Admin Console > **System** > **Settings** > **Home Page** > **Enable the widgetize community home page**.

Home Page Options

Home is an optional page that you can configure with a variety of widgets. The configuration options you enable will reflect the needs and use cases of your particular community.

Note: This topic describes the options for what desktop users see when they log in to your community. To set up a landing page experience for users who are viewing the community on a mobile browser, see Creating a Mobile Community Home Page on page 39.

Table 11: Overview (Home) Page Options (System > Settings > Home Page)

Option	Description
Enable the main navigation Create menu	Enabling this setting allows users to create a variety of content, such as discussions and documents, in the community. This option is helpful for communities focused on content creation and sharing, for example, a community focused on employees getting work done together. Be sure to read Enabling the Create Menu to learn more about this feature.
Enable the widgetized community home page	• Enabling this allows you to configure a Home page with a number of useful widgets, such as the Image Navigation widget that links users to your most common places or content, the Newest Members widget to encourage adoption and participation, and a Featured Content widget that links to your community's important content. • If you do not enable a community Home page, your users will not see the Home button and News will be the page users see when they log in.
Simple home page	Enabling this will remove the left sidebar that includes links to Inbox and Actions. This option is helpful if you want to de-emphasize the participatory and collaborative features of the application and focus more on content consumption, for example, in a customer or partner support community where people are typically trying to find answers to questions.

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 Home pages. Check the URL of the target page for the correct value. For example, to set the default page to Activity, set the value to /activity.

This section calls out a few widgets that are commonly used on the Home page, but you have more options. See the Available Widgets Reference on page 228 for more information.

Configuring the Community Home Page

You can customize the optional Home page with a variety of widgets that feature important content. You'll need to have Home page permissions to make this change.

To customize the community Home page:

1. Make sure the widgetized home page is enabled (**Admin Console:** > **System** > **Settings** > **Home Page**).
2. From the end user interface, click your avatar in the top right corner and then select **Overview Page**.
3. Customize the page using widgets.

Note: The Community Home page is similar to place overview pages, except it cannot use a three-column view.

Setting Up Image Navigation

You can configure any place's Overview page, including the community Home page, with image-based navigation to quickly direct your users to useful pages. First, you'll add the Image Navigation Widget to your place's layout, then add images and links to the widget.

Add the Image Navigation Widget to Your Place's Layout

1. Go to the place you own and click **Manage** > **Overview Page** to begin editing the place's Overview page. (If you're editing the community's Home page, you'll click your avatar in the upper right corner, and then **Manage** > **Overview Page**).
2. From the widgets list, select **Other** > **Image Navigation Widget**.
3. Drag the widget down into your layout area and drop it where you want it.
4. Click the small triangle in the upper right corner of the widget and select **Edit this widget**.
5. Change the widget's title or leave that field blank if you do not want any title.
6. Select whether you want the header and border to be displayed.
7. Click **Save Properties**.

Add Images to the Widget

After you've added the Image Navigation Widget to your place's layout, you'll add images and links to the widget, then publish the updated layout of the place.

1. Click the small triangle in the upper right corner of the Image Navigation Widget and select **Edit this widget**.
2. Click **Add a new image link**.
3. In the "Provide a Target Link" field, type in the URL that you want the image to link to.
4. Provide a caption for the image. You can use the caption Jive provides automatically, or overwrite it with your own.
5. Select the image you want to use for this link, and then click **Save**.
6. Repeat these steps until you have all the images you want to display in the widget. The limit is 8. You can move them around to change the order in which they are displayed by dragging and dropping them.
7. When you're finished, click **Publish Layout** on the editing page.

Setting Up the Search Widget

The Search widget allows your users to quickly search a specific space or group in your community, or the entire community.

1. Go to the place you own and click **Manage** > **Overview Page** to begin editing the place's Overview page. (If you're editing the community's Home page, you'll click your avatar in the upper right corner, and then **Manage** > **Overview Page**).
2. From the widgets list, select **Content** > **Search Widget**.
3. Drag the widget down into your layout area and drop it where you want it.
4. Click the small triangle in the upper right corner of the widget and select **Edit this widget**.
5. Use the title "Search Widget" or create your own, for example, "Search this Group" or "Search Me!"
6. Select the number of results to return in the search.
7. Select the place to perform the search. This can be any place in the community, or the entire community (which would be your "root" space).
8. Click **Save Properties**.
9. When you're finished making changes to your place's layout, click **Publish Layout**.

Setting Up the Ask Widget

The Ask (a place) widget allows users to quickly ask a question in a specific space or group in your community, or the entire community. After the user types a question into the Ask widget, the search function displays possible answers based on matching keywords. If the user doesn't see the correct answer in the results list, they can create a discussion right from the widget. This can be very helpful in places designed to support customers or employees.

1. Go to the place you own and click **Manage** > **Overview Page** to begin editing the place's Overview page. (If you're editing the community's Home page, you'll click your avatar in the upper right corner, and then **Manage** > **Overview Page**).
2. From the widgets list, select **Content** > **Ask (place)**.
3. Drag the widget down into your layout area and drop it where you want it.
4. Click the small triangle in the upper right corner of the widget and select **Edit this widget**.
5. Use the title "Ask (place)" or create your own, for example, "Ask Us a Question". You can also change the text that will be displayed on the actual Ask button, for example, instead of "Ask It," you might want "Submit Your Question".
6. Specify the place you want to perform the search. You can search in the current place, a single place that you specify, or all public places in the community (this would be your "root" space).
7. Select the number of results to return in the search.
8. You have some options for what will be displayed in the search results. You can select one, some, or all of these options:

Option	Description
All Questions	Displays in search results all questions that have been asked, whether or not they have been answered.
All Discussions	Displays only discussions in search results.

Option	Description
Answered Questions	Displays only Answered Questions in search results.
Documents	Displays only documents in search results.

9. Select the place you want questions posted to. This can be different from the place where the Ask widget is located. For example, you could put the Ask widget in an "Employee Questions" group, but post the questions to the "Employee Q&A" group.
10. Click **Save Properties**.
11. When you're finished making changes to your place's layout, click **Publish Layout**.

Setting Up the Answered Questions Widget

The Answered Questions widget allows your users to quickly see a list of questions that have been answered in a specific space or group in your community, or the entire community. Answered questions displayed in this widget are those that include a reply or comment marked as a "Correct Answer".

1. Go to the place you own and click **Manage** > **Overview Page** to begin editing the place's Overview page. (If you're editing the community's Home page, you'll click your avatar in the upper right corner, and then **Manage** > **Overview Page**).
2. From the widgets list, select **Content** > **Answered Questions**.
3. Drag the widget down into your layout area and drop it where you want it.
4. Click the small triangle in the upper right corner of the widget and select **Edit this widget**.
5. Use the title "Answered Questions" or create your own, for example, "Recently Answered".
6. Select the number of answered questions to display in the widget.
7. Select the order in which you want the answered questions to be displayed.
8. Specify the place you want to pull the answered questions from. Typically, you'll want this to be the current place, but it could be any other place in the community as well, or the entire community (this would be your "root" space).
9. Click **Save Properties**.
10. When you're finished making changes to your place's layout, click **Publish Layout**.

Creating a Mobile Community Home Page

Community managers can create a tile-based, mobile-compatible community home page for users accessing the community with a mobile device.

The Community Overview page for desktop users relies on widgets, which can't be viewed on a mobile device. You can now design a version tailored to mobile users. When accessing the community on a mobile device (and not using the iOS or Android native app) users can see a welcome message you provide as well as image-rich dynamic content delivered through up to 8 tiles. This view will also be available in the reduced-browser view when you access the community on a desktop browser.

The Place Templates Tile Reference on page 236 includes more information about individual tiles. (Not all tiles are available for the mobile home page.)

To set up your mobile home page:

1. Under your name or avatar, click **Manage** > **Mobile Home Page**
   By default, the page contains the following tiles, with no content defined:
   - Carousel tile
   - Ask a Question tile
   - Key Content and Places tile
2. Click the **Edit page** link to configure these tiles or add different ones.
3. In the Welcome Message text box, type up to 500 characters of the message you want to display at the top of the mobile home page. Keep in mind this message will be displayed in a very compressed space, so keep it short!
4. Add or delete any tiles you want to add to the page, and configure them to contain the information you want by clicking the gear icon. You can use the arrows to move the widgets up and down.
5. Click **Save**.
6. If you want to preview the mobile page, just go to the community home page and resize your browser. When you've reduced the browser size enough, the mobile home page replaces the regular one.

Enabling or Disabling the Create Menu

The Create menu allows users to create a variety of content, such as discussions and documents, in the community. You can enable or disable this feature.

Fastpath: System > **Settings** > **Home Page** > **Enable the main navigation create menu**

Internal communities	By default, internally-facing communities (those that typically involve only employees or other internal audiences) have the Create menu enabled to encourage users to contribute to the community by creating documents, discussions, and so on.
External communities	By default, externally-facing communities (those that typically involve customers, vendors, and other external audiences) have the Create menu disabled to encourage users to search the community for answers before asking a question. **Caution:** With the Create menu off, you'll need to create places through a different process. Be sure to read Group Creation Options and Space Creation Options on page 247.

When the Create menu is enabled, you'll see a pencil icon in the upper right corner of the user interface.

Tip: Status Update creation can also be enabled or disabled and is configured separately. Be sure to read Configuring User Update Settings on page 112.

Creating Community-Wide Announcements

If you have permissions, you can create a system-level announcement by selecting **System Announcements** from the menu under your username or avatar and then clicking **Add a new announcement**.

You can create a system announcement that will be displayed for all users on the upper right of all Activity pages, under the Community Announcements heading and above Recommendations. Each announcement will also be displayed as a banner at the top of the Overview Page. You can preview the images and text in your announcement as you create it. If multiple announcements are set to be displayed at the same time, users can click through them in a predetermined sequence.

To create a community announcement and determine the order it will be displayed in:

1. Click your avatar or username in the upper right corner and then **System Announcements**.
2. Click **Add a New Announcement**.
3. If you want to feature a URL in your announcement, select the **Announce a link** check box and type or paste your URL in the text box. Jive automatically detects the page title and suggests a display title and image from the linked page. You can choose to use these or replace them with your own title and image as described in the following steps.
4. Give the announcement a title. This is the heading users will see when deciding whether to expand the announcement, so make it short enough to be scanned easily.
5. Optionally, add an image. You can upload an image by browsing, or use drag and drop. You'll see the image in preview on the right after you select it. Make sure the **Include an image** check box is selected: once you've selected an image, you can still see it the configuration screen even if you have disabled image display. (However, it will not be visible in the preview unless **Include an image** is enabled.)
6. Add a short text description with further details of the announcement. Again, shorter is better, since announcements are designed to fit in a small space. If you want to link to further information, you can put a URL in the description text and it will be a live link: however, you can't currently put a named link in the announcement text. To feature a URL in your announcement, use the **Announce a link** feature, which will link the URL to your announcement title.
7. Decide how long the announcement should be displayed by selecting a start and end date. Announcements start at 12:00 (AM) on the start date and expire at 23:59 on the end date, in the announcement creator's time zone.
8. Decide whether to send a notification about the announcement by selecting or clearing the **Send Inbox notifications** check box. Users who have their Inbox set to provide email notifications (this is the default setting) will receive an email as well as seeing the announcement displayed in Activity pages.

9. After you save your announcement, you can return to the System Announcements page and determine the click-through order by dragging and dropping the cards. Click-through order is left to right and top to bottom.
10. If you have rights to edit community announcements, you can edit or expire them directly by using the links directly within the announcement.

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.

Changing the Name of the Root Space

You can change the name and description for the root space from the Admin Console. By default, the root space is named "Jive".

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, up time, 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 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 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.

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 as well as the community 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 community 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.

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.
- 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.

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 the following usage information collected by the application:

- 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 (licenseable 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.

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.

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!

Setting the Locale and Time Zone

You can set the default locale, time zone, and character set for your community. The correct locale helps to make people's experience in the community feel more familiar and comfortable.

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. For communities that want to support a broad variety of languages, Jive requires using "UTF-8" (Unicode) as your character encoding.

You can use the Locale settings to determine 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** > **Settings** > **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.
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** > **Settings** > **Locale**).

Note: The server time zone set on the operating system can occasionally override some of the other Locale settings. If you encounter unexpected mixed-language results on your site, try checking the OS language set on the machines where you installed Jive.

Directory Server Integration Guide

If your enterprise already uses an LDAP directory server such as OpenLDAP or Active Directory to manage users, you can configure your Jive community to integrate with it. By default, the application doesn't use a directory server. Instead, it stores all user data in a database and performs authentication with that data. When you integrate with LDAP, Jive will authenticate against your directory server. During setup, you specify which users and groups defined in the directory server you want the application to use.

The instructions for integration assume that you are or have access to the administrator of your directory server, and that you're familiar with the Jive Admin Console. If you don't have this expertise, you may want to contract with Jive Professional Services or another outside resource with expert knowledge about administering a directory server.

Note: If you're using Active Directory, make sure it allows LDAP querying. You might also be interested in reading LDAP Querying Basics at the Microsoft web site, or LDAP Attributes at the Computer Performance web site.

LDAP Security

The Jive application database never caches or stores user credentials. However, if the LDAP system property `ldap.ldapDebugEnabled` is on (true), directory server traffic can be logged, and user passwords can be printed in plain text to the application's `sbs.out` log file if connections to LDAP are unencrypted (non-SSL). It is your responsibility to ensure that your LDAP communication runs over an SSL connection.

Supported Directory Servers

Jive can be integrated with a variety of directory servers.

Jive regularly tests LDAP integration with the following providers:

- OpenLDAP
- Microsoft Active Directory
- OpenDS
- Sun ONE

and can typically assist with configuration for these providers. Troubleshooting assistance for other LDAP integrations may require an engagement with Jive Professional Services.

Overview of Directory Integration Steps

To set up directory server integration, you need to gather information about your LDAP server configuration, identify the location of your key directory server and tree, map your users and (optionally) groups so Jive can synchronize to them, and then test your implementation to ensure it is successful.

Directory server integration relies on preparation and testing to be successful. If you use this list of overview steps to plan your integration, and if you run a test implementation to ensure that you have correctly identified the users, groups, and fields you want to sync with your Jive instance, you can avoid some frustrating missteps associated with integrating these two complicated products.

1. Gather information about your server configuration. To complete the integration setup, you will need:
   - The address of your directory server and how it will communicate with Jive. If you're using Jive to host your community, you can contact Support for assistance with setting up the connection between these servers. Make sure you account for server referrals, especially if you use Active Directory.
   - The Base DN associated with the users you want to sync with Jive. You may or may not want to include all the users in your organization, so make sure your Base DN is associated with the part of the tree that includes the users you are targeting. Keep in mind that if you plan to map groups as well as users, your BaseDN needs to be at a tree level that contains both users and groups. You can also narrow down your users by specifying a User DN relative to the Base DN during setup.
   - The DN associated with an Administrator account that has read access to your directory server. (This account does not need to be linked to a Jive user.)
   - The field identifiers associated with any directory service fields you want to sync to Jive profile fields. For example, the Username field is typically associated with the sAMAccountName field for Active Directory. A good method for obtaining this information for your directory server setup is to export an LDIF file.
   - Any LDAP filter expressions you need to limit the number of users returned when you sync Jive to your LDAP tree. If you don't filter, synchronizing to your directory server will return every user associated with the Base DN you supplied, and your Jive community may be populated with users who don't need to be there. The LDAP Explorer website is a helpful resource for information about LDAP filters. For filter information focused on Active Directory, see LDAP Query Basics on the Microsoft website.
   - The field identifiers for any groups you want to map to permissions groups in Jive. You don't need to map any groups if you want to manage permissions entirely in the Jive community. You will also need to specify an attribute such as member or memberOf that can be used to associate users and groups.
2. Start the directory server integration setup by going to the Admin Console and selecting **People** > **Settings** > **Directory Server Settings**. Note that the individual fields on this screen have helpful tool tips that you can access by hovering on the question mark next to the field.
3. Supply your connection settings and test the connection by clicking **Test Settings** at the bottom of the screen. If you can't connect, you may need to check your credentials. The account you're binding with must have read access to users and groups for the entire subtree rooted at the base DN.

4. Click **Save** to save your connection settings and display the rest of the configuration screens in a tabbed view.
5. In the User Mapping screen, map any Jive profile settings you want to populate from your directory server by supplying an LDAP string. Fields for which you provide a mapping will be updated from the directory server whenever a sync takes place, typically when the user logs in (see User Synchronization). Click **Advanced Settings** to add any user filters you want to use to narrow down the number of users you will sync.
6. Click **Test Settings** to validate your mappings against the directory server. If the attribute you specified can't be found, you'll see an error message identifying the problem.
7. In the Group Mapping screen, decide whether to use and synchronize the permissions groups you have set up in LDAP or use Jive to assign users to permissions groups. (Note that group permissions have nothing to do with social groups in Jive.) You can choose to maintain some Jive-created permission groups even if you use LDAP-managed groups: however, make sure they are distinctly named.
8. Go to the User Synchronization screen to determine when and how you'll synchronize your user information between LDAP and Jive.

Mapping Users from a Directory Server

If you're provisioning users from a directory server, you can use the User Mapping screen to map selected user fields to be synchronized with your Jive user information.

Fastpath: Admin Console: People > Settings > Directory Server Settings > User Mapping

You can use the User Mapping screen to determine what information LDAP and Jive will share and how they'll keep user information synchronized. You can also use this screen to specify how Jive will identify external users who have access to externally accessible groups, and which users marked in LDAP will be disabled in Jive.

To set up User Mapping:

1. In the Admin Console, click **People** > **Settings** > **Directory Server Settings**
2. Make sure you've defined a valid connection to an LDAP directory server in the Server Configuration screen. (If you don't have a working configuration saved, you won't be able to see the rest of the configuration screens.)
3. Select **User Mapping**.
4. Map the user account fields to connect user accounts based on the LDAP fields that will be used to create and enable a Jive account based on the directory listing.
5. If you plan to enable Externally Accessible Groups and want to identify users based on an LDAP match rather than by inviting them directly from the group, specify a name-value pair using the User Type Field and the External Contributor User Type Value.
6. If you want to disable Jive user accounts by identifying them in LDAP, specify a name-value pair using the User Disabled Field and User Disabled Field Value settings. You may do this using a field that's predefined for this purpose. For example, Active Directory uses UserAccountControl=514 to mark

disabled users: you can specify UserAccountControl as the User Disabled Field and 514 as the User Disabled Value. You can also use any other available name-value pair to disable users based on an attribute. To make this work, you should also select **Disable federated user accounts not found in the directory** in the User Synchronization tab.

7. Specify any profile fields you want to synchronize by providing the field information from your directory.
8. If you want to apply a user filter to narrow down the number of users you will sync, use the User Filter and User RDN fields to apply them. For more information about preparing user filters, go here.

Mapping Groups from a Directory Server

If you're provisioning users from a directory server, you can maintain permission groups in Jive or use your LDAP permission groups.

Fastpath: Admin Console: People > Settings > Directory Server Settings > Group Mapping

Keep in mind that if you switch between maintaining groups in Jive and in LDAP after your initial setup, you will need a migration strategy.

To connect your LDAP groups to Jive :

1. In the Admin Console, click **People** > **Settings** > **Directory Server Settings**
2. Make sure you've defined a valid connection to an LDAP directory server in the Server Configuration screen. (If you don't have a working connection defined, you won't be able to see the rest of the configuration screens.)
3. Define and save some User Mappings.
4. Select **Group Mapping**.
5. Select **Use LDAP to manage Groups** and provide the group mapping information for your directory server.

Using LDIF to Inventory Your Directory

Exporting an LDIF file from your server can help you extract key information about your LDAP settings that's useful in setting up your Jive integration.

The information you'll use to set up your user and group mappings for directory server integration can be exported easily into a format called LDIF (LDAP Data Interchange Format). You can use this information yourself or provide it to a Jive Support engineer.

Any LDAP directory browser provides the ability to export to and import from an LDIF file. If you're using Active Directory, you can use the ldifde command line tool. Another excellent tool is JXplorer, which helps you to validate your LDAP mappings and provides an easy-to-use LDIF export. Here's an example of the `ldifde` command which will yield an LDIF output like above:

The following example shows an LDIF output generated by executing `ldifde -f output.txt -d ou=Jive_Users,dc=support,dc=jive,dc=com`:

```
    dn: CN=Cyr \, Karl,OU=Jive_Users,DC=support,DC=jive,DC=com
    changetype: add
    objectClass: top
    objectClass: person
    objectClass: organizationalPerson
    objectClass: user
    cn: Cyr , Karl
    sn: Cyr
    physicalDeliveryOfficeName: Awesome
    givenName: Karl
    initials: KC
    distinguishedName: CN=Cyr \, Karl,OU=Jive_Users,DC=support,DC=jive,DC=com
    instanceType: 4
    whenCreated: 20081119215504.0Z
    whenChanged: 20090202220617.0Z
    displayName: Cyr , Karl
    uSNCreated: 4391224
    memberOf: CN=FilterGroup,OU=Jive_Users,DC=support,DC=jive,DC=com
    uSNChanged: 4399897
    department: Awesome
    name: Cyr , Karl
    objectGUID:: 2tnXRo7VxE6zc72YqLtOTw==
    userAccountControl: 66048
    badPwdCount: 1
    codePage: 0
    countryCode: 0
    badPasswordTime: 128769530029375000
    lastLogoff: 0
    lastLogon: 128742007081093750
    pwdLastSet: 128716053043750000
    primaryGroupID: 513
    objectSid:: AQUAAAAAAAUVAAAAF8sUcR3r8QcekDXQw9wAAA==
    accountExpires: 9223372036854775807
    logonCount: 0
    sAMAccountName: karl
    sAMAccountType: 805306368
    userPrincipalName: karl@support.jive.com
    objectCategory:
  CN=Person,CN=Schema,CN=Configuration,DC=support,DC=jive,DC=com
    dSCorePropagationData: 20081119220919.0Z
    dSCorePropagationData: 20081119220919.0Z
    dSCorePropagationData: 20081119220919.0Z
    dSCorePropagationData: 16010108151056.0Z
    mail: karl@fake.com
```

Synchronizing LDAP Users

You can manually synchronize users or synchronize them during a nightly batch job, but make sure you allow for performance and take care to use the correct rules.

Fastpath: Admin Console: People > Settings > Directory Server Settings > User Synchronization

Typically, a user's profile is synchronized to LDAP each time the user logs in to the community. This occurs if you selected **Synchronize User's Profile on Login**. You can also run synchronization nightly to catch up with any changes during the day. However, you may occasionally want to synchronize users manually. You may want to synchronize manually when:

- You have added a number of new users in LDAP who have never logged into the community

- You want to mass-disable community users from LDAP.

To set up synchronization:

1. In the Admin Console, click **People** > **Settings** > **Directory Server Settings**
2. Make sure you've defined a valid connection to an LDAP directory server. (If you don't have a working connection defined, you won't be able to see the rest of the configuration screens.
3. Click **User Synchronization**.
4. If you want to automatically synchronize fields every night, select **Scheduled sync task enabled**.
5. If you want to synchronize each user's fields whenever they log in, select **Synchronize user profiles on login**.
6. If you want synchronization to result in user accounts that have been deleted from LDAP being auto-disabled, select **Disable federated user accounts not found in the directory**. If you check this box, you can also disable users based on matching a field value if you set the User Disabled Field and User Disabled Field Value fields in the User Mapping tab. See User Mapping for more information about these fields.
7. If you want to synchronize right now, click **Run Synchronization Task Now.**.

LDAP Certificates

By default as of Jive 7.0, your Jive instance will verify that you have a valid SSL certificate installed in the JVM if you're running LDAP over SSL. But you can change this setting and run in an insecure mode if you need to.

Fastpath: Admin Console > **System** > **Settings** > **System Properties**.

To switch the SSL certificate behavior so that a valid certificate is not required, go to **Admin Console** > **System** > **Settings** > **System Properties** and change the system property "ldap.ssl.certverification" to **false**. You'll need to restart your instance after making this change.

LDAP System Properties

You can modify LDAP system properties to reset some elements of your LDAP configuration.

These settings are for expert users. To use system properties, go to **System** > **Management** > **System Properties**. Restart your instance after making any system property changes.

Table 12:

Property	Meaning	Sample Value(s)
ldap.ssl.certverification	The SSL certification verification switch	By default=true, which verifies the SSL certificate is valid when you're running LDAP over SSL. If you set this to false, you can run in an insecure mode.
ldap.serverType.id*	The type of LDAP instance	2=AD, 3=openLDAP, 4=other
ldap.host*	The hostname of IP address of the LDAP server	ldap.jive.com
ldap.port*	The port number of the LDAP server	389 (default) or 636 (SSL)
ldap.usernameField*	The LDAP field name used to look up user name values	uid
ldap.baseDN*	The Distinguished Name of the base of your LDAP tree	DC=support, DC=jive, DC=com
ldap.nameField^	The element key for the name attribute	cn
ldap.firstNameField^	The element key for the First Name attribute	givenName
ldap.lastNameField^	The element key for the Surname attribute	sn
ldap.emailField*	The element key for the Email attribute	mail
ldap.connectionPoolEnabled	Specifies whether to enable connection pooling. See http://download.oracle.com/javase/jndi/tutorial/ldap/connect/config.html	true
ldap.followReferrals	Specifies whether LDAP queries will follow referrals. This property should always be set to true for Active Directory.	true
ldap.adminDN*	The DN for the LDAP admin user. This user does not need to be a Jive user.	CN=AdminMan,OU=Domain Users,DC=support,DC=jive,DC=co

Property	Meaning	Sample Value(s)
ldap.adminPassword*	The encrypted password for the LDAP admin	a54313f2d3bc98fb5234566995246
ldap.adminPassword.key*	The key used to encrypt the admin password.	
ldap.adminPassword.encrypted*	Specifies whether or not the Admin password is encrypted. This property should always be set to true.	true
ldap.ldapDebugEnabled	Specifies whether LDAP debug logging is on. **Caution:** If ldap.ldapDebugEnabled is on (true), LDAP traffic can be logged, and user passwords can be printed in plain text to the application's `sbs.out` log file if connections to LDAP are unencrypted (non-SSL). It is your responsibility to ensure that your LDAP communication runs over an SSL connection. **Important:** LDAP logging is extremely verbose and should never be used in production unless Support recommends it. Using debug mode can cause serious performance problems or system failure.	false
ldap.sslEnabled	Specifies whether to use an SSL connection to communicate with the LDAP server.	false
ldap.initialContextFactory		
ldap.searchFilter	The filter applied to a remote directory when searching for users	
ldap.groupNameField	The field that maps a group to its CN in LDAP.	cn
ldap.groupMemberField	The field that maps a group to its members.	member

Property	Meaning	Sample Value(s)
ldap.groupDescriptionField	The field that maps a description of a group.	description
ldap.posixMode	Specifies whether to connect to LDAP in POSIX mode. POSIX groups store their member associations by common name (CN) rather than full distinguished name (DN).	false
ldap.posixEnabled	Specifies whether to connect to LDAP in POSIX mode. POSIX groups store their member associations by common name (CN) rather than full distinguished name (DN).	false
ldap.groupSearchFilter^	The filter applied to a remote directory when searching for groups.	(objectClass=group)
ldap.managerField	Maps the DN of a user's manager. Used when syncing relationship fields.	manager
ldap.photoField	Maps a photo to a user's profile.	photo
ldap.lastUpdatedField	Used to check if an LDAP record has been updated since the most recent sync.	creationdate
ldap.userGroupMember^	The field that maps a user to a group. This is a user attribute.	memberOf
ldap.userDN^	A RDN (relative to the baseDN) which contains users to sync to SBS.	ou=People
jive.sync.user.ldap	Specifies whether user synchronizations are enabled.	true
jive.sync.relationships.ldap	Specifies whether user relationships are synchronized from LDAP.	false
jive.sync.profile.ldap.photo	Specifies whether profile photos are synchronized from LDAP.	false
jive.sync.profile.ldap.login	Specifies whether profiles are synchronized at login.	false
jive.sync.auto.disable	Specifies whether Jive should disable user accounts which cannot be found in the LDAP directory.	

Property	Meaning	Sample Value(s)
jive.sync.auto.disable.att.name	The name of the attribute which indicates whether or not an account is disabled in LDAP.	userAccountControl
jive.sync.auto.disable.att.value	In Active Directory, use Microsoft article 305144 as a reference for setting user account properties. You can also set up a bit-specific filter such as: `userAccountControl:1.2.840.113556.1.4.803:=2`	514 (see link)
jive.usernames.case.insensitive	Setting to `false` makes case sensitive comparisons when users register or log in, for example, **bbrag** is a different user than **BBragg**. When set to `true`, there is no disctinction between **bbragg** and **BBragg**. You may need to set this property to `false` when existing usernames in your Lightweight Directory Access Protocol (LDAP), Active Directory (AD), or single sign on (SSO) are case sensitive.	true
GroupManager.className	Controls whether or not permission groups are synchronized from LDAP.	com.jivesoftware.base.ldap.LdapG (for LDAP groups) com.jivesoftware.base.database.D (default group manager)

Setting Up Single Sign-On

Single Sign-On allows you to integrate Jive authentication with an external identity provider.

You can use Jive's local database storage to authenticate users out of the box. However, you may find it useful to integrate your external identity provider with Jive so you can centralize identity management and provide your users with a consistent login experience. Many Jive communities implement SSO as part of a larger audience profile synchronization effort that includes LDAP and/or SAML.

Getting Set Up

If you already have a Jive community with more than a few users set up, you need to plan a migration strategy before you implement SSO, particularly if you will use SAML or Kerberos. If you implement SSO without migrating users first, you will orphan your existing users—information they contributed to the community will still exist, but they will be unable to log in under the credentials that created that content.

If you need help migrating your user data to another authentication scheme before you enable SSO, you should contact Jive Professional Services.

Understanding SSO with SAML

When you implement single sign-on (SSO) with SAML 2.0, information for each user is passed from the IdP in the form of a digitally-signed XML document.

SAML is a protocol for exchanging authentication credentials between two parties, a service provider (SP) and an identity provider (IdP). In this case, Jive plays the role of SP. The SP sends a request for authentication to the IdP, which then tries to authenticate the user. Authentication typically uses a username and password. The IdP typically also contains user information such as login ID, name, email address, department, and phone. After authenticating the user, the IdP then sends a SAML XML response message back to the SP, which then logs the user in.

Depending on your requirements, you can use SAML solely for authentication users; for group authorization; or for populating the Jive profile by synchronizing from the IdP on login.

Jive authentication through SAML includes the following stages:

1. A user visits Jive and requests a page that requires authentication.
2. Jive redirects the user to the configured IdP. The request URL includes a base64-encoded version of some request XML.
3. If authentication doesn't succeed, the user sees a login screen.
4. The IdP sends an encoded XML-based response in a redirect to Jive. If the user was successfully authenticated, this response includes the information we need to create a Jive representation of the user.
5. Jive parses the XML and validates the necessary signatures, decrypting if necessary. A valid response from the IdP at this point indicates the user has been successfully authenticated.
6. Jive parses the XML response from the IdP and creates or updates the user, using any override attributes you specified in Jive. If users have been seeded beforehand and shouldn't be updated, profile sync can be disabled.
7. The user is authenticated with Jive and redirected to the requested destination.

Getting Ready to Implement SAML SSO

Before you begin configuring a SAML SSO implementation, make sure you read about the requirements and best practices.

A successful SAML implementation requires the following prerequisites.

- An identity provider that complies with the SAML 2.0 standard. For more information, see SAML Identity Providers. You should make sure you have expert knowledge of how to configure your identity provider before proceeding.
- Familiarity with the SAML 2.0 specification. Before you begin the process of configuring Jive as a SAML 2.0 service provider to your IdP, you need to understand the details of how SAML works or else enlist the assistance of a SAML professional. The links that follow can supply some of this information.

- Oasis SAML Technical Overview (.pdf)
- Wikipedia entry on SAML 2.0

SSL Implementation

It is theoretically possible to implement SSO without SSL, but this raises some difficult security challenges. You should implement SSL, and you'll find it much easier to set up SSO if your jiveURL uses https, not http.

Disable Storage Provider File System Caching

Before you begin setting up SAML, go to **System** > **Settings** > **Storage Provider**and click **Edit**. Then select **No** under Cache Enabled. You won't be able to modify your IdP metadata unless caching is disabled.

LDAP Integration

If you're going to use LDAP in conjunction with SAML, we recommend using SAML for authentication only, while using LDAP for user provisioning, user deprovisioning, and profile synchronization. LDAP setup can be a lengthy process including VPN setup and testing, so allow time for this setup process if you're implementing LDAP as part of your SSO implementation.

Migrating Existing Jive Users

If you already have existing users on your community and have not yet implemented SAML, the best practice for migrating users is to enable **Username Identity** to look up existing users by username. In most cases, you should also enable **Merge Local Users** to ensure that existing users are automatically federated. This recommendation assumes that either the email address or the username matches between existing accounts and the SAML response. If neither of those fields matches, you can:

- Update the existing email addresses in Jive before using Username Identity to sync them
- Update the usernames in Jive before using Username Identity to sync them
- Add the external IDs in Jive and federate the users via another method. (You can use the REST API or, if you need more assistance, a partner or Professional Services can handle this by creating a database script.)

Caution:

If you may have unfederated local users that you do not want to merge, you should not select **Merge Local Users**. Instead, mark only the accounts you want to merge as federated before enabling Username Identity.

Required Information

Before you begin the configuration process, you must have the following information available:

- The IdP metadata (URL location or file content). Specifying a URL usually makes updates easier. Your metadata needs to include the following information:

- The IdP entity ID
- The IdP KeyInfo element
- The IdP Location that defines your endpoints

If you can't verify that this information is included, talk to your IdP administrator.

Note: To integrate Jive with SAML, you need the complete metadata file, not just the information described above.

- The friendly attribute names sent with each SAML assertion.

Planning for Jive User Provisioning and Profile Synchronization

When you implement SAML, you need to decide on a strategy for which members of your organization will be included in the Jive Community, and with what rights. For example, you'll need to decide whether all your organization's users should be able to create accounts in the Jive community, and whether you will assign them to authorization groups. If you're primarily responsible for the technical implementation of this feature, make sure you discuss these decisions with your Community Administrator.

Configuring IdPs for SSO

Certain IdPs require special configuration before you can set up SAML SSO.

The following list describes some known configuration prerequisites for specific IdPs. These are tips and, obviously, do not provide a complete description of required IdP configuration for your identity provider.

ADFS

Set the expected digital signature to SHA-1	ADFS expects the digital signature to be SHA-256, but Jive sends it as SHA-1. To change this expectation, go to the Advanced tab of your Relying Party Trusts profile and set the secure hash algorithm to SHA-1.

Siteminder

Use the jive entityID as the Siteminder profile name	Typically, the Jive entityID, which is set using the Base metadata URL in the Advanced tab of your SAML SSO settings, is the same as the jiveURL.

SAML Identity Providers

Jive can be integrated with a wide variety of SAML IdPs.

Jive regularly tests SAML support with integrations to the following IdPs:

- Microsoft ADFS (the most common SSO provider used by our customers)
- Shibboleth: (the open-source standard for IdPs)

and can typically assist with configuration for these providers. Troubleshooting assistance for other IdP integrations is available through Jive Professional Services.

Configuring SSO with SAML

SAML configuration

Fastpath: Admin Console > **People** > **Settings** > **Single Sign On** > **SAML**

Understanding SSO with SAML

Caution: Before you configure SSO, make sure you have a migration strategy for any existing Jive users. Implementing SSO without migrating your users to your new authentication provider will orphan existing user accounts, so users can't access their community content.

You can use the SAML settings dialogs to set up single sign-on with an SAML identity provider, or to enable, disable, or tweak a configured SAML SSO configuration.

Note: Before you begin configuring SAML setup, please read Getting Ready to Implement SAML SSO.

Setting Up the IdP Connection

To begin setting up the connection between Jive and your identity provider, use the following steps:

1. In the Metadata tab, type the metadata URL for your SAML provider and click **Load**. If you don't have a metadata URL, you can click **Edit Metadata** to paste in the XML containing the connection metadata. If there's a firewall between the Jive server and your IdP server, you'll have to use the cut-and-paste method. Note that this is the only time a connection between these two servers is required.
2. Optionally, edit the metadata if it contains any non-conforming code and click **Save Settings** to load it.
3. In the User Attribute Mapping tab, map the user attributes in the Jive profile to your IdP's attributes. For more information about this topic, see User Attribute Mapping. Note that importing or saving your metadata populates the General tab with a list of attributes from your IdP, so you can use it as a reference when you specify the attributes you want to map.
4. If you want to assign users to groups by passing a special group attribute from your IdP to Jive, select **Group Mapping Enabled**.
5. Click **Save Settings**.
6. Click **Download Jive SP Metadata** at the top right of the SAML tab to download the Service Provider metadata you'll need to complete your IdP-side configuration.

User Attribute Mapping

User Attribute Mapping is used to identify fields in the Jive profile that you plan to populate from the IdP profile by synchronizing them on login. To map a field, specify the exact IdP attribute used to identify it in the text box and select the **Federated** check box. Any fields you don't map will be user-configurable in the Jive profile settings. (A field that you specify, but do not mark as federated, will be populated with the specified value but still configurable.) By default, Jive uses the NameID property as the key unique identifier for a user. You can select **Override Subject NameID for Username** and specify a different attribute if you want to use a different key identifier.

Group Mapping

You can assign users to security groups automatically by passing a special group attribute from the IdP to Jive. Select **Group Mapping Enabled** on the Advanced tab to enable this functionality and provide the group mapping attribute. The group mapping attribute will be used to get security group names from each assertion. If the corresponding groups with these names don't exist, they will be created when you synchronize, and users will be added to these groups. Note that SAML SSO does not support mixed group management. You can either manage your permissions groups using the IdP, or using permission groups created in Jive.

General SAML Integration Settings

The following settings on the General tab are used in a typical SSO configuration.

Debug Mode	Enable to provide detailed logging for troubleshooting authentication problems. You need to enable this setting during setup and validation, but turn it off in production.
Username Identity, Merge Local Users	Enable the Username Identity setting if you have existing users in Jive and you are newly implementing SAML. (You don't need to enable it if all your accounts will be created through SSO auto-provisioning.) Jive uses a permanent, unique identifier (External ID) to connect existing users with their SSO login. If users have never logged in using SSO, they will not have an associated external ID. When **Username identity** is enabled, Jive will map any existing federated users to an existing user account using their username or email address during their first SSO login. To automatically federate existing users on login, you should also enable **Merge Local Users**. If you use Username Identity without also enabling **Merge Local Users**, make sure your existing users are marked as federated users. Otherwise, unfederated users will not be synchronized.
Provision new user account on login	Enable this setting to ensure that when a new user logs in, the user account is automatically created within Jive. This setting is enabled by default and

	should not be disabled unless you seeded the Jive community with users before enabling SSO.
Enable disabled user account on login	Enable this setting to reenable a disabled user's Jive account when s/he logs in.
Sync user profile on login	Enable this setting to update users based on the remote user profile each time they log in.
Sign Assertions	This option is enabled by default. It requires that to pass validation, the `AuthnResponse` must have a valid signature on the Assertions within the Response, If the Response itself is signed, it also requires that the signature be valid. (It does not require that the Response be signed.) Clearing the check box enforces that the Response must be signed, and any signature on the Assertions is ignored. Most IdPs sign the Assertions section in the AuthnResponse. If you use SFDC, however, you should clear this check box, because SFDC only signs the entire Response.
SSO Service Binding	Defines whether Jive should send the request to the IdP with an HTTP GET Redirect or a POST. The default service binding is urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST, which is the most commonly used binding. In order to use this binding, you must ensure that a Location binding with this value is in the IdP metadata. POST is typically preferred to Redirect, because older versions of Internet Explorer and some firewalls have restrictions on the length of the HTTP path. **Note:** If you're configuring ADFS, keep in mind that using POST can cause problems for users on Safari.
Logout URL	By default, `/sso/logged-out.jspa` is a page that doesn't require authentication. If guest access is disabled, users need to land on a non-authentication-requiring page. (Otherwise they'd be automatically logged in again.) If guest access is enabled, you can set this value to `/index.jspa` to redirect the user back to the instance homepage,

	but as a guest user instead of as the account they were logging out of. Another option is to set it to the IdP logout URL, so that the user is logged out of both Jive and the IdP. We do not support the SAML SingleLogout (SLO) protocol. Changing this setting requires you to restart the Jive server. **Note:** If you specify a relative URL as the logout URL, such as `/sso/logged-out.jspa`, it needs to be a unique substring among all URLs within Jive, because any URL that matches this string will not trigger the SSO process. For example, setting the string to `/` is a bad choice, because this value would match all URLs in Jive and entirely prevent SSO from working.
Maximum Authentication Age	Identifies the maximum session time (in seconds) that's set for the IdP. The default setting is 28800 seconds, or 8 hours. However, to avoid login failures, you need to set this to match the maximum session set on the IdP. (Some IdPs are set to expire sessions less often.)
Response Skew	Specifies the maximum permitted time between the timestamps in the SAML Response and the clock on the Jive instance. The default value is 120 seconds. If there is a significant amount of clock drift between the IdP and Jive, you can increase this value. The same value is also used for the skew in the NotBefore check in the response. If you see an error indicating a problem with the NotBefore check and you aren't able to fix the clock difference problem, you can try increasing this value. However, increasing the response skew value can increase your security risk.

Advanced SAML Integration Settings

The settings on the Advanced tab are used to refine and troubleshoot a SAML integration.

The following settings on the Advanced tab control some less commonly used SSO configuration.

Request Signed	This setting determines whether the saml request is signed or not. Enabling this setting can increase security, but it's incompatible with some IdPs. This setting is disabled by default.
Base metadata URL	This value sets the desired URL for the entityID and endpoint URLs. This URL should be an https. If you aren't using a URL with https, you need to get help from Support to continue setting up SSO.
Enable Username Confirmation for New Users, Enable Email Confirmation for New Users, Enable Name Confirmation for New Users	These settings define the behavior for new users when they first log in. When they're selected, users will be asked to confirm that they want to use the relevant value (username, email, or name) that is provided by the Identity Provider. They can also change these values if they wish. By default, these settings are all disabled, since in most cases the intended result is for users to be forced to use the username, email, and name defined for them in the corporate directory. The Enable Name Confirmation setting has an additional application when users typically log in with either a single-word username or an email address, but may need the option to provide a first/last name combination. If you select this check box, users can also modify those profile fields after initial login. **Note:** These fields also apply to any users who may be logging into your community using External ID.
External Identity is Case-Sensitive	Use this setting to determine whether the value used for the external identity should be case-sensitive. You should disable this setting in a case where the external identity value changes under different circumstances, for example when it's sometimes all lowercase and sometimes all uppercase.
Force Authentication	Forces any user with an existing IdP session to log in again.
Passive Authentication	When guest access is enabled, issues a SAML AuthnRequest upon first access with "isPassive=true", which should cause the IdP to

	simply redirect back to Jive if the user doesn't have an active session with the IdP.
NameID Format	For most IdPs, using the default setting is correct.
NameID Allow Create	By default, this check box is cleared. You should leave it cleared unless you receive an error about NameID creation while setting up your SAML integration.
Sign Metadata	Specifies that metadata should be signed. You should clear this check box UNLESS your IdP requires that the metadata be signed. If you use ADFS, you must clear this check box.
IDP Want Response Signed	Use this setting to add a configuration to the SP metadata that tells the IdP that the SAML response should be signed, instead of only the assertions within the response. You should not enable this setting unless Support recommends it.
Requested AuthnContext	Along with Requested AuthnContext Comparison, this optional setting is used to add additional information to requests in certain specific cases. It's disabled by default.
Requested AuthnContext Comparison	Along with Requested AuthnContext, this optional setting is used to add additional information to requests in certain specific cases. It's disabled by default.
RSA Signature Algorithm URI	Defines the algorithm used in the digital signatures used within the SAML messages. Most IdPs use the default value of http://www.w3.org/2001/04/xmldsig-more#rsa-sha256. You may need to change this value if your IdP uses a different algorithm.
Require Valid Metadata	Use this setting to determine whether the IdP metadata you provide to Jive should be validated with respect to any `validUntil` timestamps. Some IdPs generate metadata with arbitrary `validUntil` timestamps on their metadata, which can cause validation to fail and keep Jive from running. This option is disabled by default.

Include Scoping	This check box is unselected by default. If you use ADFS, it must remain unselected. Some IdPs may require a scoping definition.
Proxy Count	This setting specifies the maximum number of proxies any request can go through in the request to the IdP. The default value is 2. If your IdP needs more than 2 proxy redirects, adjust this value upward.
Key Store	This feature is used to configure Jive with a specific certificate that will be used for encryption and signing in place of the self-signed certificate Jive generates. You should only use this feature after consulting with Support.

SAML SSO Attribute Mapping Tips

Determining your IdP's Attributes

The easiest way to figure out how your IdP's attributes are set is to set the Email field in the General tab of Jive to something you know isn't in the response, like xxxxemail, and then look at the error message for all the available attributes in the SAML Response. Many IdPs assign both a Name and a Friendly Name to each assertion attribute. When you're setting up Attribute Mapping, you should use Name.

By default, user mapping uses the SubjectNameID attribute, which defines the user name, as a unique identifier to link the Jive account with the IdP identity. You can use a different attribute for either the user name or the External Identifier. The External Identifier should be a value that will remain the same even if the user name and email address change. In ADFS, this attribute will typically be the unique objectGUID attribute.

For ADFS, the Name value typically looks like a URL, for example http://schemas.xmlsoap.org/ws/2005/05/identity/claims/email

Jive doesn't support mapping to complex profile fields such as multiple select lists or addresses.

Minimum Required Mapping Fields

By default, Jive user accounts require Username, Email, Firstname, and Lastname to be populated. If your SSO server will be used to generate accounts automatically on login, make sure the following fields are mapped:

- ExternalIdentity
- Username
- Email

Setting Up an Entry Page for External Users

The Login Entry Page settings determine the initial login page wording if your community uses SAML SSO and also has externally accessible groups enabled.

Fastpath: Admin Console: People > Settings > Single Sign On > Login Entry Page

If you use SAML SSO for authentication, and you've also enabled external users (users outside your internal network) to be invited to groups, you can use the Login Entry Page settings to customize how both community users and external users experience the login page. You can use the default wording provided, or edit the wording in all the supported languages. When users access the login page, their browser settings will determine which language they see.

To configure the login entry page:

1. Make sure SAML SSO is configured in your community.
2. Enable external groups. You should now be able to see the Login Entry Page dialog under **People** > **Settings** > **Single Sign On**.
3. Select the language you want to edit and change the text to how you'd like it to appear on the initial login page. This is the page users will see the first time they navigate to the site directly, as opposed to clicking through from an invitation. You'll probably want to change the text for all the languages your users typically use when accessing your site. You can change the page title and the field labels as well as the explanatory text. (Community user instructions and external user instructions are both displayed at the same time, in different regions of the page. You can see what this looks like, and preview any changes you make, using the **Preview Pre-login Page** button.) Keep in mind when you design your text that your regular community users will typically be logged in automatically using SSO, while external users will need to provide user name and password to access the site.
4. Click **Save**. If you want to revert to the original text at any time, you can click **Reset to Defaults**.

Troubleshooting SAML SSO

Running SSO in debug mode will help you troubleshoot your integration.

An attribute is missing, or was mistyped

In the following sample error message, the name of the attribute configured for the user's email address was named `email`, but that doesn't exist in the saml message. In this example, `MAIL` is the name of the correct attribute.

```
com.jivesoftware.community.aaa.sso.SSOAuthentica
 User did not have the required
 attributes send from the identify
 provider. Missing attribute: email.
 Given attributes: [MAIL, title,
 companyname, FIRSTNAME, LASTNAME]
```

"Missing attribute" field in an error message is blank

If you see a message like this:

```
com.jivesoftware.community.aaa.sso.SSOAuthentica
 User did not have the required
 attributes send from the identify
 provider. Missing attribute: .
```

Jive is trying to sync a single name as Firstname and Lastname. To work around this problem, set the system property `saml.nameField` to the same attribute the first name is populated from.

Authentication works on some nodes, not others

You may discover that the certificates in the metadata for each node are different: Jive metadata won't be the same on each node and so authentication will succeed on some nodes and fail on others. To verify that the same key is being used on each node, go directly to the path `/saml/metadata` for each node. This problem occurs when Storage Provider file system caching is enabled. To disable it, go to **System** > **Settings** > **Storage Provider**and click **Edit**. Then select **No** under Cache Enabled.

"Responder" message.

If you get any status message in this format:

```
            <samlp:Status>
            <samlp:StatusCode

 Value="urn:oasis:names:tc:SAML:2.0:status:Respo
>

 <samlp:StatusMessage>something_is_wrong</
samlp:StatusMessage>
            </samlp:Status>
```

this indicates a problem with your IdP configuration.

An assertion fails on the notBefore condition

If the IdP clock is ahead of the Jive clock by even a second, the notBefore check fails and you get the message

```
Assertion is not yet valid,
 invalidated by condition
 notBefore ?
```

This problem can be caused by clock drift on either end, but you can also try addressing it by adjusting the Response Skew setting in the General SSO settings.

username doesn't exist in attribute

If you see the following message:

```
ERROR
 org.springframework.security.saml.SAMLProcessin
 - There was an error during SAML
 authentication
java.lang.IllegalArgumentException:
 [Assertion failed] - this argument
 is required; it must not be null
```

The attribute with the username does not exist—it may be in the Subject NameID instead, in which case you should make sure the Override Subject NameID for Username checkbox is cleared in the General tab of your SAML settings. Otherwise, you may need to add the `username` attribute to the SAML message.

IdP-Specific SAML SSO Issues

Some problems and workarounds only apply to specific IdPs.

ADFS

Responder error with details mentioning the Scoping element.

To fix this problem, select the **Include Scoping** check box in Advanced Settings.

PingFederate

A UAT instance doesn't work in the same browser where a production SSO IDP session existed

This problem is caused by a session cookie handling problem. You can work around it by always creating a new browser session before testing in UAT.

Siteminder

IdP metadata won't save in Jive

OpenSAML has a bug where the validUntil timestamp on the IdP metadata's IDPSSODescriptor is checked incorrectly, and will only pass validation if the timestamp is invalid. The workaround is to remove the IDPSSODescriptor validUntil attribute from the metadata.

AudienceRestriction attribute contains incorrect or multiple entityIDs for jive instance	This problem occurs when the SP profile name in SiteMinder is not the same as the entityID in Jive, causing a validation error.

Understanding SSO with Kerberos

When you implement single sign-on (SSO) with Kerberos, LDAP handles all the authorization and user synchronization, while Kerberos handles authentication.

Note: Kerberos is only supported with on-premise installations of Jive. It is not available for Jive-hosted communities.

Kerberos is an authentication protocol that is meant to be used in conjunction with an LDAP-enabled instance. LDAP handles all authorization and user synchronization, while Kerberos handles authentication. On Windows and Mac machines that are joined to an Active Directory domain, users can seamlessly log into Jive without entering a username or password, or even seeing a login screen. Users who are not logged into the domain on their computers will still see a standard login form. Because authentication uses a single token passed from the operating systems, no redirect is required. The token is verified against the configured Key Domain Controller (KDC), and if it's valid, the user is logged in.

Communication with the KDC typically uses the standard service principal string and password. However, you can also specify a keytab and krb5.conf file.

Configuring SSO with Kerberos

Fastpath: **Admin Console** > **People** > **Settings** > **Single Sign On** > **Kerberos**

Understanding SSO with Kerberos

Important: Before you configure SSO, make sure you have a migration strategy for your existing Jive users. Implementing SSO without migrating your users to your new authentication provider will orphan existing user accounts, so users can't access their community content.

Setting Up Kerberos SSO

Service Principal	The service principal used to communicate with the KDC and validate any user tickets passed to Jive. Typically, the Service Principal value is the user name for an account.
Realm	The realm for the service principal account user name you specified.
(KDC) Key Distribution Center	The hostname for the key distribution center. You may not need to provide this information if the realm already resolves to the KDC.

Password	Specifies the password for the service principal account user name you specified.

Advanced Settings

The following settings on the Advanced tab control some less commonly used SSO configurations.

Debug Mode	Enable to provide detailed logging for troubleshooting authentication problems. You should disable this setting in production.
Use Keytab for Authentication	Enable to specify a keytab file as an alternate credentialing method. To upload your keytab file, you need to Base64-encode it and paste it into the text box provided.
Use KRB Configuration File	Enable to specify a krb5.conf file. Then paste the file contents into the text box provided.

Understanding SSO with External Login

When you implement single sign-on (SSO) using an external login, users can choose to log in using any of several different authentication providers including Facebook, Google, and OpenID.

External logins are a good choice for public communities because authentication can be passed to a third-party provider. The community user enters credentials on the provider site. The authentication token is then passed back and verified on the Jive side. Community users can log in with any number of different providers and have all their details pre-populated. For sites that support an avatar attribute, avatars are synchronized as well.

An external login implementation can optionally include Facebook Connect authentication. Both OpenID and Facebook Connect use the Attribute Exchange standard for exchanging information, which enables Jive to pull in profile information about new users. After login the user sees a confirmation page and can verify profile information, pick a username (if this information isn't prepopulated from the profile), and proceed to the Jive community.

OpenID with Facebook Authentication

Enabling Facebook authentication requires you to:

- Set up an app on the Facebook developer site. You'll need both the application id and the application secret to configure single sign-on.
- Under **People** > **Settings** > **SAML** > **Advanced** in the Jive admin console,select the **Enable Username Confirmation for New Users** check box.

Configuring SSO with External Login

Fastpath: Admin Console > **People** > **Settings** > **Single Sign On** > **External Login**

Understanding SSO with External Login

Important: Before you configure SSO, make sure you have a migration strategy for your existing Jive users. Implementing SSO without migrating your users to your new authentication provider will orphan existing user accounts, so users can't access their community content.

To implement SSO for Jive with external logins, you set this page to **Enabled** and select the top four identity providers you want users to choose from on your site. Select identity providers by reordering them into the yellow area on the page. If you disable an external login type after enabling it, Jive users will need to authenticate against Jive directly instead of using an external login.

To troubleshoot authentication problems, you can enable **Debug Mode**. You should disable this setting in production.

Facebook Configuration

Before you can enable Facebook login, you need to create an app on the Facebook developer site. Provide your app credentials (the Application ID and secret) to complete SSO authentication with Facebook. When you're creating your Facebook app, you'll need to provide your Jive URL for both the **App Domains** field and the **Website with Facebook Login** field.

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.

Enabling the Antivirus Feature

The antivirus feature helps make your community more secure.

With the antivirus feature enabled, when a user tries to upload an external file to the community (for example, a Microsoft Word document, an Adobe PDF, and so on), the file will be scanned for a virus before being posted. If a virus is found, the file will not be posted in the community.

The antivirus feature is powered by ClamAV. Jive polls the ClamAV database every thirty minutes for virus updates.

Cloud customers will need to contact Jive Support to enable the antivirus feature. In addition, you'll need to create an "Antivirus Management" group (**People** > **Management** > **Create User Group**) and add users to it who will receive an Inbox notification whenever the antivirus feature finds malware. The user who attempted to upload a virus will be listed in the notification.

On-prem customers can enable the antivirus feature themselves as follows:

1. In the Admin Console, go to **System** > **Settings** > **Antivirus** and select **Enable**.
2. Click **Save**, and then refresh the browser page. This will populate the URL field from Tenancy Services.

3. For Notify Author, select **Yes** if you want the application to send the author an Inbox and email notification when a file is rejected. You can also designate an administrative group of users to receive a notification.
4. Set the timeout in milliseconds for the antivirus scanner to complete a scan. The default is 300,000 milliseconds.
5. Click **Save**.

Managing Impact Metrics

You can see Impact Metrics for Documents, Blog Posts, Discussions, and Videos when you enable Cloud Analytics for your site. You can see Impact Metrics for only Documents and Blog Posts if your site instead uses the Analytics database.

Jive On-Premise and Jive Hosted installations use the Analytics database by default, but you need to configure and enable the database to use it. If you want to use Cloud Analytics and expose more Impact Metrics features, you can create a support case in the Jive Community using the form found here in the Jive Community.

Features Available When You Enable the Cloud Analytics Service

- Top Departments and Department Filtering
- Email Tracking Counts
- Top Referrers List
- Subscribers Toggle
- Impact Metrics for Discussions and Videos
- Real Time Results

Note: You can avoid the 15-minute delay and get Impact Metrics on content created prior to it being enabled when you use Cloud Analytics service instead of the Analytics database.

Configuring the Analytics Database

Identify the Analytics database so Community Manager Reports and Impact Metrics can use it to collect data.

Community Manager Reports and Impact Metrics data for content begins accumulating when you configure and enable the Analytics database. You cannot capture Impact Metrics data from before this happens unless you use Cloud Analytics instead of the Analytics database.

Note:

Fastpath: Admin Console: System > Settings > Analytics > Database

To configure the database:

1. Select the preset database driver and use the information prefilled into the Database URL and JDBC Driver Class fields. Make sure you change [host-name] and [database-name] to their actual values.

2. Enter the database user name and password so Jive can establish a connection to the database. As with the core database user, the Analytics database user should be able to create and modify schemas, and they have permission to select, insert, update, and delete queries.
3. Use the defaults for Minimum Database Connections, Maximum Database Connections, and Connection Timeout fields. You can adjust these fields to fit your community's specific needs later, if necessary.
4. Click **Test Connection** to see if Jive can make the connection to the database.
5. Click **Save**.

Enabling the Analytics Database

After configuring the Analytics database, you can enable it to start collecting impact metrics and Community Manager Reports data on documents and blog posts.

Fastpath: Admin Console: System > Settings > Analytics

Click **Enabled** to begin accumulating data from Jive in the Analytics database.

Enabling Analytics Events

Once the Analytics database is configured and enabled, you need to enable all Analytics events.

Context for the current task

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

1. Select all events in the list.
2. Click **Save**.

Configuring Structured Outcomes

The Structured Outcomes feature lets users mark top-level content items, as well as comments and replies, as Final, Official, Outdated, and so on. You can select which marking options community users will see, or disable them altogether. You can also limit this feature to specific users or a group of users.

To limit this feature to specific users, you'll need to assign them the Mark Outcomes permission. Be sure to read Limiting Structured Outcomes to Specific Users on page 74 for more information.

Note: Helpful and Correct Answers are not part of the code base of the Structured Outcomes feature.

1. In the Admin Console, go to **System** > **Settings** > **Structured Outcomes**.
2. From here, you can enable and configure Structured Outcomes, or disable them altogether:

Option	Description
Enable and configure	To select which badges users will see, make sure that Structured Outcomes are **Enabled**, and then

Option	Description
	select the badges that will display to users (Final, Official, Outdated, and so on).
Disable	To disable this feature, click **Disabled**. Note that if Structured Outcomes were previously enabled and used in the community, users will still see the previously marked Outcomes badges on content items; but users will not be able to mark any content items from this point forward.

3. Click **Save**.

Limiting Structured Outcomes to Specific Users

You can limit the Structured Outcomes badging feature to specific users, or a group of users, by giving them Mark Outcomes permissions. Only these users will see the marking options on content. All users will be able to see the badges that are assigned to any content items.

1. In the Admin Console, go to **System** > **Settings** > **Structured Outcomes** and make sure **Enabled** is selected.
2. Click **Yes** beneath "Limit the marking feature to those users who are granted the "Mark Outcomes" homepage permission," and then **Save**.
3. Go to **Permissions** > **Home Page Permissions** and select the user or group of users whom you want to see the Structured Outcomes marking options.
4. Click **Edit Permissions** > **Mark Outcomes** > **Set Permissions**.

Configuring Badge Thresholds

You can configure when the Most Liked badge will be displayed on top-level content items, and when discussions marked as questions will display the Assumed Answered badge.

The Most Liked badge is displayed on top-level content items that meet the threshold criteria set in the Admin Console. When the Most Liked badge is displayed, users can click on the badge to see the comments or replies with the most Likes.

The Assumed Answered badge is displayed on discussions marked as questions (for example, the author selected the "mark this discussion as a question" option when creating the discussion) that do not have any replies marked as Correct Answer but do have a configurable number of replies marked as Helpful.

To change the default settings for these options:

1. In the Admin Console, go to **System** > **Settings** > **Structured Outcomes**.
2. Set the following:

Setting	Description
Minimum number of comments or replies before the Most Liked badge is displayed	There must be more than this number of comments on the top level content item before

Setting	Description
	the Most Liked badge is eligible to display. For example, if this were set to 4 and a document had 3 comments, the document would never display the Most Liked badge, no matter how many Likes one of the comments had.
Minimum number of Likes on a comment or reply to be included under the Most Liked badge	For an individual comment or reply to be included in the list displayed when a user clicks the Most Liked badge, the comment or reply must have at least this number of Likes.
Maximum number of replies or comments to be displayed under the Most Liked badge	This is the maximum number of replies or comments that will be included in the list displayed when a user clicks the Most Liked badge. For example, if you set this to 10, and there are more than 10 comments or replies that qualify to be displayed, only the 10 most-liked comments or replies will be displayed in ranking order in the list.
Minimum number of replies flagged as Helpful before the question is marked Assumed Answered	For discussions that are marked as questions (in other words, the author has selected the "mark this discussion as a question" option when creating the discussion), the Assumed Answered badge will display on the discussion after this number of Helpful replies have been marked *and* if no replies have been marked Correct Answer.

3. Click **Save**.

Disabling the Your View Feature

The Your View feature allows your community members to create a page just for themselves that they can configure with a variety of data tiles. Your View helps community users quickly navigate to their favorite people, places, and content. This feature is enabled by default.

The Your View tab appears as a menu item in the left sidebar navigation, along with the links to Inbox, Activity, and so on. If you disable Your View, the tab does not appear at all.

To disable the Your View feature:

1. In the Admin Console, go to **System** > **Settings** > **Your View**.

2. Click **Disabled** and then **Save**.

Configuring Document Options

As the administrator, you can configure how uploaded documents are handled using the Admin Console.

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.

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.

Use **Read Tracking Age Threshold** to set the amount of days after which unanswered discussions will be marked as read.

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 here.

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

You can **enable** or **disable** the Correct Answer feature in your community. With this feature enabled, you can collect stats about Correct Answers in your community, such as the number of Correct Answers on a given day (refer to the separate Community Manager Reports documentation for more information). There can be only one Correct Answer per discussion. The following kinds of users can mark a reply as the **Correct Answer** on discussions marked as questions.

- Community administrators
- Owners of the place where the question was posted
- The user who posted the question

Note that 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 place owners can mark a discussion as a question at any time (but they cannot unmark 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

Blogs and blog content can be managed in several ways depending on their location.

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 using the Admin Console. A person who has been assigned permission to do so can also create their blog in the community. 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.

Blog Type	Scope	Creating	Permissions	Management	System-Wide Settings
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. Even if you have Enabled blogs here, you will still need to set the permissions for users to create blogs on **Permissions** > **Blog Permissions**. Be sure to read Setting Global Blogs Permissions.
Comments	Enable or disable blog post comments. Disabling comments will cause comments not to be visible to community users. 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, without restriction.

For example, you can migrate a space blog so that it becomes a group blog. 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 user name for the person whose blog it should become (you can also browse for the user name). A person can have only one user blog.

3. Click **Submit**.

Configuring Spell Check

As a community manager, 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**

Disabling Projects

If your community includes the Projects feature, you can disable it if your community won't be using projects.

Fastpath: Admin Console: System > Settings > Projects

Disabling the Projects feature essentially means hiding project-related user interface elements. For example, Projects won't appear on the Create > Places menu or the Places page. If there are already projects in the community when you disable the feature, those projects will become inaccessible -- in other words, 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.

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 Inbox of the receiver(s). You can enable or disable direct messages for users from the Admin Console. By default, direct messages are disabled for internal Jive communities.

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

You can require that users must be connected to send direct messages or shares to each other. 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

You can enable and disable content sharing from the Admin Console.

The sharing feature allows users to alert others about interesting content items. Shared content notifications are private and appear only in the Inbox of the receiver(s). By default, sharing is disabled for internal Jive communities.

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

You can require that users must be connected to send direct messages or shares to each other. 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.

Enabling Social Media Sharing

You can enable or disable the ability of community users to share community content to a variety of social media channels, such as Facebook, Twitter, and Gmail. By default, this feature is disabled. For security reasons, we recommend not enabling this feature in internally-facing communities (typically those that involve only employees or other internal audiences).

When you enable this feature, users will be able to share documents, discussions, and blog posts on a variety of social channels. Users can even share community places if a place owner has enabled the Social Sharing widget in the place. You have the option of enabling some channels and not others.

In addition, you have the option of tracking your community's sharing stats via AddThis.

1. In the Admin Console, go to **System** > **Settings** > **Social Media Settings** and **Enable** social sharing.
2. You can enable or disable click tracking; this is optional. If you enable this, AddThis will collect your community's sharing stats. You'll also need to specify your AddThis profile ID. (If not, leave the profile ID field blank).
3. In the Toolbox HTML field, select how you want your sharing buttons to be displayed for users in your community (vertical, horizontal, and so on) as well as which channels to feature (Facebook, Twitter, and so on). For specific code illustrations, refer to the documentation from AddThis.
4. Click **Save Settings** when you're finished.

Understanding Embedded and Attached Images

Images attached to content are handled and displayed slightly differently than images that are inserted using the insert image icon.

Users can attach various kinds of files 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, and so on. When a user *attaches* an image, a preview of the image shows with its link. Previewing makes it easier for people to see whether it's the image they want before clicking its attachment link. The maximum preview size is set by default to a 25-pixel square. Attached images that are larger are made smaller to fit inside this square.

Users can also *embed* images in some content types by clicking the insert image icon in the content editor. Embedded images are displayed in the content itself. An image embedded in content can display as a thumbnail if it's too big, based on the maximum height and width you specify in the Images settings.

By default, you can attach 30 items (of any file type) to any piece of content, with a maximum attachment size of 51200, and you can embed 50 images. The attachment setting is set by the Jive administrator and is not configurable by community administrators. To modify the way embedded images are handled, see Configuring Support for Images and Attachments.

To specify the handling of attachments, including image previews, see Configuring Support for Attachments.

Configuring Support for Embedded Images

Jive users can insert images in documents and blog posts. The Images settings control the behavior of embedded images, as opposed to images that are attached to content as links.

Fastpath: Admin Console: System > Settings > Images

You can use the Images settings to enable and disable image embedding in content, and to specify the maximum number and size of images as well as when and how they should be displayed as thumbnails. Unless otherwise specified, image sizes are specified in pixels. These settings do not affect images that are attached to content as links. For more information about the difference, see Understanding Embedded and Attached Images.

Note: You can use the Attachments settings under **System** > **Settings** > **Images**to determine how previews of attached images are displayed.

Content Type Settings

Content type settings let you specify which kinds of images (as determined by their MIME type) should be allowed as embedded images. You might find that some image file types aren't needed, or are in fact unwanted. If you want to prevent some kinds of images from being uploaded, you can disallow them by adding them to the Disallowed Content Type list.

Configuring Support for Attachments

If you find that users are attaching many large files to their content and the application is slower as a result, you should consider creating limits by adjusting the size and quantity settings. You can also enable and disable image previews, and specify the preview size for attached images. Note that embedded images have their own set of limits than can be configured. See Understanding Images and Attachments for more details about the differences.

See Configuring Support for Embedded Images for information about setting embedded image behavior.

Note: Image preview sizes are specified in pixels and attachment sizes are specified in kilobytes.

Content Type Settings

Content type settings let you specify which kinds of files (as determined by their MIME type) should be allowed as attachments. You might find that some file types aren't needed, or are in fact unwanted. If you want to prevent some kinds of files from being uploaded, you can disallow them by adding them to the Disallowed Content Type list.

Using the Sitemap Feature

The sitemap feature is enabled by default in external Jive communities (typically those used by an organization's customers and vendors), so that web crawlers can more easily find and index a community's pages. From the Admin Console, you can turn off this feature or manually send a sitemap update to specific search engines.

Fastpath: Admin Console: System > **Settings** > **Sitemap XML Settings**

Disabling the Sitemap Feature

To disable the sitemap feature, uncheck **Sitemap auto-submission enabled?**

Manually Submit a Sitemap

To manually submit a sitemap, list the URLs of the search engines you want to send your sitemap to in the **Search engine submission URLs** box and click **Save**. Then click **Send sitemap update**.

External File Storage

Jive can integrate with a number of external storage solutions on a licensing basis. You can integrate it with many more storage providers with minimal development.

By default, Jive uses an external binary storage repository or its own database to store uploaded files. But Jive has the capability to connect to different storage providers, so you can store and organize large files in your storage provider and then socialize them in a Jive group or space. Jive currently provides the following configurations as add-ons:

- SharePoint
- Box.com
- Google Drive
- Dropbox

These connectors provide two-way synchronization between files uploaded to a web part or folder in the storage provider, and a place in Jive where these files are socialized. For more about integration with

SharePoint, see the Jive for SharePoint documentation. For more about Box, see External File Storage in Box.

If you want to connect a different storage provider to Jive, you can write an integration and use two-legged oAuth to connect your storage provider with Jive. For more information, see the main Add-ons documentation and visit the Jive Developers site.

External File Storage in Box

If you want to be able to manage your uploaded files via Box.com instead of Jive, you can set up a place-level connection to synchronize files as well as comments about the files from both sides.

To integrate selected Jive places with Box as the external file storage provider, and to socialize the documents you store in your Box folders, you can connect a Box account to a Jive community. The initial relationship is created when you connect a Box admin account to your community. A Box Integration user with rights to this account is created in Jive. When community users and administrators create places, a folder within the Box account is created and identified with the name of the place. Files added to or modified in that folder from either the Box side or the Jive side are then synchronized. When a Jive user uploads a file to the group, the file is posted to the Box group using the Box Integration user.

This means Jive users don't need Box accounts to access the information in places to which they have rights. They can access and modify any files posted there from the Jive side. However, they won't have access to the contents of the folder from the Box side unless they also have a Box account. Box users who have access to the folder will also need a Jive account if they want to add more documents to the Jive-linked Box folder or modify its contents. Users can comment on documents from either side, and their comments will be visible from both Box and Jive.

Note: If you connect a space to Box, be aware that spaces with the All Registered User permission in Jive will be mapped to All Enterprise Users in Box. Users who have this permission in Box will be able to see the content, even if they don't have rights to access the Jive space.

Setting up the Integration

The complete setup includes these steps:

1. Make sure your Jive installation includes the Extended APIs plugin. For more instructions, see Installing the Extended APIs JAR File.
2. On the Box side, apply the correct settings to your Box enterprise account as described in Configuring Box to Work with Jive.
3. On the Box side, create the Box Integration User. This user is the account you'll use to connect your Jive community to Box. It's also the basis for the Jive system user that will be a member of every Box-linked place in Jive, linking it to the associated Box folder.
4. On the Jive side, connect Jive to Box using the Jive Integration User credentials. Then decide whether users can create new places with a Box-connected folder, as described in Connecting to External File Storage.

Note: If you're using an SSO solution such as Okta with Box, make sure the integration user is defined as an admin. Otherwise, the IdP could remove the integration user's administrative privileges from Box, breaking the integration.

Using More than One External Storage Provider

You can use more than one type of external storage. For example, you can have some of your groups store files in Jive for SharePoint, and some in Box.com. After you've set up the initial community connections to your storage accounts, connections are set up group by group. When you create a group, you decide whether the group will use native Jive storage or another storage. However, you can't connect the same group to more than one storage provider.

Configuring Box to Work with Jive

You'll need to configure your enterprise Box account with the right settings before you set up the Jive connection.

To set up the Box side for the Jive connection:

1. Log in as the Box enterprise administrator.
2. In Box, browse to **Admin Console** > **Enterprise Settings**.
3. Navigate to the Security tab and select **Prevent users from changing their primary email address**.
4. Navigate to the User Settings tab.
5. Under **New User Defaults** > **Restrict external collaboration**, make sure the **Folders owned by managed users can only be collaborated within** check box is cleared.
6. Save your settings.

Setting up the Box Integration User

Before you enable the Box-Jive connection, you'll need to set up a Box integration user on the Box side that can post information to Box on behalf of Jive. This user will be used to create the connection to Jive.

The Box Integration User exists only for the integration, and should never be used for any other actions. It should never be logged in for any reason as either a Box user or a Jive user. In the Box admin console, make sure you have enabled auto-accept for the enterprise. This user needs to be provisioned to handle unlimited storage, or at the highest level possible.

Note: Other Box Enterprise Admins will have access to this user: you should ensure that they don't change the settings.

To set up the Box integration user on the Box side:

1. Log in as the Box enterprise administrator.
2. In Box, browse to **Admin Console** > **Users**.
3. Create a Box user named Box Integration User. Make sure that **Storage allocation (GB)** is set to **Unlimited**. If that isn't possible, set it to the maximum allowed storage allocation.
4. Click **Add User**.
5. Select the newly created Box Integration User.

6. Under **Edit User Access permissions** > **Co-Admin**, make sure the **User is granted administrative privileges** check box is selected.
7. Under **User is granted administrative privileges** , make sure you also select the following check boxes: **Manage users**, **Manage groups**, **Log in to users' accounts**, and **Run new reports and access existing reports**.
8. Save.
9. Log out and log in again as Box Integration User.
10. Browse to **Account Settings**.
11. On the Account tab, make sure that **Account Information - Account type** is set to **Enterprise**.
12. Navigate to the Content and Sharing tab and modify your settings as follows.
    a) Set **Enable external links** to **Nothing, restrict sharing**.
    b) Set **Let link viewers** to **Preview and download the shared item**.
    c) Navigate to **Collaborating on Content** > **Incoming Invitations** and make sure the **Automatically accept incoming collaboration invitations** check box is checked. This ensures that as soon as a user joins the Jive group, the user is also added as a collaborator to the linked Box folder without needing to take further action.

Note: If you're using an SSO solution such as Okta with Box, make sure the integration user is defined as an admin. Otherwise, the IdP could remove the integration user's administrative privileges from Box, breaking the integration.

Connecting to Box External File Storage

You can enable and disable the ability to store uploaded files in Box through the Jive Add-Ons interface.

Fastpath: Add-ons > Storage Providers

Note: There is no way to disconnect Jive from Box after the two have been integrated, so make sure you start with the correct account.

You can use the Add-Ons settings to connect to Box, to set Box as the default storage provider for uploaded files, and to decide which users can set up places to be connected to a Box folder. Each place you connect to Box will store uploaded files in a separate folder inside that account. These files can be updated on either the Jive side or the Box side, and social interactions such as comments on added files will be visible on both sides.

Note: Only uploaded files will be stored in the external storage provider. Images and attachments will continue to use whatever binary storage location you're already using for your community.

To make the initial connection, you'll need an account with Box.com that has enough storage to handle the files Jive users will post in the places you connect to Box. You'll want to provision a dedicated Box account called the Box Integration User specifically for this integration. This account should be an enterprise account with the co-admin role. The instructions for setting up this user and your Box environment can be found here.

Note: The Box Integration User exists only for the integration, and should never be used for any other actions. It should never be logged in for any reason as either a Box user or a Jive user.

To set up the connection on the Jive side, use these settings:

1. Click your avatar in the top right and select **Add-ons**.
2. Connect to a Box account: find Box on the Add-Ons tab, click the gear icon, and select **Settings**. (You should already have Box installed, so you will find it on the Installed tab, but if you don't, click **Available** to show uninstalled add-ons.) Then click **Configure**. You'll be prompted to provide the account credentials for the Jive Integration User. This user needs to be pre-created using the instructions in Setting up the Box Integration User. Provide your credentials and click **Grant access to Box**. Then click **Save** and **Activate**.
3. Go to the Storage Management tab and click **Add Integration**.
4. Select **Jive+Box** as the Provider Type. In the Display Name field, type the name you want community users to see displayed when you are selecting a storage provider for the group. Then click **Add**.
5. If you want all your community users to be able to create groups that use this Box connection for storage, select the **Enabled** check box.
6. If you want only some of your users to be to be able to create places that use this storage instance, clear the **Enabled** check box and start typing the name of a Jive permission group in the Permissions Override field. These groups will be granted permission to create groups linked to this storage instance.
7. User Mapping Options determine how the storage connection will connect Box users with Jive users. You should always use the default setting, which is email address.

External File Storage in Dropbox

If you want to be able to manage your uploaded files via Dropbox instead of Jive, you can set up a place-level connection to synchronize files from both sides.

To integrate selected places with Dropbox as the external file storage provider, and to socialize the documents you store in your Dropbox folders, you can connect a Dropbox account to a Jive community. The initial relationship is created when you connect a Dropbox account to your community. When community users and administrators create places, a folder within the Dropbox account is created and identified with the name of the place. Files added to or modified in that folder from either the Dropbox side or the Jive side are then synchronized.

When a Jive user uploads a file to the group, the file is posted to the Dropbox group using the Dropbox Integration user. This means Jive users don't need Dropbox accounts to access the information in places to which they have rights. They can access and modify any files posted there from the Jive side. However, they won't have access to the contents of the folder from the Dropbox side unless they also have a Dropbox account. Dropbox users who have access to the folder will also need a Jive account if they want to add more documents to the Jive-linked Dropbox folder or modify its contents.

Setting up the Integration

The complete setup includes these steps:

1. On the Dropbox side, create the Dropbox Integration User. This user is the account you'll use to connect your Jive community to Dropbox. It's also the basis for the Jive system user that will be a member of every Dropbox-linked place in Jive, linking it to the associated Dropbox folder. The only requirements for this account are that it be dedicated to the integration, and that it have sufficient storage to handle the files you want to make available in Jive.
2. On the Jive side, connect Jive to Dropbox using the Jive Integration User credentials. Then decide whether users can create new places with a Dropbox-connected folder, as described in Setting Up External Storage in Dropbox on page 89.

Tips, Tricks, and Limitations

- You can't change the name of anyJive group that's connected to Dropbox.
- Likewise, you can't change the filename of a binary file inside a Dropbox-connected Jive group.
- If you need to delete a binary file in the Jive group and replace it with a file with the same name, you'll need to delete it permanently from Dropbox first. Trying to re-add a file with the same name before deleting it from Dropbox will result in errors and a bad state.
- Moving a file from one Dropbox-connected Jive group to another one and then back will fail, as will any action that creates a duplicate filename situation in Dropbox.

Using More than One External Storage Provider

You can use more than one type of external storage. For example, you can have some of your groups store files in Jive for SharePoint, and some in Box.com. After you've set up the initial community connections to your storage accounts, connections are set up group by group. When you create a group, you decide whether the group will use native Jive storage or another storage. However, you can't connect the same group to more than one storage provider.

Setting Up External Storage in Dropbox

You can enable and disable the ability to store uploaded files in Dropbox through the Jive Add-Ons interface

Fastpath: Add-ons > Storage Management

To connect Jive to a Dropbox account:

1. Click your avatar in the top right and select **Add-ons**.
2. Make sure the StreamOnce add-on is installed.
3. On the Storage Management tab, click **Add Integration**.
4. Select **Dropbox** as the Provider Type. In the Display Name field, type the name you want community users to see displayed when you are selecting a storage provider for a group. Then click **Add**.
5. If you want all your community users to be able to create groups that use this Dropbox connection for storage, select the **Enabled** check box.

6. If you want only some of your users to be to be able to create places that use this storage instance, clear the **Enabled** check box and start typing the name of a Jive permission group in the Permissions Override field. These groups will be granted permission to create groups linked to this storage instance.
7. User Mapping Options determine how the storage connection will connect Dropbox users with Jive users. You should always use the default setting, which is email address.
8. Click **Edit Settings** to connect to a Dropbox account.
   a) Click **Save** to save your instance settings.
   b) Click **Save** to continue.
9. Click **Save** to save the integration. You'll now see it listed in the Storage Management tab.
10. If you want to make Dropbox the default storage provider for new places that are created in the community, select it in the Storage Management tab. Clearing the **Allow users to choose Jive as internal storage** check box removes the option to store uploaded documents in Jive for all newly created places.

External Storage in Google Drive

If you want to be able to manage your uploaded files via Google Drive instead of in Jive, you can set up a place-level connection to synchronize files as well as comments about the files from both sides. Note that you need a Google Apps enterprise implementation configured with specific permissions groups to use this integration.

Using More than One External Storage Provider

You can use more than one type of external storage. For example, you can have some of your groups store files in Jive for SharePoint, and some in Box.com. After you've set up the initial community connections to your storage accounts, connections are set up group by group. When you create a group, you decide whether the group will use native Jive storage or another storage. However, you can't connect the same group to more than one storage provider.

Google Drive Permissions Setup

To ensure Jive can share permissions with Google Drive, you need to enable administrative APIs and set up specific permission groups on the Google side.

To apply space permissions correctly, make sure you have the following administrative setup in Google Apps. (Individual Google Drive accounts are not supported.)

1. In the Google Apps Control Panel, enable the Administrative APIs. You can find instructions in the Google documentation here.
2. Add two new groups in Google Apps: AllRegistered and Everyone. These groups are mapped to user permission groups in Jive that have the same names, allowing both sides of the integration to share the same users.
3. Add the Google users who will use the integration to both groups.
   If you use Active Directory to manage and permission groups on both the Jive side and the Google side, permission groups will be mapped and maintained automatically using Active Directory

synchronization. If you don't use Active Directory to manage permission groups, setting up the integration in Jive will create user permission groups on the Google side to match those on the Jive side that are applied to spaces.

Setting Up External Storage in Google Drive

You can enable and disable the ability to store uploaded files in Drive through the Jive Add-Ons interface.

Fastpath: Add-ons > Storage Management

To connect Jive to a Google Drive instance:

1. Click your avatar in the top right and select **Add-ons**.
2. Make sure the StreamOnce add-on is installed.
3. On the Storage Management tab, click **Add Integration**.
4. Select **Google Drive** as the Provider Type. In the Display Name field, type the name you want community users to see displayed when you are selecting a storage provider for a group. Then click **Add**.
5. If you want all your community users to be able to create groups that use this Google Drive connection for storage, select the **Enabled** check box.
6. If you want only some of your users to be to be able to create places that use this storage instance, clear the **Enabled** check box and start typing the name of a Jive permission group in the Permissions Override field. These groups will be granted permission to create groups linked to this storage instance.
7. User Mapping Options determine how the storage connection will connect Google Drive users with Jive users. You should always use the default setting, which is email address.
8. Click **Edit Settings** to connect to a Google account.
   a) If any Google accounts have already been connected to your Jive community, you'll see them listed. Select an existing Google user to authenticate automatically, or click **Authenticate** to insert new user credentials. Note that you can't use an account that is already connected to a different Jive community.
   b) Click **Save** to save your instance settings.
   c) Click **Save** to continue.
9. Click **Save** to save the integration. You'll now see it listed in the Storage Management tab.
10. If you want to make Google Drive the default storage provider for new places that are created in the community, select it in the Storage Management tab. Clearing the **Allow users to choose Jive as internal storage** check box removes the option to store uploaded documents in Jive for all newly created places.

External Storage in SharePoint

To set up external storage in SharePoint, you'll need to configure your SharePoint instance as well as Jive.

Jive for SharePoint requires a Professional Services engagement, so make sure you contact Jive Professional Services before you try to implement it.

Note: Upgrade users should note that as of this version, Jive for SharePoint is implemented as an Add-on, rather than being delivered through the Extended APIs plugin. For more information about Add-ons, see Integrating Jive with Add-on Services.

Configuring Video

Jive supports videos in your community, but you need to whitelist certain IP addresses to provide uploaded videos when your community is behind a firewall. In addition, you can customize the video providers your community uses.

Configuring Video Provider Support

In Jive Hosted and On Premise environments, you can enable and disable certain video providers and add new providers if they are supported. By default, users can embed video content hosted by YouTube, Vimeo, Veoh, and Dailymotion.

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

When users create content and embed videos, they see the supported video provider list as part of the helper text under the embed code field. This list is modified when you enable and disable macros for each video provider in the Admin Console.

For information about enabling your users to embed videos from a non-public video archive via Kaltura and Brightcove, see Adding Kaltura as a Video Provider and Adding Brightcove as a Video Provider. Using these providers provides another layer of permissions around embedded video viewing on top of your Jive space permissions.

To enable and disable video providers:

1. Go to **Spaces** > **Settings** > **Filters and Macros** and navigate to the space for which you want to enable or disable videos. If you want to apply the setting community-wide, select the root space.
2. Scroll down to the Video Macro settings and set the macros you want to change to **On** or **Off**. Note that when you disable a provider macro that has been enabled previously, videos already embedded from that provider will show as disabled.

Setting up Your Firewall for Video

To use the video upload feature when either your community is behind a firewall, or if you restrict end user Internet access, you might want to use IP whitelisting rules to allow network communication between your Jive community and Perceptive servers. To do this, you need to use specific rules.

If your community is behind a firewall and you want to open it up using specific IP whitelisting, you need to use the Perceptive and Jive Ingress and Egress Firewall Rules. If you restrict end user network access by using specific IP or domain whitelisting, you need to use the Perceptive Playback Firewall Rules for End User Network Access

Perceptive and Jive Ingress and Egress Firewall Rules

Jive instance must be allowed access to the following ports, IP addresses, and files:

- Inbound calls to jiveURL/pubcallback.jspa and jiveURL/authcallback.jspa.
- Outbound calls on ports 80 and 443 to the IP addresses listed in List of Perceptive IPs on page 93.

Perceptive Playback Firewall Rules for End User Network Access

For Hosted and On-prem, the allowed ports must be 80, and 443. You must also either whitelist by domain or whitelist by IP address.

Whitelist by domain	Allow access to the following domains: • *.jivesoftware.com • *.twistage.com • *.edgecastcdn.net
Whitelist by IP Address	Allow access to the following IP addresses: • CDN IPs which serve the actual content for the client web browser region, which can be found in the Edgecast CDN table **Note:** These have not changed since Jive 8 • Perceptive IP addresses, which can be found in the List of Perceptive IPs

List of Perceptive IPs

The following list contains Perceptive IP addresses that should be whitelisted so video can work properly in your community.

```
107.21.212.16
107.22.216.172
174.129.240.31
174.29.238.27
184.72.239.40
184.73.232.18
23.21.76.80
23.23.90.48
23.23.94.7
46.137.165.93
50.16.187.111
50.16.210.98
50.19.127.228
52.206.223.205
52.22.44.102
52.22.98.14
52.4.125.148
52.44.119.45
52.45.236.90
52.45.54.219
52.54.180.117
52.6.145.21
```

```
54.195.246.169
54.197.254.218
54.204.24.127
54.217.228.206
54.243.35.52
75.101.144.40
79.125.11.104
79.125.12.197
79.125.20.107
79.125.24.56
79.125.25.81
79.125.6.182
79.125.6.237
```

Adding Brightcove as a Video Provider

You can allow your users to embed videos hosted by Brightcove in their content by specifying the Player ID and Partner ID associated with your Brightcove repository in a custom macro.

If you use Brightcove to host videos and want to make them available for users to post in your community, you'll need to specify the settings for your site using a macro which you can then enable and disable.

1. Upload your videos using the Brightcove Media Management UI and make sure they're available for viewing.
2. In the Brightcove media management UI, across from a video, copy the embed codes for the video
3. Get the {PLAYER_ID} and {PLAYER_KEY} that identify your site.
4. In the Admin Console under **Spaces** > **Settings** > **Filters and Macros**, edit the settings for the CustomVideoMacro: brightcove macro and use these values to populate the playerID and partnerID settings. Make sure you select the space where you want to enable this provider. If you want to apply the setting community-wide, select the root space.
5. Make sure that macro is set to **On**. (Note that when you disable a provider macro that has been enabled previously, videos already embedded from that provider will show as disabled.) When your users embed videos from the Web in content, they'll see Brightcove as a video provider option below the embed code field, and will be able to paste video embed code from Brightcove into the field to successfully post and play videos.

Adding Kaltura as a Video Provider

You can allow your users to embed videos hosted by Kaltura in their content by specifying the Player ID and Partner ID associated with your Kaltura repository in a custom macro.

If you use Kaltura to host videos and want to make them available for users to post in your community, you'll need to specify the settings for your site using a macro which you can then enable and disable.

1. Upload your videos using the Kaltura Media Console and make sure they're available for viewing.
2. Under Embedding Kaltura Media Players in Your Site, find the instructions for "Using Static HTML-based Embed Codes."
3. Following these instructions, get the {PLAYER_ID} and {PARTNER_ID} that identify your site.
4. In the Admin Console under **Spaces** > **Settings** > **Filters and Macros**, edit the settings for the CustomVideoMacro: kaltura macro and use these values to populate the playerID and partnerID

settings. Make sure you select the space where you want to enable this provider. If you want to apply the setting community-wide, select the root space.

5. Make sure that macro is set to **On**. (Note that when you disable a provider macro that has been enabled previously, videos already embedded from that provider will show as disabled.) When your users embed videos from the Web in content, they'll see Kaltura as a video provider option below the embed code field, and will be able to paste video embed code from Kaltura into the field to successfully post and play videos.

Configuring Ratings and Liking

You can configure the way ratings and liking for different types of content work to make them a more or less prominent feature of your community.

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). For example, the community might see *Joey Ramone rated The Rose City Quarterly Document* or *DeeDee Ramone liked Lan Su Garden Blog Post*.

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

Reindexing Browse Data

Browse reindexing is available for troubleshooting indexing problems with browse content.

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

Administrators can control the default behavior of feeds used to stay current on content changes.

Users can choose to receive feeds (RSS, JSON, or Atom). 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 13: 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 user name 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

You can set up profanity filters to automatically replace inappropriate language in your community.

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 the Search Tips in the end user documentation. 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 the Search Tips in the end user documentation. 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 user names 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 click here).
- Gateway Privacy Manager

  This interceptor gives you slightly finer control over how gateway-imported messages are handled. 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 user names 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 the Search Tips in the end user documentation. 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. Make sure you understand how moderation inheritance works. 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 the Search Tips in the end user documentation. 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 the Search Tips in the end user documentation. 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.

Basic Spam Prevention

You can use a variety of best practices to avoid spam in your community. Here are some general spam prevention strategies, as well as those that target specific spammers.

Community administrators of externally-facing communities should develop a strategy for dealing with spam. (Internally-facing 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 community.

In addition to these out-of-the-box features, community managers of externally-facing communities (those that serve customers, vendors, and so on) may want to enable the advanced spam prevention service.

For more information about spam prevention, you might want to check out this document in the Jive Community. Note that you must be a registered user to see this document.

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. (Community must not be using SAML).	Moderating User Registrations

Method	Description	To learn more, see this topic:
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
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
Akismet for Blog Comments	Use Akismet 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
Abuse Reporting	Allows users to report abusive content by clicking an abuse label on the content, which is then sent to a moderator.	Setting Up Abuse Reporting on page 252

Method	Description	To learn more, see this topic:
Content Moderation	Enable content moderation so that users must submit content for approval before it's published in the community.	Moderating Content
Link Moderation	Moderate content that contains external URLs that are not whitelisted. You can also configure link moderation so that all content by users who do not have a certain amount of status points is automatically moderated.	**System** > **Moderation** > **Configure Spam Link Prevention**

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

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.

Item	Description
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.

eDiscovery Search

You can search community content for specific users and export content as XML if it's needed for legal reasons or internal investigations. This is an optional, add-on feature. Contact your Jive representative for more information.

Note: Because it requires access to private and secret content, you need to be a full access admin to use this feature. Community managers of Jive Cloud communities can request special access through Jive Support.

Fastpath: Admin Console: System > Management > eDiscovery Search

If you need to extract content records for specific users during a time period, for example if you need this information for Sarbanes-Oxley compliance, you can use the eDiscovery Search feature to export current records of content a user interacted with during the selected dates. This information includes content the user has created, edited, replied to, or commented on within a specific date range. You can optionally search for interactions containing a key word or phrase. The content, along with any replies and comments associated with the content, is extracted in the form of XML documents, which contain the text component of the interactions, and binary files containing images or attachments. This information is delivered in a ZIP file.

Content returned by eDiscovery Search includes documents, discussions, blog posts, videos, polls, ideas, project tasks, status updates, and direct messages. It does not include any content the user has shared or bookmarked. This tool has access to all data in the instance, and is not restricted by content permissions while searching, so private user data may be exposed in the archive.

By default, search results are available for download for 7 days. You can reset this period by setting the `ediscovery.expirationPeriod` system property to a different number of days.

eDiscovery Search does not have access to any information that has been deleted from the community. It extracts only content, replies, and comments that exist in the community at the time of the search, including private and secret content. In the same way, a document will be extracted in the version existing at the time of the search. If a user deletes a comment or modifies a document while the search is running, and the comment or document has not been retrieved by the search yet, the deleted or changed information will not be extracted. Earlier versions of content are not returned by the search, even if they contain the search term.

To retrieve content through eDiscovery Search:

1. Start typing a user's name or click **Select People** to choose from the list. You can only search one user at a time.
2. In the **Search Criteria** field, type a single word or a phrase to search for. A phrase will be searched as entered. For example, searching `stock options` returns only content references where those words occur together in that order.
3. Select a start date and an end date. The search always begins at midnight on the start date and ends at 11:59:59 on the end date. You can't schedule a search for a day that is later than the current day. You cannot extract more than one year of data at a time. If you need to extract more than a year of data, you will need to run multiple searches spanning one year or less.
4. Wait for your search to complete: this may take a long time depending on how much data you are searching. You can only run one search at a time.

Configuring People-Related Settings

This section includes information about configuring features related to user access (such as password resets), user relationships, 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 invite others to join the community.

You can also configure the application to display a terms and conditions page when new users 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

Select **Allow users to create their own accounts** to enable user-created accounts and to allow all registered users to invite others to join via email (users will see the Send Invites button on the People browse page). When this is selected, people can sign up for a new account from the community login page. The registration process will then take them through a brief set of screens through which they add the information you've selected on the remainder of this page.

New User Account Settings

Use the following table to configure user account settings.

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.
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 correctly to continue with registration. This is a way to discourage registration by other computers simply for access to the community for sending 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 you disable, then users will need to click their name to the upper right corner and then click **Edit profile & privacy** in the Actions list.

Setting	Description
Registration Moderation	If you enable moderation for community registration requests, new requests will appear on the moderator's **Moderation** > **Pending Items** page in the community. (If you have a user administrator, that person will approve or decline requests; otherwise, the system administrator will get those requests.) To learn more, see Moderating User Registrations.
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 Configuring User Profile Templates.

Configuring Your Site's Terms and Conditions

You can write a page that describes your community's terms and conditions.

In the Admin Console, you can indicate what the terms and conditions page should include.

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

If you have SSO enabled, users will be prompted to accept the terms and conditions only when they log into the community for the first time. Without SSO enabled, users are prompted to accept the terms and conditions when they register for access to the community.

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 Settings

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 User Name Reminders

You can configure Jive to send out reminders for users who forget their user names. If a user forgets their user name, you can add an **I forgot my user name** 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 user name, select **Enabled - Users are allowed to request their user names 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 user name and request it. For more on message templates, see Editing Email Notification Templates.

Banning People

The banning feature allows you to prevent users from accessing the community.

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. By 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**

Note: If you use SAML or Kerberos SSO, you can't use the **Disable Login** setting to ban federated users. To ban federated users, you need to remove their access on the IdP. Alternately, you can turn off the **Enable disabled user account on login** setting in your SSO settings before disabling these users.

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 turned 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 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	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.

<table>
<tr><th>Setting</th><th>Description</th></tr>
<tr><td>Image Path and Large Image Path</td><td> 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: <pre>cd <jive.instance.home>
 ln -s /usr/local/jive/var/www/resources resources</pre> 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. You can upload your own 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. </td></tr>
<tr><td>Point Range or Group</td><td> You can associate 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. </td></tr>
</table>

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**. To learn more, see Moderating User-Uploaded Avatars.

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 User Update Settings

You can enable or disable status updates in your community. Status updates allow your end users to post quick status updates about what they're doing.

Internal communities	By default, internally-facing communities (those that typically involve only employees or other internal audiences) have status updates enabled to encourage users to contribute to the community.

External communities	By default, externally-facing communities (those that typically involve customers, vendors, and other external audiences) have status updates disabled.

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

Table 15: Status Update Configuration Options

Setting	Description
Enable User Status Updates	Enabling this will allow users to post status updates that will appear to the whole community.
Enable Reposting of User Status Updates	Enabling this will allow users to repost the status updates of fellow users.
Enable Status Updates in Social Groups and Projects	Enabling this will allow users to post status updates in social groups and projects.
Character Limit	Indicates the character limit of a user's status update message. The default limit is 420. You can adjust this for your users' needs.

Managing SEO in Your Community

You can manage search engine optimization (SEO) to help your Jive-x communities rank even better in web search engines by adding page-level redirects, using keywords in URLs, and describing images in alt tags.

You can take a look at other SEO-focused improvements by checking out the SEO Deep Dive.

Configuring URL Redirects

You can now redirect URLs that would normally result in 404 page-not-found errors.

In both Jive-x and Jive-n, you can mange page-level redirects by navigating to the Redirection Rules page in the admin console. This feature is intended to redirect content URLs only, such as documents, discussions, questions, and so on. Redirects in Jive are easy to use: You can add them as needed (self-service), no need to edit the Apache configuration, and no need to restart your community when adding or removing them.

Note: The limit is 7,500 redirects per community. We also recommend you use a Google Chrome browser because it performs much faster than FireFox when your community is configured with page-level redirects.

Fastpath: Admin console: **System** > **Settings** > **Redirection Rules**

You cannot redirect the following community pages:

- Vanity URLs
- Home and other primary landing pages, such as /welcome, /news
- URLs with parameters
- System URLs, for example, maintenance pages
- Login pages

1. Enter the source URL (from) in the Input URL field. This is the page to be redirected.
2. Enter the destination URL (to) in the Output URL field. This page shows up when you navigate to the page in step 1.
3. Select the type of redirect in the Redirection Type URL field. We recommend you only use the 301 option for Jive-x public communities.
4. Click **Save**.

Best Practices for URL Redirects

You can prepare for understanding and using URL redirects in your community by avoiding both regular expressions and multiple hops.

- Whenever possible, redirects should be one-to-one and not cascade or contain more than one hop. Redirects using multiple hops can impact web search crawlers and even potentially impact your community performance.

  An example a redirect with multiple hops is when URL-A redirects to URL-B which redirects to URL-C which redirects to URL-D.
- URL redirects in Jive do not permit the use of regular expressions (REGEX), including the use of wildcards.

Managing Search

Jive provides configurable search access to content and people, as well as access to external search engines that support OpenSearch.

Fastpath: Admin Console > **System** > **Settings** > **Search**

From this page, you can configure Content or User search.

Configuring Content Search

Content search indexes documents, discussions, blogs, status updates, and external content.

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.

Note: **Admin Console** > **System** > **Settings** > **Search** > **Content Search**

Reindexing Content Search

You can manually reindex content search, but it takes a long time and can slow performance. We don't recommend reindexing manually unless you have a specific search index problem you need to fix.

Fastpath: **Admin Console** > **System** > **Settings** > **Search** > **Content Search** > **Index Tasks**

Having the application regularly update the search indexes is very handy, but rebuilding an index (via the Index Tasks tab) can be very time-consuming. You should only manually rebuild if the search index becomes corrupted or you find you're missing large amounts of content in search results. Please see these detailed instructions when manually rebuilding the search index. The rebuild processing will happen on the web app node you are accessing when you initiate the rebuild. This node sends the data to the external search service you have configured.

- To rebuild the search index in the event of a search problem, click **Rebuild Index**.

  Warning: Before you click this button, consider performance and the needs of your site users. Never reindex content search manually during peak usage hours, for example, or during a sitewide campaign or event that will result in high usage.
- To check the index status of an individual content item or place, type the URL of the content item in the **Content URL** text box and click **Retrieve Modification Date**. If the date is old, you can click **Update in Index** to update only that item in the index.

Selecting a Search Service

A Jive On-Premise installation uses On-Premise Search service by default, and the Hosted installation uses the Cloud Search service by default. But you can change these defaults if necessary.

Hosted Deployment

When you elect to use Jive in a Hosted environment, by default, you use the Jive Cloud Search service with all its benefits. If you want your Hosted instance of Jive to use an On-Premise Search service, you need to contact Jive Support and Jive Hosting by filing a support ticket making this special request.

On-Premise Deployment

Your On-Premise installation of Jive can use an On-Premise Search service once you install Search service on its own node. With an On-Premise installation of Jive, you can switch between Cloud or On-Premise Search services, but when you change the Search service, you must initiate a content index rebuild. For more on this, see the Index tasks in Configuring Content Search.

- To use Cloud Search with an On-Premise implementation of Jive:
  a) File a ticket with Jive requesting access, so that the IP address is whitelisted in your instance. Every IP address connecting to Jive search needs to be granted access.
  b) From **Admin Console: System** > **Settings** > **Search**, go to Search Service Configuration and select **Cloud Search Service**.

c) Select the endpoint that makes sense for your location. To learn more about the data centers and their locations, be sure to read About Cloud Search.

- To use On-Premise Search with an On-Premise implementation of Jive:

a) Install the On-Premise Search Service. For more on this, see Jive Installation Documentation.

b) From **Admin Console: System** > **Settings** > **Search**, go to Search Service Configuration and select **On-Premise Search Service**.

c) Enter the host and port for the service you installed.

Content Search Service Status

You can use the Content Search service status to track the successes and failures of calls to the different services for search.

Fastpath: Admin Console > **System** > **Settings** > **Search** > **Content Search**

Activity Ingress	Jive uses this service to send activity data to the search system. Search uses this service to receive everything that has been indexed. For example, content creation, updates to content, user creation, user updates, place creation, updates to places, likes and comments all get posted to the activity ingress and get indexed. Failures to this service mean that events will queue up on the web app node waiting to be pushed into search.
Query	Jive uses this service to execute search queries. The Query service enables Jive to access the content that has been indexed. For example, Jive uses this service when you use spotlight search on the Search page, when you select content under the "Show more like this" heading, when you use the user picker, and when you use most fields that auto-suggest searches as you type. Failures to this service means searches will fail.
Tenancy and Directory	These services always use the same host and port. If they use localhost, they are referring to the host and port that you configured for On-Premise search. This service is the entry point into search and tells Jive where to go for all the other services, and it assigns a tenant ID to the Jive instance so it can be uniquely identified by all search services. Failures to these services mean search is not working. If you are using On-Premise search, make

sure the Search node is up and running, and that you can telnet from the Web App node to the On-Premise Search node at the configured port. If you are using Cloud search, make sure your firewall is setup properly. If your firewall has been setup properly, then gather your logs and contact Support. For more on ports, see List of Required Ports and Domains.

Configuring Search Synonyms

You can configure the search feature to recognize synonyms for improved search results.

The synonym search feature improves search results by allowing you to create lists of synonyms. For example, you might want a search for "big" to return results for "large", and vice versa. Or, if your users search using terms specific to your industry, you might want to set up a synonym that associates commonly used terms, such as "mobile" and "phone".

You can also set up synonyms for the names of users. For example, you might want to set up "James,Jim,Jimmy" or "Susan, Suzy, Susie".

Synonyms are language-specific. If you have multiple languages enabled, you need to enable them per language.

Note that by default, new synonyms work only on new content. If you want to apply new synonyms to preexisting content, you need to rebuild the Content Search index, which takes significant time and can affect system resources. For more information, see Search Index Rebuilding.

To set up search synonyms:

1. Go to **Admin Console** > **System** > **Settings** > **Search** > **Content/User Search** > **Synonyms**.
2. Type in a comma-separated list of synonyms.
3. Click **Add Synonyms**.
4. Rebuild the content/user search index.

Promoting Content Search Results

You can create rulesets to ensure that particular keywords always return specific content results, even when that keyword does not occur in the content.

Fastpath: Admin Console: System > Settings > Search > Content Search > Promoted Results

Promoting a result ensures that when you type certain keywords, a content item you select will always be at the top of the results. You can associate multiple keywords or key phrases with a single content item by entering the terms separated by commas. You can also associate different content items with the same keyword, so that several content items show up when a user queries that keyword. Use the **Priority** field to detemine which promoted results for a keyword appear first. For example, if you wanted the European, American, and Asian holiday schedules in your organization to be promoted for the keyword “holidays”, you could create a rule for each document linking it to the keyword “holidays.” Then you could rank these schedules 1, 2, and 3 in the results by assigning the rules priorities 0, 1, and 2.

Keep in mind the following limitations when promoting results:

- Keywords must be at least three characters long.
- Single keywords can function as wildcards in spotlight search, but when you specify a key phrase, the query must be an exact match for the key phrase. (Standard searches typed in the search page, or entered by typing in the search field and pressing `Enter` do not support wildcards unless you type `*` as part of the string.) For example, if you specify "quarter" as a keyword, your selected content will be returned for spotlight search queries on "quart" as well as "quarter." But if you specify "quarterly sales," your selected content will not be returned for queries on "quarter," "quarter sales," "quarterly," or "sales," only for queries on "quarterly sales."
- No two rules can have the same priority number, so multiple rules for the same keyword or keyword combination must be in sequential order.

Note: Spotlight search does not need to have all promoted words in order to promote a result.

To create rules and rulesets for promoting results:

1. In the Keyword(s) field, add one or more keywords separated by commas.
2. In the Content Link field, type the full URL of a content item, for example `https://yourcommunity.com/docs/DOC-46692`.
3. Click **Add**.
4. If you want more results to be returned for the same keyword(s), add more rules with the same keyword(s) and different content. Then assign a priority to each rule within the group of rules. You can do this automatically by creating the rules in order of document priority, but you can also edit the Priority field after a rule is created to move it anywhere in the list. Moving a rule to a higher priority will move other rules down in priority, affecting the numbering of all rules below it. Priority applies only within a group multiple rules with the same keyword or keywords. Note that when you change the priority of an existing rule, the rules above and below it will be renumbered to create a sequential list.
   Because the rules will appear in one sequential list, you might end up with a sequence like this one, which represents two rulesets:

   ```
   24. keyword1 document g
   25. keyword1 document a
   26. keyword1 document q
   27. keyword2, keyword3 document x
   28. keyword2, keyword3 document r
   28. keyword2, keyword3 document n
   ```

   The first ruleset says that when keyword 1 appears in a query, the first three results will be documents g, a, and q. The second ruleset says that when either keyword 2 or keyword 3 appears in a query, the first three results will be documents x, r, and n.

Connecting to a Search Service

Use the Search Service Configuration settings to connect to your Search service from your web application nodes. For an on-premise installation, you have the option of either connecting to Jive's Cloud Search service or installing and connecting to an On-Premise Search service.

Fastpath: **Admin Console** > **System** > **Settings** > **Search** > **Content Search**

For more information about selecting a Search service, see Selecting a Search service.

To change the search service your instance is using, modify the settings as follows: -->

Setting	Options	Description
On-Premise Search		
	On-Premise Search Service Host	Enter the host name that Jive can use to connect to the Search service. For On-Premise Search, this is the host name for the node where you installed Search. Default is **`localhost`**. Refer to system requirements for information on Search node size.
	On-Premise Search Service Port	Enter the tcp port that Jive can use to connect to the Search service. Default is **`30000`**.
Cloud Search		
	Search Endpoint	For Cloud Search, select the public cloud search end point in your area. For connection information, see Connecting to Jive-Hosted Services.

Configuring User Search

You can use the Admin Console to adjust user search performance and change the user experience.

Fastpath: **Admin Console** > **System** > **Settings** > **Search** > **User 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.

User Search Status

You can enable searching for user information, or turn user searching off. Click **Update** to save a status setting.

Search Settings

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 user changes	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.
User index update time	How often the index is updated.

Index Tasks

Rebuilding an index manually can be very time-consuming. You should only manually rebuild if you really have to, for example, if you modify the stop word list, add or remove a synonym or the search index becomes corrupted. Initiate a user index rebuild to add new user information to the index without rebuilding the index.

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.

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.

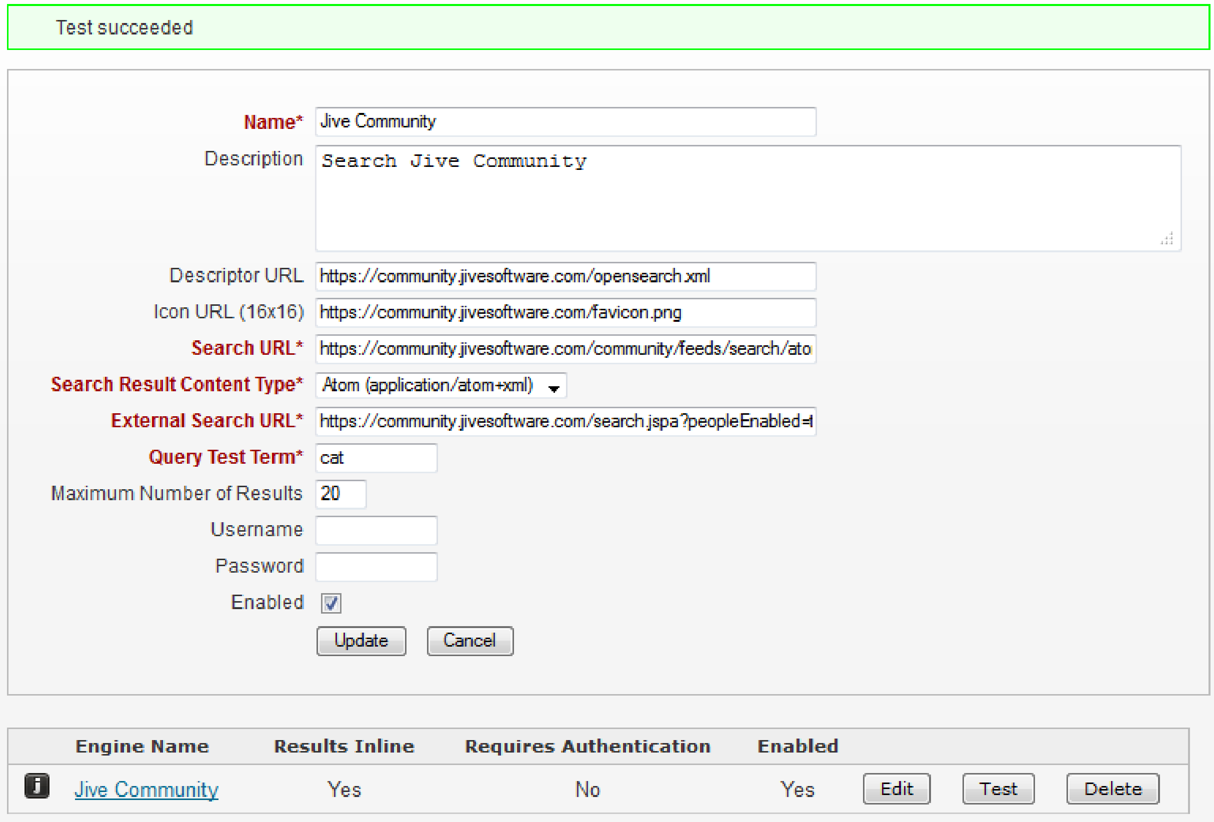
Fastpath: Admin Console: System > Settings > OpenSearch Engines

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 that:

- 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 directly; 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, a sidebar will display a link that people can use to search for their phrase at the OpenSearch location. If they search, their results are displayed 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 user name 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.

Configuring Services Directory for On-Premise Search

The On-Premise Search service relies on a configuration file in `/usr/local/jive/services/search-service/` called `serviceDirectory.json` that provides the host and port the On-Premise Search service needs to bind to for all of the logical services hosted within it.

Because all of the services in On-Premise search are provided by the Search service process, the host and port for every logical service needs to be the same, and needs to point to a non-loopback local network interface. The default host value is `0.0.0.0`, which causes the On-Premise search to scan all local network interfaces and choose the first non-loopback one it finds. On multi-homed machines, On-Premise search may not choose the desired network interface. Therefore, if you are running On-Premise search on a multi-homed machine, you need to explicitly configure which network interface you want to bind to by changing the host values in the `serviceDirectory.json` file.

Important: The On-Premise Search service may be bound to the wrong interface if:

- The service is up and locally accessible.
- The service is not accessible from the web application nodes, but you can ping the On Premise Search host from the web application nodes.

Here is a sample file:

```
{
  "defaultServiceDirectory" : {
    "directory" : {
      "host" : "search.yourOrganization.com",
      "port" : 30000
    },
    "search" : {
      "host" : "search.yourOrganization.com",
      "port" : 30000
    },
    "searchIndexManage" : {
      "host" : "search.yourOrganization.com",
      "port" : 30000
    },
    "rebuildSearchIndex" : {
      "host" : "search.yourOrganization.com",
      "port" : 30000
    },
    "activityIngress" : {
      "host" : "search.yourOrganization.com",
```

```
       "port" : 30000
     }
   },
}
```

Configuring JVM Settings for the Search Process

If you're using On-premise Search, you can configure the heap, ports, logging path, and other settings for the Java virtual machine (JVM) that runs the Search process.

For a list of the settings you can adjust for On-premise Search, refer to the Startup Property Reference.

Note:

- Best practice is to set minimum and maximum heap sizes to the same value.
- The heap size you set for the Search service is independent of the heap size you set for the web application.

Enabling Content Search in Multiple Languages

You can enable documents to be indexed and searched in a language-specific manner.

Note: Content synonyms are language-specific when you enable multiple language search, so make sure you set them per language. For more on synonyms, see Configuring Content Search.

Fastpath: Admin Console > **System** > **Settings** > **Locale** > **Enable multi-language search**

1. Enable multi-language search and enter the allowed search languages.
2. Set the locale for any space whose content should be indexed in a language other than the system default language or its parent space language (**Spaces** > **Settings** > **Space Settings** > **Locale**).
3. Rebuild the search index (**System** > **Settings** > **Search** > **Content Search** > **Index Tasks** > **Rebuild index**). Re-indexing your content enables you to search existing and new content in one of the allowed languages that you selected for the parent space.
4. If multi-language search is enabled and there are more than one allowed languages, the main search page will show an additional language filter so you can select your preferred language when performing searches.

Setting Up Email

You can choose 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 to reply to content or create content as discussions, blog posts, and so on in the application, directly from the email.

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:
Users must have unique email addresses.	Jive Software recommends not setting Jive user names to be the email addresses of users. If you do this, the user's email address string will show up in the user's profile page URL, even if you have set email visibility to Private To User. If you are using SSO for authentication, make sure you have set it to authenticate each user's user name.	Configuring Support for Content Created Via Email (Incoming)
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 process via the Setup Tool.	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:
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
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 you 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 user name** 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 user name 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**. This email address also serves as the reply-to address if the content is sent out from Jive.
Account Username	Email account user name.
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 (native Jive 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
jive.digest.emailSendDay	The day of the week that weekly digest emails are sent.	5 (Thursday) an integer 1-7, Sunday = 1
jive.digest.emailSendHour	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>
```

Adding Unsubscribe Link to Email Footers

By editing the email footer template, you can enable users to unsubscribe to email notifications directly from the email notifications they receive.

The unsubscribe link is added to the email notification footer by default in external communities. It is NOT added to the email notifications footer by default in internal communities.

Fastpath: Admin Console > **System** > **Settings** > **Message Templates**

To enable the unsubscribe link in all email notification footers:

1. Click the edit icon for the Email Footer template.
2. Select **Yes** to enable users to unsubscribe from all email notifications directly from the emails they receive.

   Note: If you select **No**, you will still see code and text that refer to the unsubscribe link, but this will not show up in the output.
3. Click **Save Changes**.

Localizing Email Notification Templates

Set the email templates for additional languages so that users will receive auto-generated emails in their language.

When you create email templates with the locale specified as part of the file name, 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 UI 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 French 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 Digests

By default, email digests are sent at 9:00 a.m. PST on Thursdays. Users can select in their Preferences to receive emails daily, semi-weekly, weekly, or never; the default is weekly. Users receive the digest email at the configured time in their timezone. If a user has not explicitly set a timezone in their Preferences, the application server's timezone is used.

Out of Memory Errors 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 "Email or Stream Notifications?" topic in the end user documentation.

- 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**).

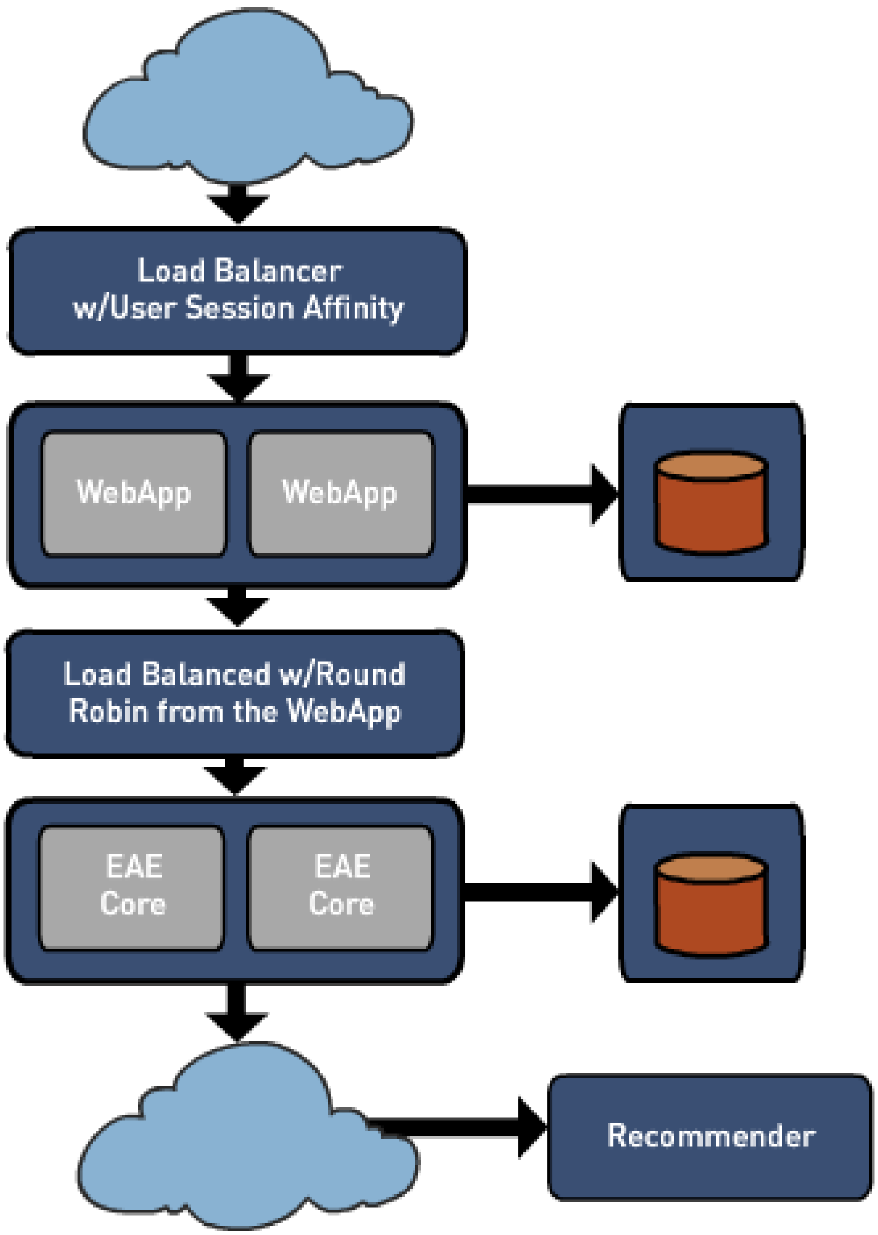
Setting Up the Activity Engine

The Activity Engine powers the activity tracking functionality 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.

What is the Activity Engine?

The Activity Engine powers the stream functionality in Jive. 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 for both on-premise and hosted customers. For on-premise customers, the Activity Engine includes 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, the Activity Engine automatically runs its own upgrade, synthesizing content to deliver to activity 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 activity 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 stream and Inbox.

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 Jive Package and Starting Up. You can then configure the basic settings that control Jive's connection to the Activity Engine's core processes on the **Admin Console: System** > **Settings** > **Activity Engine** page. The table below lists the additional settings that you can adjust on the Activity Engine.

Properties of the Activity Engine

To set any of these properties, as the jive user, run the following: `jive set <property> <newvalue>`

Property	Purpose	Default Value
eae.core.coreAddress	Address of the Activity Engine server.	localhost
eae.core.corePort	Port of the Activity Engine server.	7020
eae.core.coreMinWorkerThreads	Minimum number of threads to listen for incoming socket connections from the Jive web application.	4
eae.core.coreMaxWorkerThreads	Maximum number of threads to listen for incoming socket connections from the Jive web application.	2048
eae.core.user-recency-enabled	Controls whether or not only active users will have their streams populated.	true
eae.core.user-recency-timeout	The age in milliseconds after which a user will be considered inactive.	2592000000 (30 days)

Property	Purpose	Default Value
eae.core.user-recency-buffer	Update user recency time no more than once in this time period in milliseconds.	86400000 (1 day)
eae.core.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-entries-buffer to 24 hours (in milliseconds = 86400000).	7200000
eae.core.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
eae.core.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
eae.core.log-monitor-directory	The path (absolute or relative to service configuration directory) where performance monitoring logs are saved.	var/monitoring
eae.core.log-monitor-period	The frequency in milliseconds that samples are written to the monitoring logs.	60000

Deploying Multiple Activity Engines

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 refreshed.
- 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 en queue 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 en queued on the User Stream 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 Activity Streams

Fastpath: Admin Console: System > Settings > Activity Engine

File Handle Limits Exceeded

If your Activity Engine has exceeded its open file handle limits, you may see output like the following:

```
2013-06-27 04:10:25,894 [pool-7-thread-9] INFO
 [67073a51-1525-4ca9-80d0-382b2ae58899]
 com.jivesoftware.eae.service.dao.impl.StreamConfigurationDAOImpl - Added
 missing stream source connections for user User{userId=43415}
java.io.IOException: Map failed
        at sun.nio.ch.FileChannelImpl.map(FileChannelImpl.java:748)
        at
 com.jivesoftware.eae.stream.kvindex.KeyIndexer.mmap(KeyIndexer.java:238)
        at
 com.jivesoftware.eae.stream.kvindex.KeyIndexer.index(KeyIndexer.java:216)
        at
 com.jivesoftware.eae.stream.kvindex.KeyIndexer.get(KeyIndexer.java:165)
        at com.jivesoftware.eae.stream.kvindex.RevolvingKeyIndexer
$Door.get(RevolvingKeyIndexer.java:228)
        at
 com.jivesoftware.eae.stream.kvindex.RevolvingKeyIndexer.get(RevolvingKeyIndexer.java:14
```

```
        at
 com.jivesoftware.eae.stream.lucene.LuceneFilteredStreamService.handle(LuceneFilteredStr
        at
 com.jivesoftware.eae.service.dao.impl.StreamsServiceDAOImpl.dispatch(StreamsServiceDAOI
        at
 com.jivesoftware.eae.service.impl.ExclusionManager.trackObject(ExclusionManager.java:21
        at
 com.jivesoftware.eae.service.processing.activity.ExclusionHandler.handleActivity(Exclus
        at
 com.jivesoftware.eae.service.processing.activity.ExclusionHandler.handleActivity(Exclus
        at
 com.jivesoftware.eae.service.queue.AbstractPipelineProcessor.handlePipeline(AbstractPip
        at
 com.jivesoftware.eae.service.queue.AbstractPipelineProcessor.process(AbstractPipelinePr
        at
 com.jivesoftware.eae.service.queue.PhasedQueueConsumerRunnable.run(PhasedQueueConsumerR
        at java.lang.Thread.run(Thread.java:662)
Caused by: java.lang.OutOfMemoryError: Map failed
        at sun.nio.ch.FileChannelImpl.map0(Native Method)
        at sun.nio.ch.FileChannelImpl.map(FileChannelImpl.java:745)
        ... 14 more
```

In this case, you'll want to increase the soft and hard file handle limits as follows:

1. Edit /etc/security/limits.conf as follows (note that your file may use the "*" wildcard to specify all users instead of the "jive" user as shown here -- either way, the fix is the same):

```
                jive    soft    nofile      200000
                jive    hard    nofile      200000
```

2. Verify that the new settings have taken effect:

```
$ su jive -c "ulimit -n"
```

3. Edit /etc/sysctl.conf to increase the vm.max_map_count. (For most large implementations 500,000 is a good value, but some installations require a higher value depending on usage patterns or overall usage.) It should look like this:

```
vm.max_map_count = 500000
```

4. Reload:

```
$ sysctl -p
```

5. Verify that the new settings have taken effect:

```
$ sysctl vm.max_map_count
```

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.
- Make sure that the web node(s) and the Activity Engine node(s) are configured to use NTP and share very similar, if not identical, times. If they are out of sync, you may see delays.

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 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. 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
- 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 is dynamic. Its 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, 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.

The number of Likes displayed on a discussion listed in Trending Content is the total number of Likes on that discussion *plus* the total number of Likes of all the replies to the discussion.

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: Jive Software will never request that you share with us your cryptographic keys.

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, 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.

Disabling Jive Genius Recommender Service

The Jive Genius functionality 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 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 Add-ons and Apps

Jive enables you to use add-ons, or extensions, to configure Jive. These add-ons can contain apps, tiles, streams, external storage providers, analytics services, and other extension points to Jive.

When you select **All Add-ons**, you see all available add-ons.

What are Add-ons?

Add-on Services are a secure way of extending the Jive Platform with third-party integrations.

A Jive add-on is an archive file, containing configuration settings and other data, that can be installed into your Jive community.

What's the Difference Between Add-ons and Apps?

Add-ons define the way that Jive Platform extensions are bundled and deployed into the Jive community. An App is a particular type of Jive Platform extension that extends the Jive UI. An add-on can contain any number of apps, tiles, streams, templates, external storage frameworks, analytics services, cartridges, and other extension points. It is up to the developer exactly what is bundled within an add-on: some add-ons only contain configuration information and require the Jive server to communicate with a third-party service; other add-ons are standalone and do not depend on a third-party service. A community administrator can manually upload an add-on package into the community. Additionally, add-ons can be installed for an entire community by a community administrator using the Jive Add-ons Registry. Add-ons can either pull data out of the community or bring data in. If you want to know more about apps, add-ons, and how to develop Jive integrations using the latest APIs, please visit the Jive Developer website at developer.jivesoftware.com.

The following add-on services are available:

External Storage Provider	Leverages options outside of Jive for storing and synchronizing binary files uploaded to a Jive place.
API Services	Brings external data into Jive or shares Jive data with third-party integrations using the Jive API service.
Analytics Services	Generates credentials that allow access to the Jive Data Export API. Provide these credentials to consumers of your analytics data so they can

	access the export service. These credentials may be revoked at any time.
Other Add-ons (Client Apps Only)	Some client apps can only be found in the All add-ons tab. These "Other" add-ons aren't storage providers and don't include tiles or templates.
Build Your Own Add-ons	Brings external systems into Jive by building extensions for them. For instance, you can connect Jive to your bug tracking system or your version control system so that when a user views a Jive Place, they get a view of that other system. Not only can a user view information from that other system, but you can provide actions to the user without them ever having to leave Jive.

Manage Access to the Add-ons Registry and Apps Market

Use the Cloud Settings page in the Admin Console to enable or disable the connection to the Add-ons Registry or the Apps Market.

Note: This functionality is only available to upgrading customers.

The Add-ons Registry allows your Community Manager to install add-ons (which include apps) for the entire community; the Apps Market allows users to install apps from Jive's apps marketplace.

1. In the Admin Console, go to **Add-ons** > **Cloud Settings**.
2. Click **Enabled** or **Disabled** beside the Apps Market section or the Add-ons Registry section to change access.

   Note: The Add-ons Registry includes packages that are provided by third-party developers. Jive Software makes no warranty or guarantee about the reliability, performance, quality, or functionality of any third-party software, and any third-party packages you install are therefore provided as is. Use of third-party software is subject to their license and/or support terms.

Managing the Apps Market

Although installing apps through add-ons (either by using the Add-ons Registry or by uploading the package manually) is the recommended way to deploy apps, you can still use the Apps Market, if it is enabled.

We now encourage that you use the add-on deployment mechanism for new Jive App development work. With add-ons, you can easily deploy fully-featured apps (along with tiles, streams, and many other extension types) into your community. For more information about add-ons, refer to What are Add-ons? on page 147. However, if you still need access to the Apps Market, it is possible to enable it.

For information on enabling the Apps Market, refer to Manage Access to the Add-ons Registry and Apps Market on page 148.

For additional documentation on the Apps Market, refer to Apps Market information found in the Jive 7.0 Community Administrator Help.

Install Add-ons

Find and install add-on services available for your community.

By browsing what's available, you can find add-ons that you haven't installed. Here's where you access all add-ons available in Jive's Add-ons Registry.

Note: The Add-ons Registry includes packages that are provided by third-party developers. Jive Software makes no warranty or guarantee about the reliability, performance, quality, or functionality of any third-party software, and any third-party packages you install are therefore provided as is. Use of third-party software is subject to their license and/or support terms.

1. Click your avatar in the top right and select **Add-ons**.
2. From the Add-ons tab, select **All Add-ons** > **Available**.
3. Find the add-on you want and click **Install**.
4. Select **Install**. Decide whether you want to preview this add-on or immediately install it in your community:

Option	Description
Select This service is visible only to me	Selecting this will make the feature available to you only. Make this selection if you would like to test this feature before making it available to your community.
Unselect This service is visible only to me	Unselecting this will make the feature available to your entire community.

Note: If you choose to select **This service is visible only to me**, create a secret group and test the add-on before making it available to everyone.

5. Click **Install**.
6. Some add-ons using API Services or Storage Providers require further configuration after being installed. If the add-on you just installed needs further configuration, the Settings page opens. Click **Configure Now** to do that. (You can access the Settings page from the add-on listing later if you don't want to configure it now.)
7. Change the settings for the add-on.
8. Click **Save and Activate** when you're done.

Configure and Activate Add-ons

After you install an add-on that contains a configuration file, you'll be sent to the Settings page. If you cancel out of this page, you'll continue to see a Settings button and, if available, an Uninstall button until you complete the configuration. (You may not have to manually change a configuration file.)

1. From the Add-ons tab, select **All Add-ons** > **Installed**.
2. To configure the new add-on, click the **Settings** button.
3. Click **Configure Now...**.
4. Change the add-ons settings and click **Save**.
5. Click **Save and Activate** when you're done.

Enable Add-ons for External Contributors

If you want external contributors to your community to be able to use an add-on, you can enable access.

The setting to enable external contributor access is only visible if your community has enabled externally accessible groups under **System** > **Settings** > **Externally Accessible Groups**. All external contributors in your community will be able to access an add-on you enable: you can't restrict access to members of specific groups.

Apps that are bundled in add-ons will be displayed in the App Launcher when external contributors click the Apps tab.

To enable an add-on for external contributors:

1. Click your avatar in the top right and select **Add-ons**.
2. From the Add-ons tab, select **All Add-ons** > **Installed**.
3. Click the gear icon next to the add-on you want to grant access to.
4. Select **Enable for External Contributors**. You'll see the Externally Accessible label in the list of Add-ons. To disable again, just change the setting back to **Disable for External Contributors**.

Manage App Visibility Using Security Groups

Limit the visibility of an app using security groups from the Add-ons tab.

You can specify one or more security groups whose users can see a particular app. This functionality is only available for apps you have installed.

To change the visibility of an app:

1. Click your avatar in the top right and select **Add-ons**.
2. From the Add-ons tab, select **All Add-ons** > **Installed**.
3. Click the gear icon next to the add-on containing the desired app and select **Settings**.
4. Click the gear icon in the **App Security** column of the row containing the app you want to manage. The **Manage App Security Groups** dialog appears.
5. If you don't have security groups already specified for this purpose, click the **Admin Console** link in the dialog box and create those groups. After creating security groups, return to **App Security** for this app.
6. Type the first few letters of the name of the security group whose users should see this app. When the correct security group appears in the dropdown list, select it.
7. Repeat the previous step until all security groups are specified.
8. Click **Save Changes**.

Once security groups are associated with an app, only users within those security groups can see the app. The app will not appear to other users.

Uninstall Add-ons

Most add-ons can be uninstalled if you decide you no longer want them.

Some add-ons are provided as part of Jive, and you cannot uninstall them. You can always uninstall non-Jive add-ons that you don't want. If Jive Software determines an add-on is malicious, we may decide to ban it, and we will remove it from your environment as soon as possible.

Note: If you uninstall an add-on from the Add-ons registry because it is malicious, or simply because it is not working as expected, please inform Jive Support promptly so we can investigate.

To uninstall an add-on:

1. Click your avatar in the top right and select **Add-ons**.
2. Select **All Add-ons** > **Installed**.
3. Click the gear icon next to the add-on you want to uninstall and select **Uninstall**.
4. Select **Uninstall**.

Managing Storage Providers

The External Storage Framework allows you to create connections to any file storage provider, so users can bidirectionally synchronize updates to a place in Jive and a location on the storage provider.

You can read more about the external storage add-ons already available in Jive here: External File Storage. If you want to integrate your chosen file storage solution with Jive, it's easy to use the External Storage Framework and Jive's APIs to develop a connection to a provider, add it as a Storage Provider, and enable it in your community. External Storage integrations let you:

- Use your storage provider of choice as the back-end binary storage for documents and attachments uploaded into some or all the places in your community
- Connect Jive Places to folders, sites, or other storage locations on your storage provider
- Synchronize permissions members between Jive and your storage provider
- Synchronize file versions and updates between Jive and your storage provider
- Synchronize comments on files between Jive and the storage provider (if comments are available in your storage provider)
- Limit the integration's availability to specific users and permission groups
- Decide whether the external storage provider should be the default location for storing files within a Jive Place

Information about what you need to create a storage provider is available at developers.jivesoftware.com and in the Jive Community Developers space. For more information about creating and uploading an add-on using the Registry Console, see Building Your Own Add-Ons.

Managing API Add-ons

API Add-ons bring external data into Jive or share Jive data with third-party integrations using Jive APIs. These add-ons expose tiles, templates, apps, and other Jive extensions.

If an add-on includes a storage provider, it will show up in the Storage Provider tab. Once installed, you can manage settings for API Add-ons using the gear icon. For more on the Jive Add-ons Registry, see Enable Access to the Add-ons Registry.

Reconnecting to Add-on Services

If you reconnect to an add-on service after changing a configuration or becoming disconnected, you'll have to reauthenticate.

Re-establish the add-on's connection to its service, which initiates an authentication process, even if it had previously been authenticated. Reconnecting to an add-on service requires that you re-authenticate all tiles used by this add-on.

To reconnect an add-on to its service:

1. From the Add-ons tab, select **All Add-ons** > **Installed**.
2. Click the gear icon next to the add-on that you want to reconnect to its service.
3. Select **Reconnect to Service**.
4. When the dialog opens, click **Reconnect now** if you're okay with the add-on re-establishing its connection to and re-registering with the third-party service. You will need to reconfigure any tiles receiving updates so they continue receiving them.

Checking for Add-on Updates

Check your add-on to see if there are updates that you can download from the add-on registry.

Updates happen automatically, but if you have suspended automatic updates you can use this procedure to check and download and update.

To check for an update to an add-on:

1. Click your avatar in the top right, and select **Add-ons**.
2. From the Add-ons tab, select **All Add-ons** > **Installed**.
3. Click the gear icon next to the add-on that you want to check for updates.
4. Select **Check for Updates**.
5. If the add-on has updates available, click **Update**; otherwise, you'll see the "This add-on is up-to-date" message and you can click **Close**.

Viewing Active Add-on Tiles in My Community

You can use the Add-Ons interface to see which tiles from an add-on are being used in your community and manage access to them place by place.

Not only can you look at which tiles are active in your community, you can also use the Community Authorization option to see which Jive places contain those tiles. You can always use this page to revoke the service's access to a tile.

To see active tiles:

1. Click your avatar in the top right, and select **Add-ons**.
2. From the Add-ons tab, select **All Add-ons** > **Installed**.
3. Next to the add-on you're interested in, click the **gear icon** > **Community Authorization**.
4. To revoke a service's access to tiles in a place, click the **Revoke Access** button. This revokes access to all tiles in one place. If you want to cut a service off from your community, you need to perform this step for every place that has tiles that connect to the same service.

Managing Analytics Add-ons

Analytics Add-ons generate credentials that allow access to the Jive Data Export API. Provide these credentials to consumers of your analytics data so they can access the export service. These credentials may be revoked at any time.

Generating Client IDs and Secrets

Creating a client ID and secret lets you access the Data Export API to use community data in a safe and secure way.

To add a new client ID and secret:

1. Click your avatar in the top right, and select **Add-ons**.
2. From the Add-ons tab, select **Analytics Services** > **New Client**.
3. Enter the Client name. Make sure you use a descriptive name that will help you remember the system it's being used for.
4. Click **Generate Client ID & Secret**.

Retrieving a Client ID and Secret

You can retrieve the client ID and secret for your add-on if you lose track of it. Keep in mind that access to the ID and secret can compromise your add-on’s security.

To find an add-ons client ID and secret:

1. Click your avatar in the top right, and select **Add-ons**.
2. From the Add-ons tab, select **All Add-ons** > **Installed**.
3. Click the gear icon next to the add-on that you're interested in.
4. Select **View Client ID and Secret**.
5. When the Client ID and Secret dialog opens, copy and paste the information to where you can find it when you need it.
6. Click **Done**.

Revoking Access to a Service

You can remove the Jive credentials that if you need to prevent tools from accessing the Data Export API.

You can use the revoke access/uninstall feature as a way to control access of your community data. You can always create a new client if you mistakenly revoke an access.

1. Click your avatar in the top right, and select **Add-ons**.
2. From the Add-ons tab, select **All Add-ons** > **Installed**.
3. Click the gear icon next to the add-on that you're interested in.
4. Select **Uninstall**.
5. When the Confirm Uninstall dialog opens, click **Uninstall**.

Managing Other Add-Ons

Some add-ons don't fit into any other category, but still show up in the All Add-ons category. These "other" add-ons include add-ons you built yourself as well as any client apps from the Jive Add-ons Registry that don't contain any tiles or templates.

Registry Add-ons that do contain tiles or templates show up in the API Services category.

You can find Other add-ons by clicking your avatar in the top right, and selecting **Add-ons** and then select **Add-ons** > **All Add-ons** > **Available**.

Reconnecting to Add-on Services

If you reconnect to an add-on service after changing a configuration or becoming disconnected, you'll have to reauthenticate.

Re-establish the add-on's connection to its service, which initiates an authentication process, even if it had previously been authenticated. Reconnecting to an add-on service requires that you re-authenticate all tiles used by this add-on.

To reconnect an add-on to its service:

1. From the Add-ons tab, select **All Add-ons** > **Installed**.
2. Click the gear icon next to the add-on that you want to reconnect to its service.
3. Select **Reconnect to Service**.
4. When the dialog opens, click **Reconnect now** if you're okay with the add-on re-establishing its connection to and re-registering with the third-party service. You will need to reconfigure any tiles receiving updates so they continue receiving them.

Checking for Add-on Updates

Check your add-on to see if there are updates that you can download from the add-on registry.

Updates happen automatically, but if you have suspended automatic updates you can use this procedure to check and download and update.

To check for an update to an add-on:

1. Click your avatar in the top right, and select **Add-ons**.
2. From the Add-ons tab, select **All Add-ons** > **Installed**.
3. Click the gear icon next to the add-on that you want to check for updates.
4. Select **Check for Updates**.

5. If the add-on has updates available, click **Update**; otherwise, you'll see the "This add-on is up-to-date" message and you can click **Close**.

Building Your Own Add-ons

You can build your own add-ons to leverage services and share information between Jive and external or internal systems.

Building the Add-on

Get started building add-ons by consulting the Add-ons developer documentation in the Jive Developer Community.

If you have an internal or external system that you want to use to share information with Jive, then you might consider building your own add-on. Get started building add-ons by consulting the Add-ons developer documentation in the Jive Developer Community.

Use the following guidelines to get you started:

- Read the Jive Platform Developer Introduction.
- Join the Jive Developer Community.
- Create your add-on!
- Bundle your add-on package either using the Jive SDK or manually.
- Upload the add-on to your community and make it visible only to yourself to test it out.
- Let the community use your add-on.
- Publish your add-on to the Add-ons Registry.
- Whenever you make new updates to your add-on, publish them to the Add-ons Registry.

Uploading Your Own Add-ons

You can build your own add-ons to leverage systems in Jive. Once you build the add-on, upload it to Jive using the Add-ons page.

When you first upload an add-on to your community, we recommend that you first restrict the add-on’s visibility to yourself and test out your tiles by creating a secret group for them. This strategy reduces the impact on your community and gives you a chance to your add-on without setting up an entire separate test environment.

To upload an add-on:

1. Click your avatar in the top right, and select **Add-ons**.
2. From the Add-ons tab, select **All Services** > **Upload Package**.
3. Click **Browse** to find the .jive ZIP package.
4. If you're not ready to publish this add-on to your community, select **This service is visible only to me**.
5. To test your add-on, create a secret group and experiment with your add-on functionality before making it available to everyone.

Letting the Community Use Your Add-on

Once you're happy with the add-on you've produced and tested, you're ready to turn it on in your community.

If you uploaded your add-on using the "This service is visible only to me" option, then you need to actually publish it to your community when it's ready. This allows others in your community to use the tiles and/or templates provided by your add-on.

To push your add-on into the community:

1. Click your avatar in the top right, and select **Add-ons**.
2. From the Add-ons tab, select **All Add-ons** > **Installed**.
3. Click the gear icon next to the add-on that you're interested in.
4. Select **Visible to entire community**.
5. When the Permit All Users Access to this Add-on dialog opens, click **Uninstall**.

Publishing to the Add-ons Registry

If you want to publish your add-on in the Jive Add-ons Registry, you need to be part of the Technology Partner group.

Once you're a registered Jive Developer, you can use the following steps to publish your add-on to the Add-ons Registry. After publishing your add-on, Jive will review it. After passing the review, all Jive communities will be able to install the add-on.

1. Click your avatar in the top right, and select **Add-ons**.
2. From the Add-ons tab, select **All Add-ons** > **Installed**.
3. Click the gear icon next to the add-on that you want to add to the Add-ons registry.
4. Select **Publish to Add-ons Registry**.
5. If you have a Jive Developer account, enter your username and password, and click **Submit**. If you’re not, click Create an account to apply to become one.

   Note: After you sign up to become a Jive developer, you receive a UUID, client ID and client secret. Please record these values as you'll need them to publish updates to your add-on.

Pushing Updates to Add-ons Registry

If you add improvements to your add-on after you publish it, you may want to publish the updates to the Add-ons registry so other communities can enjoy these changes.

To update your add-on in the Add-ons Registry:

1. Click your avatar in the top right, and select **Add-ons**.
2. From the Add-ons tab, select **All Add-ons** > **Installed**.
3. Click the gear icon next to the add-on that you want to update in the Add-ons registry.
4. Select **Push Update to Add-ons Registry**.

5. If you have a Jive Developer account, enter your username and password, and click **Submit**. Create an account if you want to apply to become one.

Retrieving a Client ID and Secret

You can retrieve the client ID and secret for your add-on if you lose track of it. Keep in mind that access to the ID and secret can compromise your add-on's security.

To find an add-ons client ID and secret:

1. Click your avatar in the top right, and select **Add-ons**.
2. From the Add-ons tab, select **All Add-ons** > **Installed**.
3. Click the gear icon next to the add-on that you're interested in.
4. Select **View Client ID and Secret**.
5. When the Client ID and Secret dialog opens, copy and paste the information to where you can find it when you need it.
6. Click **Done**.

Viewing Active Add-on Tiles in My Community

You can use the Add-Ons interface to see which tiles from an add-on are being used in your community and manage access to them place by place.

Not only can you look at which tiles are active in your community, you can also use the Community Authorization option to see which Jive places contain those tiles. You can always use this page to revoke the service's access to a tile.

To see active tiles:

1. Click your avatar in the top right, and select **Add-ons**.
2. From the Add-ons tab, select **All Add-ons** > **Installed**.
3. Next to the add-on you're interested in, click the **gear icon** > **Community Authorization**.
4. To revoke a service's access to tiles in a place, click the **Revoke Access** button. This revokes access to all tiles in one place. If you want to cut a service off from your community, you need to perform this step for every place that has tiles that connect to the same service.

Using Service Diagnostics

Some add-on services use diagnostics, or a health check, that show the network status and provide other system messages.

Use the Service diagnostics to check on the network connection status of an add-on, as well as any messaging from the resources connected to that add-on. Not all add-ons include service diagnostics, so don't be surprised if there's no link.

To check the health of your add-on:

1. Click your avatar in the top right, and select **Add-ons**.
2. From the Add-ons tab, select **All Add-ons** > **Installed**.

3. Click the gear icon next to the add-on that you want to check for updates.
4. Select **Run Service Diagnostics**, if available. Some add-ons do not include diagnostics.
5. Check the diagnostics to see if there are any communication issues with the add-on.
6. Click **Close** at the bottom of the dialog.

Understanding Add-ons Alerts

Add-on alerts are typically triggered when Jive is having trouble communicating with the third-party add-on service. Some possible reasons include the following.

Fastpath: End User Interface: Your Avatar > Add-ons > All Add-ons

Some possible reasons include:

Registry failure	This alert can occur immediately after you first register Jive with the third-party service, if the external service is down or the certificate is failing. It could also occur if you recently changed your jiveURL. Try clicking the gear icon to re-register the service. If that doesn't resolve the alert, make sure the certificate and the jiveURL are correct.
Configuration failure	This alert can occur if your configuration information is incorrect. If you recently created or edited your configuration settings, verify that they are correct. This alert could also be caused by a network-level communication problem.
Service call failure	This alert can occur when Jive cannot reach the third-party service because the network is down, or because of some other communication issue. Jive will try to sync with the third-party service for seven days: after that, it will stop trying and surface this alert. To resolve it, try fixing the underlying issue (typically a communication or configuration issue) and re-enable synchronization with the service.

Troubleshooting Add-ons

You can diagnose and fix common problems with add-ons by looking at our troubleshooting tips.

Why Can't I Uninstall this Add-on?

Certain Add-ons cannot be uninstalled because they're distributed as part of Jive. These add-ons don't have the Uninstall option when you click the gear icon.

There are no add-ons in All Add-ons > Available

The Add-ons registry may have been disabled, so check the Jive property **jive.appsmarket.registry.enabled**. The Add-ons registry is disabled by default on hosted and on-premise instances, so you may need to set this system property to "true". If you don't have access to Admin Console: **System** > **Management** > **System Properties**.

I can no longer configure tiles and they are not updating

The integration service may be down or unreachable. If it seems that everything is up and running you may need to reconnect. From the gear menu, select "Reconnect to Service" to generate a "register" call, similar to that which was performed when the add-on was first installed.

My add-on is gone! Can I get it back?

There are only two ways add-ons are uninstalled when it's not done by your own Community Admin. First, if we need to ban the add-on in the Add-ons registry. An add-on might be banned because it violates Jive policies, or because it references a cloud service that is no longer available. Second, add-ons delivered by a plugin may be discontinued. This may be due to licensing or Jive edition changes, or because the plugin was uninstalled.

When trying to configure a tile, the dialog hangs with a "Loading..." message

The lightweight User Interface provided by add-ons for configuring tiles is almost always served on the integration server. Ensure this server is up and running, can be reached by Jive, and has an SSL certificate that Jive will accept. If the related add-on provides a health check URL, you can "Run Service Diagnostics" from the add-on management page.

Enabling Unified Communications

If you want your users to be able to connect to Jabber, WebEx, or Google Hangouts right inside the Jive interface by clicking through from hover cards or other locations where they want to invite collaboration, you can set up connectors for these applications in your community using the Add-Ons and Apps functionality.

Jive Connector for WebEx	Lets your users easily create online meetings with groups of people in the community, as well as people outside of it.
Jive Connectors for Jabber and Lync	Lets your users communicate with people in the community using voice or chat via the Jabber or Lync client. Contact points are associated with hover cards.
Jive Connector for Hangouts	This add-on allows access to phone calls and video chats directly from your Jive community using Google Hangouts.

Jive Identity Connector	This add-on syncs user profile information between your Jive-n instance and its associated Jive-w mobile apps (Jive Circle and/or Jive Chime).

Requirements for Cisco Connectors

To enable connections to WebEx and Jabber through the Cisco Connectors for these programs, you'll need a Cisco PBX and a recent version of Jive.

Jive System (All Connectors)

- Jive 7.0.2 or higher, or Jive Cloud
- Community Manager rights to your Jive site

Jive Connector for Jabber

- Cisco Unified Communications Manager version 8.6 or higher for Voice/Video
- Cisco Unified Presence Services version 8.6 or higher (or WebEx Connect Messenger Service) for Instant Messaging (IM)
- Cisco Jabber Desktop client version 8.6 or higher (Mac or Windows), configured to handle xmpp: and tel: URIs from the user's web browser

Jive Connector for WebEx

- Cisco WebEx, version WBS29 or higher, with an active corporate account
- Cisco WebEx Meeting Center, for meeting participation

Requirements for Lync/Skype for Business

To enable connections to Microsoft Lync/Skype for Business you'll need recent versions of Jive and Microsoft Lync/Skype for Business.

Jive System

- Jive 7.0.3.1 or higher, or Jive Cloud. JiveX communities are not supported.
- Community Manager rights to your Jive site

Lync

Lync 2013, Lync 2010, Lync client for Lync Online, or Skype for Business.

Requirements for Hangouts

To enable the Jive Connector for Hangouts, you'll need a recent version of Jive and the Google Hangouts browser plugin.

Jive System

- Jive 7.0.3.1 or higher, or Jive Cloud.

Note: Jive-x communities are not supported.

- Community Manager rights to your Jive community.
- Your community users will need an email address and/or phone number in their profile. You can configure your community to populate phone and email fields from a directory server or your users can enter that information themselves by clicking their avatar, selecting **Edit Profile** > **Your Profile**, and entering their phone number and email.

Google Hangouts

- Your community users will need a Google account.
- Your community users will need to either use Google Chrome as their browser or, if they use Firefox, Safari, or Internet Explorer, to install the current version of the Google Hangouts browser plugin.

  Note: Users who aren't already using the Hangouts will be prompted to install the plugin when they first access Hangouts.

Enabling the WebEx Connector

To set up an integration between WebEx and your Jive site, you'll need to install the Jive Connector for WebEx add-on from the Available tab in the Add-ons interface.

The WebEx integration allows one-click access to online meeting technology without leaving your Jive community. To set up the integration, you'll need community manager rights in your community. This enables you to install the add-on and configure the global settings for the app. To get set up:

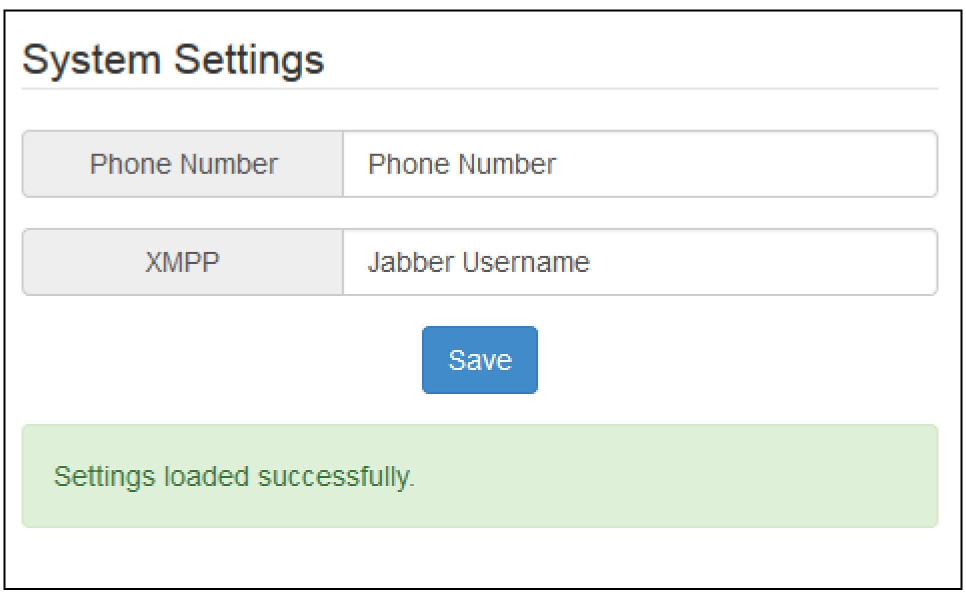
1. Make sure your community meets the requirements.
2. In Jive, click the menu under your name or avatar and select **Add-ons**.
3. Make sure the **Available** tab is selected.
4. Click the gear icon next to Jive Connector for WebEx and click **Install**.
   The add-on will be installed.
5. Click **Apps** in the header of your Jive site. You should see the Jive WebEx app listed in the launcher screen.
6. Click the Jive WebEx app and select the Global Preferences tab. (This tab won't be displayed unless you have Community Manager rights.)
7. Provide the WebEx server URL you want users to have pre-populated when they use the integration. The standard format for this URL is `https://yourcompany.webex.com`.
8. Save the Global Preferences.

Enabling the Jabber Connector

To set up an integration between Jabber and your Jive site, you'll need to install the Jive Connector for Jabber add-on from the Available tab in the Add-ons interface.

This Jabber integration allows one-click access to voice talk and chat using Jabber as the client. To set up the integration, you'll need community manager rights in your community. This enables you to install the add-on and configure the profile fields associated with the app. If your community uses SAML SSO or a directory server for user provisioning, you may also need access to your directory server or IdP to ensure a custom profile field in Jive can be populated. To get set up:

1. Make sure your community meets the requirements.
2. In your community's profile settings, define a custom field that will define the xmpp ID for Jabber: this should be the same as the user's email address. This field should be populated by your directory server or IdP using the correct attribute, typically `mail`. (Even though you probably already populate the email field, you still need to define the custom field.) We recommend naming the field "Jabber Username" for easy identification. You can create the custom field by accessing **People** > **Settings** > **Profile Settings**. Then click **Create new field** and add a text field for the Jabber username. Set the default visibility of the field to **Everyone**, and enable all attributes except **Editable**. Your directory server admin can modify your directory server or your SAML SSO settings to ensure the field is populated for users.
3. In Jive, click the menu under your name or avatar and select **Add-ons**.
4. Make sure the **Available** tab is selected.
5. Click the gear icon next to Jive Connector for Jabber and click **Install**.
   The add-on will be installed.
6. Click the Jive Jabber app and in the System Settings dialog, provide the field names in the Jive contact database that the integration will use to find the phone number and xmpp ID for each user.

   The xmpp ID should be located in the Jabber Username field you created in Step 2, and the phone field is typically named Phone Number. You can confirm this information by opening the Jive admin console and clicking **People** > **Settings** > **Profile Settings**. Enter the field names into the app configuration screen exactly as they appear in the Profile Settings dialog. (Note that a translation of the field name may be displayed in the profile, but the profile settings will show the actual field name.) Users who don't have this information populated in the fields you identified will not be able to connect using the Jive

Jabber integration, and users who are using Jabber in Jive will not see the buttons they need to connect to these users, either on their profiles or on the hover card. If your community is not already populating these fields from a directory server, and you have made these fields editable on the profile, you can get users to provide the information themselves by clicking **Edit Profile** under their name or avatar.

Enabling the Lync/Skype for Business Connector

To set up an integration between Lync and your Jive site, you'll need to install the Jive Connector for Lync add-on from the Available tab in the Add-ons interface.

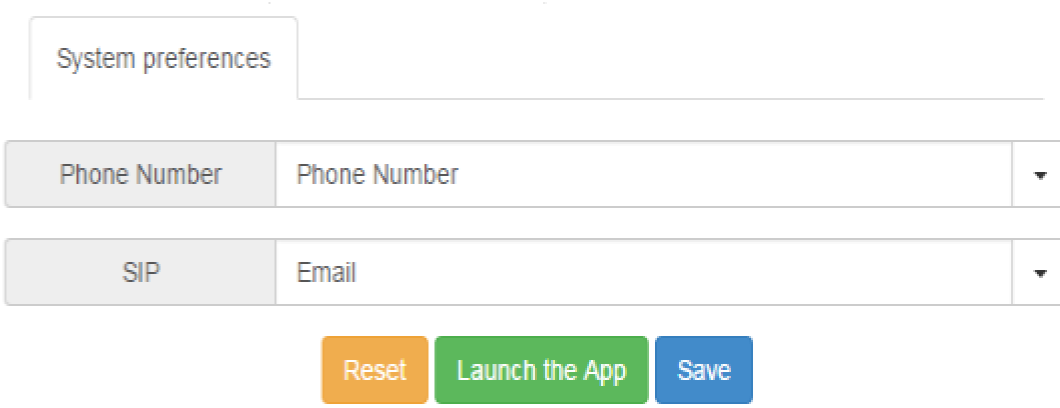
This Lync integration allows one-click access to voice talk and chat using Lync as the client. To set up the integration, you'll need community manager rights in your community. This enables you to install the add-on and configure the profile fields associated with the app. If your community uses SAML SSO or a directory server for user provisioning, you may also need access to your directory server or IdP to ensure the correct profile fields in Jive are populated.

The following reference table shows which buttons and contact methods each profile field enables. If you need to, you can remap these methods to a different profile field using the app configuration described in Step 6.

Button	Contact Method	Default Profile Field
	Lync calling	Email address
	Lync chat	Email address
	Phone system calling	Phone Number

To get set up:

1. Make sure your community meets the requirements.
2. In your community's profile settings, make sure you define the user's email address. This field is typically populated by your directory server or IdP using the `mail` attribute.
3. In Jive, click the menu under your name or avatar and select **Add-ons**.
4. Make sure the **Available** tab is selected.
5. Click the gear icon next to Jive Connector for Lync and click **Install**.
   The add-on will be installed.
6. Click the Jive Lync app in your Apps menu, and in the System Preferences tab, provide the field names in the Jive profile that the integration will use to find the phone number and/or email address for each user. The image below shows the default values.



The phone field is typically named Phone Number, although you can also map this setting to a mobile number. (If you only want to enable Lync calling, leave the Phone Number mapping blank.) You can confirm the field name information by opening the Jive admin console and clicking **People** > **Settings** > **Profile Settings**. Enter the field names into the app configuration screen exactly as they appear in the Profile Settings dialog. (Note that a translation of the field name may be displayed in the profile, but the profile settings will show the actual field name.)

Users who don't have this information populated in the fields you identified will not be able to connect using the Lync integration, and users who are using Lync in Jive will not see the buttons they need to connect to these users, either on their profiles or on the hover card. If your community is not already populating these fields from a directory server, and you have made these fields editable on the profile, you can get users to provide the information themselves by clicking **Edit Profile** under their name or avatar.

Enabling the Jive Connector for Hangouts

The Jive Connector for Hangouts add-on allows access to phone calls and video chats directly from your Jive community using Google Hangouts.

To get set up:

1. Make sure your community meets the requirements.

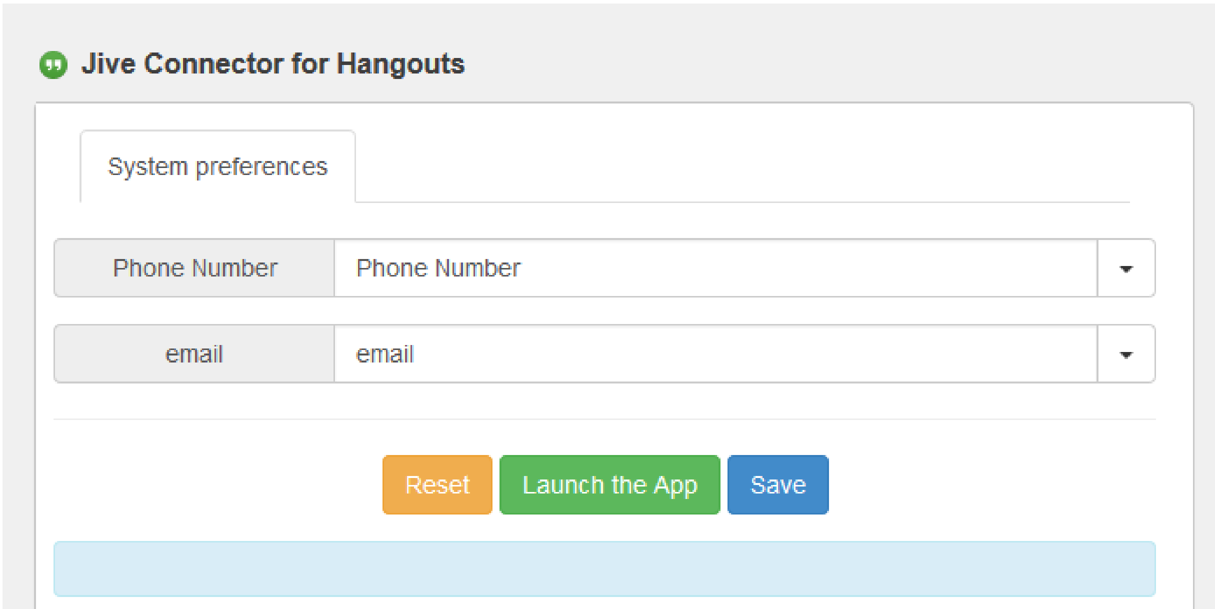
   Note: If you use Google for Work, you may have to enable Hangouts.

2. In Jive, click the menu under your name or avatar and select **Add-ons**.
3. Select the **Available** tab.
4. Next to Jive Connector for Hangouts, click **Install**.
5. **Note:** If you want to test this add-on before making it available to your entire community, select **This service is visible only to me**.

   Click **Install**.
   Successfully installed "Jive Connector for Hangouts" will appear once the add-on has installed.
6. In the top navigation of Jive, click **Apps** and select **Jive Connector for Hangouts**.

7. Select the user profile fields that Jive Connector for Hangouts should map to for phone number and email address.

   The add-on requires a community user's phone number to make phone calls and email to start video chats. The image below shows the defaults.



Attention: If your community does not populate phone and email fields from a directory server, your users will need to enter that information themselves by clicking their avatar, selecting **Edit Profile** > **Your Profile**, and entering their phone number and email.

8. Click **Save**.

Your community users can now use Google Hangouts to make phone calls and video chats with your Jive community.

Note: You can restrict access to Hangouts to specific user groups.

Setting Redirection Rules

Custom redirection rules can be used when you need a particular URL to point somewhere else within your community. This is useful, for example, to ensure your user's browser bookmarks work after moving content within the community.

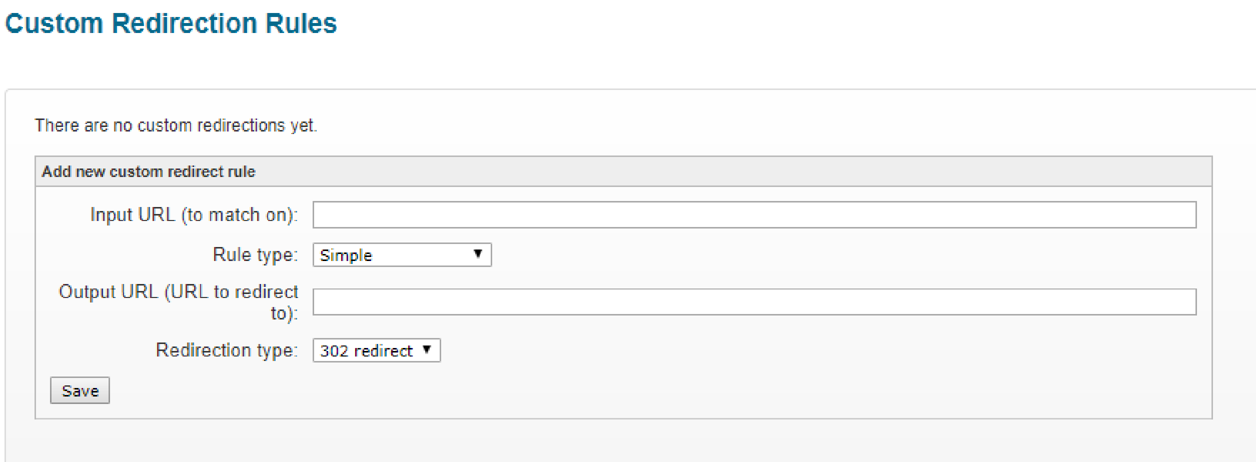
Benefits of this plugin:

- No need to modify the Apache configuration.
- More robust to future changes to the environment (migration, adding capacity,upgrades).
- Allows for "self-help" by enabling your team to add new redirects at any time.

- No restarts necessary to add new redirects.
- Redirects can be permanent (HTTP 301) or temporary (HTTP 302).

How to Use

Redirection rules are configured from the **Admin Console > System > Settings > Redirection Rules** page.



Once configured, whenever the application handles a new request, it checks against all the redirection rules and if a match is found, it issues a redirect to the output URL. Input rules match both the full URL (http://example.com/communityA) and the URL minus the domain (/communityA).

Important Notes

- As a safety feature, rules do not redirect from any URL that begins with /admin and each rule does not get executed more than once per request. For example, you cannot create an infinite loop by creating rules that redirect from A to B and B to A. Multiple rules can be executed for each request, for example, A to B and then B to C. The rules are checked in the order from top to bottom, so to execute a particular rule before others, move it to the top. All changes to the list take effect immediately.
- Jive supports two rule types:
  - **Simple** rules that are an explicit 1:1 match - if the exact input URL is found, the application will redirect to the output URL.
  - **Regular Expression** rules that allow the use of Java regular expressions in input and output URLs. This makes the input rule catch more than one URL, and do a simple string replacement into the output URL.
- Redirection rules can only redirect requests for source URLs contained in the domain of the Jive application.
- It is recommended to test new rules on a test site before implementing on production. At times, especially with regular expression rules, you create redirect rules you didn't intend, which could break parts of a site.
- This plugin is not intended to handle large redirection lists. If required, then it is recommended to use Apache rewrite rules.

- The Mobile plugin performs similar functionality as this plugin (catches requests and looks for mobile devices, to redirect them to mobile versions of pages). Since the plugin load order isn't predictable, this plugin could interfere with that process. If this occurs, the best solution is to remove the redirect plugin and use Apache rewrite rules instead.
- 301 type redirect rules cannot be used to redirect off-domain (that is, it cannot redirect from your site at example.com to a different domain such as google.com).
- If your site has a context (mysite.com/**mycontext**/), input rules will have to include the context: /mycontext/community/sales, for example.
- Simple rules are case insensitive. Regex rules are case sensitive, by default. However, you can create a Regex rule that matches insensitively by adding `?i` at the beginning of the input URL.

Creating a Redirection Rule

To create a redirection rule.

1. Navigate to **Admin Console**: **System** > **Settings** > **Redirection Rules**
2. Select **Rule Type** as either **Simple** or **Regular Expression**.
3. In the **Input URL (to match on)** field, specify the old URL.
4. in the **Output URL (to redirect to)** field, specify the new URL.
5. Select the **Redirection Type** as either **301** or **302**. A 301 redirect means that the page has been permanently moved to the new URL, where as, a 302 redirect means that the move is only temporary.

Redirect Rule Example

For example, let's assume that we have a space name called "Sales" that is based at the URL (http://example.com/community/sales). The Admin of that space later decides to change the name of the space to "Sales Team" and changes the URL to (http://example.com/community/salesteam). Most links inside the Jive application will be automatically updated to accommodate this change but links from outside the application (such as those cached by Google or in your users' browser bookmarks) will no longer resolve. To resolve this discrepancy, navigate to the **Admin Console > System > Management > Custom Redirection Rules** page and either set up a simple redirection rule that points from `/community/sales` to `/community/salesteam` or use regular expression to set up a new redirection rule that points from `^/community/sales/(.*)$` to `/community/salesteam/$1`. Now, whenever a user follows a link to (http://example.com/community/sales), they will be redirected automatically to (http://example.com/community/salesteam).

Setting Up Records Retention

The Records Retention plugin records who does what, and when they do it, in your Jive community. It captures snapshots of the activity within a community. This plugin is a useful tool to help an organization that needs to meet legal requirements, particularly in a regulated industry. It can also be used to track activity in a community.

Records Retention is a built-in plugin for Jive Cloud and Jive version 8.0 and later. To use Records Retention with an older version of Jive, contact support.

Understanding Records Retention

The Records Retention plugin is an effective tool to track activity in your Jive community. Before using it, be sure you understand what it captures and where it sends this captured information.

What is it?

The Records Retention plugin records who does what, and when they do it, in your Jive community. It captures snapshots of the activity within a community.

Why would I use it?

This plugin is a useful tool to help an organization that needs to meet legal requirements, particularly in a regulated industry. It can also be used to track activity in a community.

What does it capture?

The Records Retention plugin captures the following events for each content type and space type:

- **Document**: Create, Edit, Rate, Like, Bookmark, Comment, Edit Comment, Like Comment, Share, Delete, Add Recipients
- **File**: Create, Edit, Rate, Like, Bookmark, Comment, Edit Comment, Like Comment, Share, Delete, Add Recipients
- **Discussion**: Create, Edit, Reply, Rate, Like, Bookmark, Share, Delete, Unmark Question, Add Recipients
- **Poll**: Create, Edit, Rate, Like, Bookmark, Comment, Edit Comment, Like Comment, Vote, Share, Delete
- **Status Update**: Create, Like, Bookmark, Comment, Edit Comment, Like Comment, Repost, Share, Delete
- **Blog**: Create, Edit
- **Blog Post**: Create, Edit, Like, Drafts, Bookmark, Comment, Edit Comment, Like Comment, Share, Delete
- **Bookmark (external)**: Create, Edit, Like, Comment, Edit Comment, Like Comment, Bookmark, Share, Delete
- **Idea**: Create, Edit, Rate, Comment, Edit Comment, Like Comment, Bookmark, Share, Delete, Move
- **Direct Message**: Create, Reply, Add Recipients
- **Announcement**: Create, Edit Share: Create, Add Recipients
- **Project**: Create, Edit
- **Space**: Create, Edit, Invite

Where does it send this captured information?

There are currently three ways to configure the Records Retention plugin:

- **Email (SMTP)**: The SMTP format converts each event into an email message and delivers it to the configured inbox(es).
- **XML**: The XML format puts XML files into the Jive server's binstore.

- **Actiance (REST)**: The REST format sends each event to an instance of Actiance Vantage using RESTful communication.

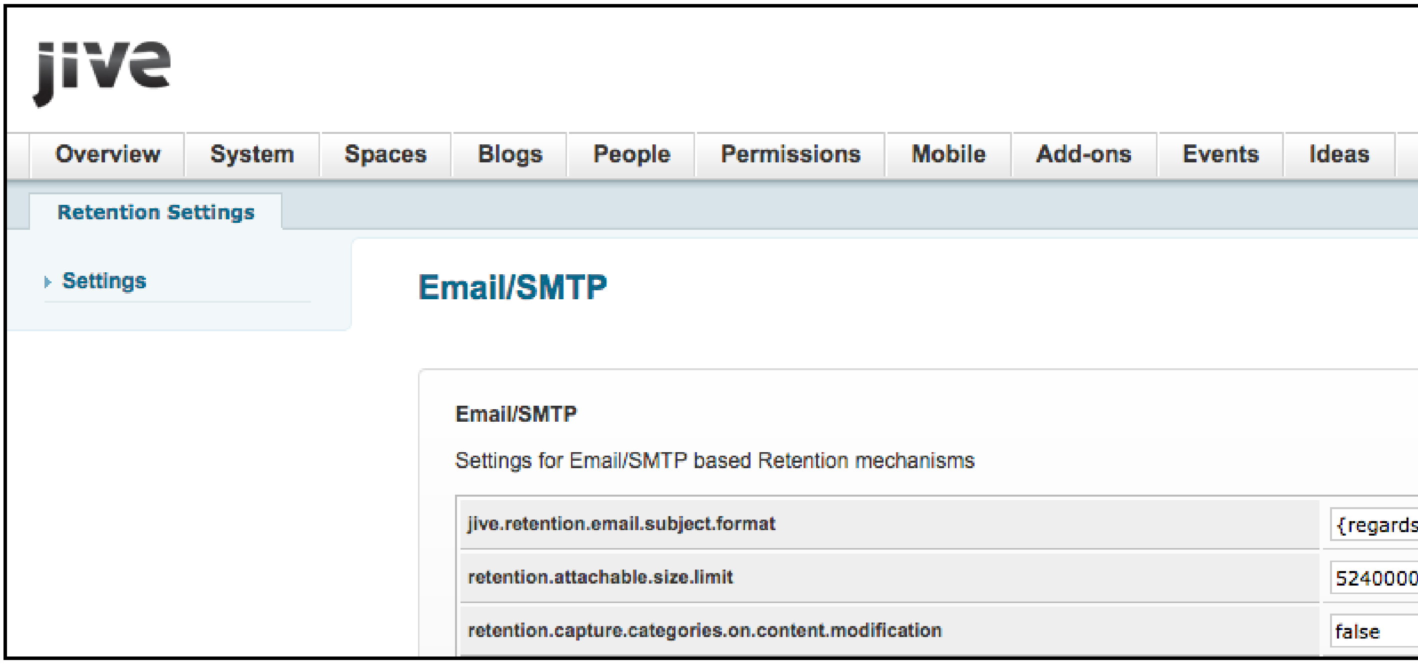
Enabling Records Retention

You'll have to set two system properties in the Admin Console in order to turn on Records Retention.

To enable Records Retention:

1. In the Admin Console, select **System** > **Management** > **System Properties**.
2. Set the `jive.module.records retention.enabled property` to `true`.
3. Add a system property with the name `__retention.delivery.task.bean.name`.
   a) If you want information delivered via **Email (SMTP)**, specify `retentionSmtpTask` for this property.
   b) If you want information delivered via **XML**, specify `actianceTask` for this property.
   c) If you want information delivered to **Actiance Vantage (via REST)**, specify `retentionRestApiTask` for this property.

After enabling the plugin (`jive.module.records retention.enabled`) and specifying the delivery type (`__retention.delivery.task.bean.name`), **Records Retention** appears as a top-level tab.



From here, you can configure the plugin.

Configuring Records Retention

Configuration for Records Retention is different depending on the delivery method you selected when enabling the plugin.

Configuring Records Retention for SMTP

You can configure Records Retention for SMTP from the Admin Console.

Once you enable the Records Retention plugin, you can configure it for your environment from the **Records Retention** tab. This tab contains a list of configurable settings. After you change any settings, click the **Save Settings** button at the bottom of the page for the settings to take effect.

Properties That Need to Be Configured

The following properties *must* be changed in order to set up Records Retention for SMTP:

- **retention.smtp.message.inbox.address**: The inbox email address where all retention messages are sent. This is typically an inbox that your archival systems scans. It can be a single email, or a comma-separated list of emails.
- **retention.smtp.reply.to.address**: The "reply to" address. You can use the same value as `retention.smtp.message.inbox.address` for this address. Bounced messages will also go to this address.
- **retention.smtp.envelope.sent.from.address**: The "sent from" address. The value of `retention.smtp.message.inbox.address` may also be used for this address. If retention messages are rejected by your gateway, you'll need to set this to an address that your gateway accepts.
- **retention.smtp.guest.email.to.use**: Replacement email address for content created by anonymous users. Not used for systems where guest access is disabled.
- **retention.smtp.systemuser.email.to.use**: Replacement email address for activity performed by the Jive system. In some scenarios, the "system user" performs actions in a batched or delayed manner, like when a user and all of their content is deleted from Jive.

Other Useful Properties

The following properties may be changed, as desired:

- **jive.retention.email.subject.format**: How the email subject is formatted. The default is `{regardsTo} [JIVE JOURNAL] - {subject}`, however this may be replaced with any hard-coded strings, along with the following replacement keys:
    - `{regardsTo}` — includes "Re:" on comments, replies and other non-root entries
    - `{subject}` — includes the raw subject or title of the root entry
    - `{contentType}` — includes the content type of the event
    - `{actionType}` — includes the action type of the event
    - `{objectId}` — includes the ID of the item affected by the event
    - `{objectType}` — includes the type of the item affected by the event
    - `{rootId}` — includes the id of the root entry of the affected conversation
    - `{rootType}` — includes the type of the root entry of the affected conversation

    For example, set this property to `{subject}` to include only the raw title of the conversation with no additional formatting.
- **retention.attachable.size.limit**: The file attachment size limit. This should be set to the same maximum size that attachments, images and uploads are configured within Jive. This should also be

less than the maximum size your email gateway will accept. This value is specified in bytes. Defaults to 52,400,000 bytes.

- **retention.deletes.processing.on**: Whether to capture delete events. Defaults to `false`. Note that delete records have very little information about the content that was deleted.
- **retention.include.author.details**: Whether to include author details in the header. Defaults to `false`. Set this to `true` to add a `X-AuthorUsername` header with the author's username as the value.
- **retention.reaper.messagearchive.number.of.days.to.keep**: The number of days for which records are retained after they are sent. Records can be saved for a period of time so you can replay events. Defaults to `30`.
- **retention.mail.smtp.server.override**: Whether to override the email settings already specified for the Jive server. Defaults to `false`. Once this value is set to `true` (and the settings are saved), a number of other settings appear (with the **retention.mail** prefix), allowing you to configure the SMTP server settings.
- **retention.max.number.of.cclist.addresses**: CC list threshold for when to send separate emails. If this value is set to `-1` (the default value), there is no threshold. For a list of email addresses larger than this threshold, the message is separated across multiple emails.
- **retention.resolve.and.store.cclists.for.spaces**: Whether to send activity to emails specified in the settings for a given space. Defaults to `true`. This feature can be turned off in order to improve performance.
- **retention.server.internalEmailDomains**: A comma-separated list of domains that are considered internal to your organization. If there is a value specified in this list, the plugin ignores users whose email addresses are not found within this list. Useful for reducing the recipient list for each email message, but does not prevent the expense of collecting user addresses on private or restricted content. If no value is specified, all email recipients are included regardless of domain.

Configuring Records Retention for XML

You can configure Records Retention for XML from the Admin Console.

Once you enable the Records Retention plugin, you can configure it for your environment from the **Records Retention** tab. This tab contains a list of configurable settings. After you change any settings, click the **Save Settings** button at the bottom of the page for the settings to take effect.

Properties That Need to Be Configured

The following properties *must* be changed in order to set up Records Retention for XML:

- **retention.xml.output.file.directory.name**: The directory where the retention files will be saved.
- **retention.xml.output.file.filename.prefix**: The filename prefix for the retention files. The remainder of the filename includes a timestamp to uniquely identify it.

Other Useful Properties

The following properties may be changed, as desired:

- **jive.retention.email.subject.format**: How the email subject is formatted. The default is `{regardsTo} [JIVE JOURNAL] - {subject}`, however this may be replaced with any hard-coded strings, along with the following replacement keys:
  - `{regardsTo}` — includes "Re:" on comments, replies and other non-root entries
  - `{subject}` — includes the raw subject or title of the root entry
  - `{contentType}` — includes the content type of the event
  - `{actionType}` — includes the action type of the event
  - `{objectId}` — includes the ID of the item affected by the event
  - `{objectType}` — includes the type of the item affected by the event
  - `{rootId}` — includes the id of the root entry of the affected conversation
  - `{rootType}` — includes the type of the root entry of the affected conversation

  For example, set this property to `{subject}` to include only the raw title of the conversation with no additional formatting.
- **retention.comma.separated.emails.for.error.reporting**: A list of comma-separated email addresses used for error reporting. If the XML creation fails (and is recoverable), an email is sent to each email address listed in this setting.
- **retention.deletes.processing.on**: Whether to capture delete events. Defaults to `false`. Note that delete records have very little information about the content that was deleted.
- **retention.error.reporting.email.subject**: Subject string for the error reporting email. If the XML creation fails (and is recoverable), an email is sent with this value as the subject.
- **retention.include.author.details**: Whether to include author details in the header. Defaults to `false`. Set this to `true` to add a `X-AuthorUsername` header with the author's username as the value.
- **retention.reaper.actiancefile.number.of.days.to.keep**: The number of days for which completed XML files are kept.
- **retention.reaper.messagearchive.number.of.days.to.keep**: The number of days for which records are retained after they are sent. Records can be saved for a period of time so you can replay events. Defaults to `30`.
- **retention.reaper.capturedbinary.number.of.days.to.keep**: The number of days for which records are kept. Once a record is sent, it is considered "done" by the retention module. However, records can be saved for a period of time so you can "replay" events. This setting refers to binaries, including attachments, images and uploaded files.
- **retention.resolve.and.store.cclists.for.spaces**: Whether to send activity to emails specified in the settings for a given space. Defaults to `true`. This feature can be turned off in order to improve performance.
- **retention.xml.directory.to.put.final.file**: Directory where completed retention files are copied.

Configuring Records Retention for Actiance Vantage

You can configure Records Retention for Actiance Vantage (via REST) from the Admin Console.

Once you enable the Records Retention plugin, you can configure it for your environment from the **Records Retention** tab. This tab contains a list of configurable settings. After you change any settings, click the **Save Settings** button at the bottom of the page for the settings to take effect.

Properties That Need to Be Configured

The following properties *must* be changed in order to set up Records Retention for Actiance Vantage:

- **retention.actiance.vantage.authkey**: The consumer key for the network.
- **retention.actiance.vantage.authsecret**: The consumer secret for the network.
- **retention.actiance.vantage.hosts**: The domain name of the Actiance Vantage server to send messages to. This value should not include a protocol or port.
- **retention.actiance.vantage.networkid**: The Network ID assigned to the collaboration network registered in Actiance Vantage.

Other Useful Properties

The following properties may be changed, as desired:

- **retention.actiance.vantage.logresponses**: Whether to log Records Retention activity. Defaults to `true`. If true, the plugin outputs additional debugging information in the logs (provided the "com.jivesoftware.retention.task.restapi.impl" logger is set to INFO or lower).
- **retention.deletes.processing.on**: Whether to capture delete events. Defaults to `false`. Note that delete records have very little information about the content that was deleted.
- **retention.include.author.details**: Whether to include author details in the header. Defaults to `false`. Set this to `true` to add a `X-AuthorUsername` header with the author's username as the value.
- **retention.reaper.messagearchive.number.of.days.to.keep**: The number of days for which records are retained after they are sent. Records can be saved for a period of time so you can replay events. Defaults to `30`.
- **retention.reaper.capturedbinary.number.of.days.to.keep**: The number of days for which records are kept. Once a record is sent, it is considered "done" by the retention module. However, records can be saved for a period of time so you can "replay" events. This setting refers to binaries, including attachments, images and uploaded files.
- **retention.resolve.and.store.cclists.for.spaces**: Whether to send activity to emails specified in the settings for a given space. Defaults to `true`. This feature can be turned off in order to improve performance.

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.

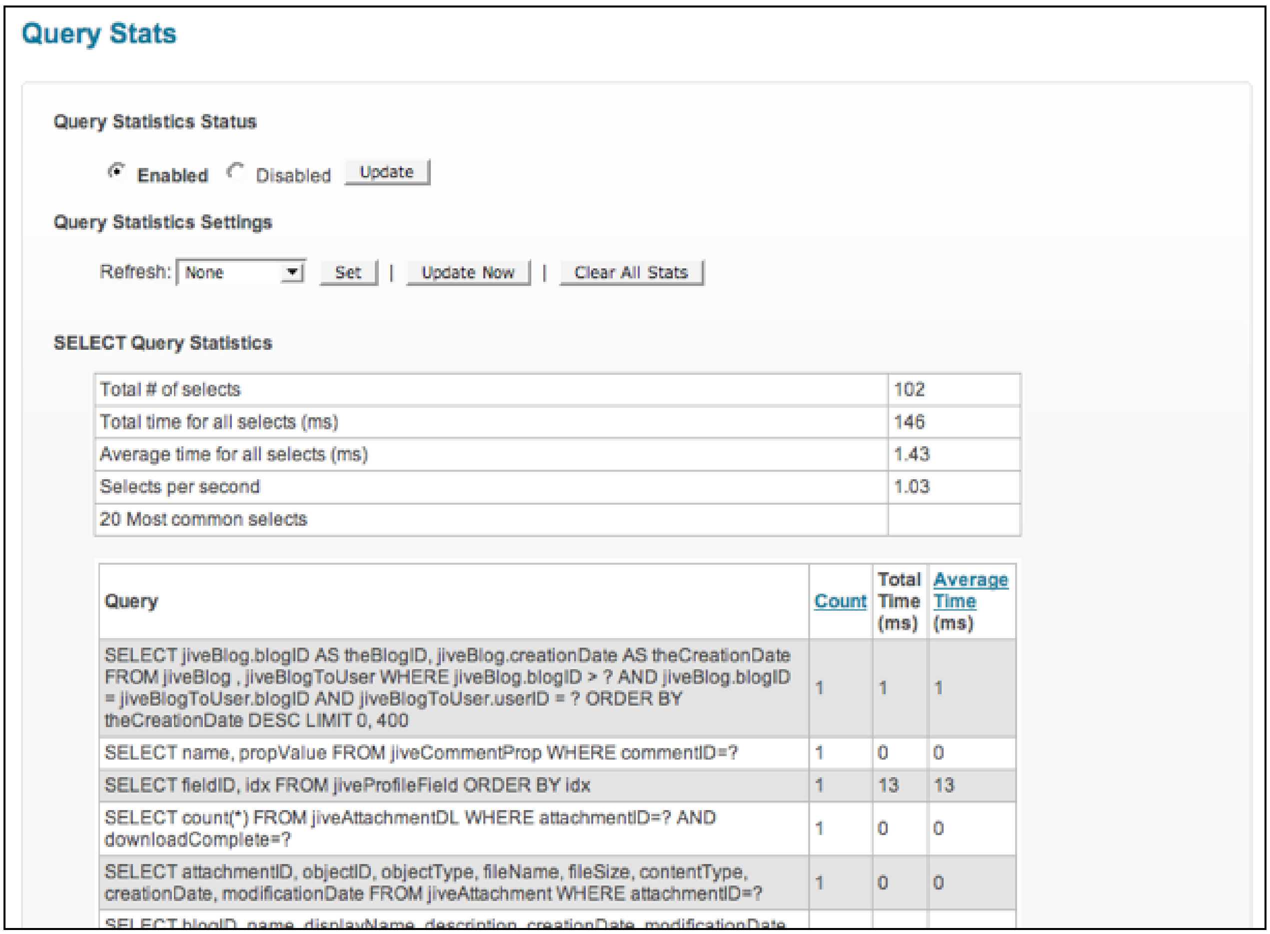
Examining Database Queries

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.

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

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.

You can filter this page by user and date.

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 drop-down menu, select the number of items you want to see, then click **Submit Query**.

Integrating Web Analytics

You can connect your community with a third-party web analytics provider to track site navigation and marketing analytics on your Jive site.

Fastpath: Admin Console: System > Settings > Third-Party Analytics

The **Third-Party Analytics** settings let you use a web analytics tool like Google Analytics or Marketo to monitor what's happening on your Jive site by inserting tracking code in your Jive pages. This code sends information back to the web analytics provider each time a page on your site is accessed. Your analytics results won't be displayed anywhere in Jive: you can view them using your analytics reporting from your analytics provider.

Note: Jive's Analytics offerings don't have any connection to this third-party data collection. They use different metrics, and results are not directly comparable.

To set up reporting, paste your Google or Marketo ID in the appropriate tab and click **Save Settings**. If you were already using this setting with a previous version, you'll see a tab that allows a more free-form JavaScript implementation. This method is no longer recommended because of security risks. If you need to implement a different third-party tool, please contact Support.

Connecting Communities with Bridges

When you connect two communities with a 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 information, ask your Jive account representative.

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. On the community you're connecting to, enable bridging for registered users (**Admin Console: System** > **Settings** > **Web Services** > **Bridging**).
2. Back on the primary community, add the bridge by going to **System** > **Settings** > **Bridges** and clicking **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 user name 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 and other extensions.

Depending on how your community is set up and which plugins you've purchased, you may or may not be able to access some of these features.

To add a theme to your community, be sure to read the Theming section.

Simple Phrase Substitution 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, be sure to read Advanced Phrase Substitution in the UI.

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.

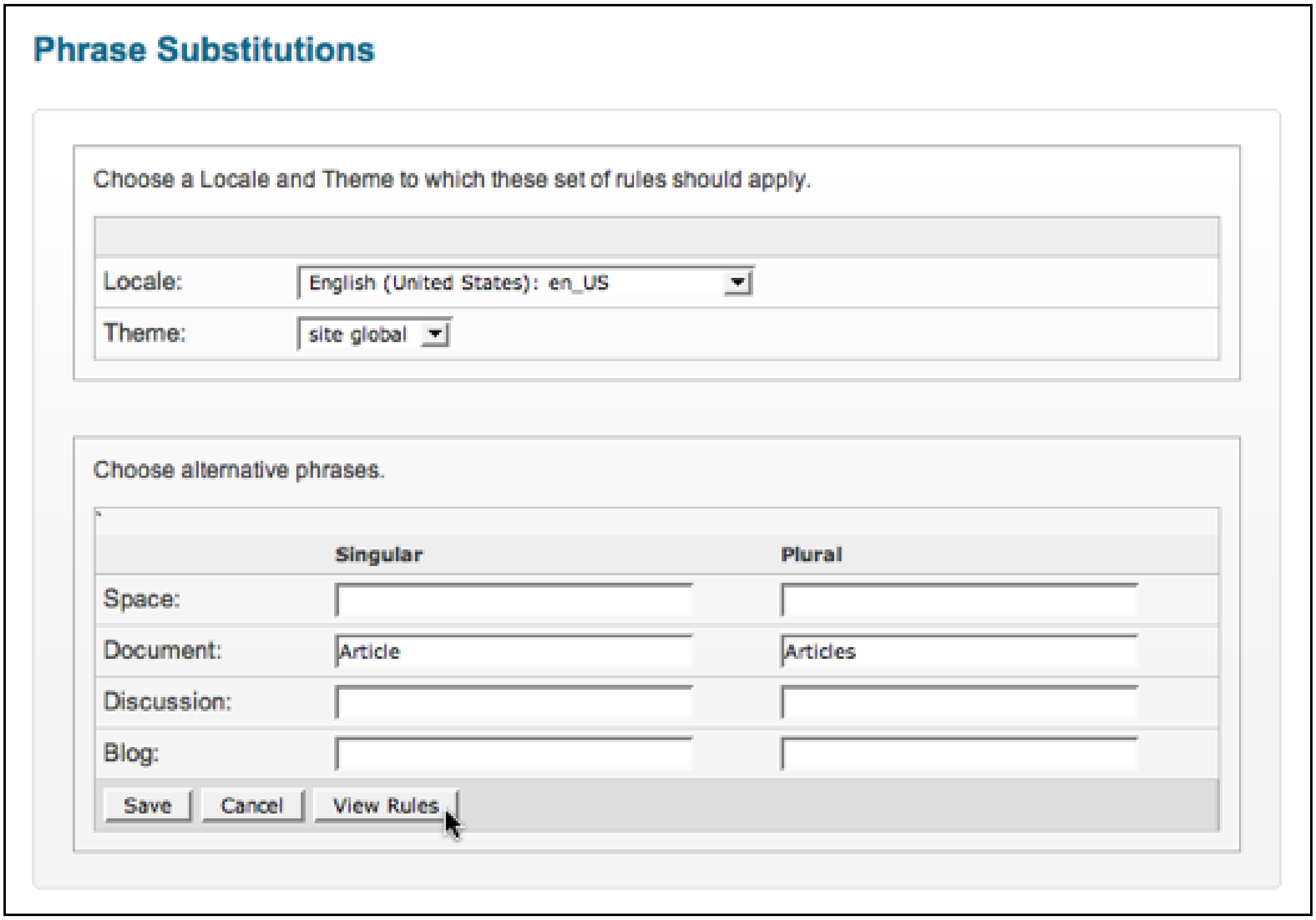
Making Simple Substitutions

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 substitutions.

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 use to customize Overview pages. As an administrator, you can control which widgets are available to users. Keep in mind that these widgets are used only on the old-style widgetized Overview pages for places. Places that have an Activity page and a Place Template use the newer, more performant data tiles and don't include widgets.

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.

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. From 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.

Fastpath: Admin Console: System > Settings > Feeds

After you have made any adjustments to the feed settings, be sure to click **Save Settings** at the bottom of the page.

If you have an internal community (i.e., communities that typically involve only employees or other internal audiences), basic authentication is required by default.

Note: For users to use the links available in feeds, 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. For more information, see Changing the jiveURL on page 25.

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, or in the content.
- 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 user name and password), you might need to prepend the feed URL with the user name 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 user name 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

Feed Subject	URL Syntax
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>
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

Feed Subject	URL Syntax
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

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 amount of space you'll need for shared storage. For more on these requirements, see Binary Storage in Required External Components

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 file system:

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`). Refer to Sizing Binary Storage for help estimating the amount of shared storage you'll need.
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.

Property	Description
checkmail.host	Email server name used for verifying mail settings provided in the System - Settings - Email Server screen in the Admin Console.
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.
document.searchComments.enabled	`true` to enable return of comments on search; false to disable it (default: true).
documentmanager.correctdeletedusers.complete	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)
email.search.allowWhiteSpace	Set to `true` if you want people search to allow white spaces in the email field. Default is false.
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

Property	Description
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.APIThrowsClause.enabled	Setting to `true` adds a security string to the beginning of every core V3 JSON response and all data returned via API. Setting to false with no query parameters removes the security string, except for vulnerable arrays. When you set to false and you add a `noThrows=true` query parameter, the security string is removed for all data, even vulnerable arrays. Default is false with no parameters.
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.
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.

Property	Description
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.<typevalue>	`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.module.video.enabled	Set to `true` if you want enable the video feature by default with only the Embed a Video option (not upload or record). Default is true. **Note:** You can use video.upload.enabled and video.webcam.enabled to enable/disable those features (both are true by default).
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.

Property	Description
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.
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

Property	Description
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.

Property	Description
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
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.

Property	Description
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)
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.PermissionHandle

Managing Places and Pages

You can use space hierarchies and specially designed place pages in your community to highlight the focus and function of different areas.

Designing Overview Pages and Place Pages

There are several locations in Jive where, if you have rights, you can design a page with customized images and information, using either widgets or tiles as building blocks. These places include:

- The Home page of the entire community, if it is enabled.
- The landing page of a place. (A place is a space, group, or project.)
- A custom page added to the navigation of a place, if Pages are enabled in your community and the Overview page has been disabled for the place.
- The Your View page, if it is enabled in your community.

Widgets and tiles both contain content blocks that allow you to lay out a page. Usually the kind of page determines which you will use, but as the following table shows, there are two different models for customizing place pages: Overview pages, which rely on widgets, and Activity pages, which rely on tiles. For help deciding which to use in a place, see Tile Pages Versus Widget Pages on page 196.

The following table shows where you can use widgets, where you can use tiles, and where you have a choice.

	Tiles	**Widgets**
Community Home Page	no	yes
Your View	yes	no
Spaces, groups, or projects (Activity page)	yes	no
Spaces, groups, or projects (Overview page)	no	yes
Spaces, groups, or projects (custom Pages)*	yes	no

*Custom Pages in a space, group, or project are not available unless the Overview page for that place has been disabled. This means you can't have Overview and custom pages activated in the same place.

Tile Pages Versus Widget Pages

In some cases, you may need to choose between designing pages based on widgets and pages based on tiles.

When you're setting up a new place, you can choose to enable an Overview page, which uses widgets, or an Activity page, which uses tiles. Place templates, which are customized for specific kinds of collaboration, always use tiles. Tiles use newer technology and are mobile-optimized; widgets cannot be displayed on a mobile device. Keep in mind that if you disable the Overview page in a place, you can choose to add additional tile-based custom Pages, which let you spread out your content over multiple tabs with less content (and thus better mobile usability).

Use widgets when:

- You are configuring a community home page for desktop users. (Widgets are your only choice here.)
- You're setting up a Jive-x community and you need to take advantage of the customer service widgets set.

- You have an Overview page you created in an earlier version of Jive and you're not ready to change the look and feel of the place.
- Your community or the audience of your Place doesn't rely heavily on mobile usage.

Use tiles when:

- You are configuring a community home page for mobile browser users. (Tiles are your only choice here.)
- Your community or the audience of your Place relies heavily on mobile usage. (For example, many sales teams operate remotely.)
- You need to bring streamed content, such as a Chatter or Facebook stream, into your place from outside the community.
- You want to include custom pages as well as an Activity page in a place. (To use the Pages feature in a place, you need to disable the widget-based Overview page in that place.)

Enabling Custom Pages in Places

The Pages feature allows place owners to add additional pages to a place.

New pages will be available as links in the main header of the place, next to the existing links to Content, Activity, and People, and can be re-ordered. This setting is enabled by default.

To enable and disable this feature:

1. In the Admin Console, go to **System** > **Settings** > **Pages**.
2. Select **Enabled** or **Disabled**.
3. Choose the number of pages you want place owners to be able to add to their places. The maximum is 5, which is the default setting.
4. Click **Save**.

Place owners will now see the option to add Pages to a place under the **Manage** menu.

Adding a Custom Page to a Place

Place owners can add additional pages to a place and configure the pages with tiles. New pages will appear as options in the main header of the place, to the left of the existing links to the place's Content, Activity, and People. Your community manager must enable this feature in the Admin Console for a place owner to see the option of adding pages to a place.

New Pages allow you more flexibility in designing your place for your specific needs. For example, you might add a Product Schedule page that shows your upcoming shipping dates and product owners. Or, you could create a page called The CEO's Blog that features your fearless leader's blog posts.

First, you'll need to set your place's navigation to Activity + Pages:

1. Go to the place you own and select **Manage** > **Settings**.
2. Click the pencil icon next to the place's name in the place header.
3. Click **Advanced Options** > **Activity + Pages**, and then **OK**.
4. **Save** this change to the place.

Add a New Page to a Place

After you've set the place's navigation to Activity + Pages, you can add a new Page to the place:

1. Click **Manage** > **New Page**. Note that you will only see this option after you've set the place's navigation to Activity + Pages. Your community manager determines the number of custom Pages you can add to a place. The limit is five.
2. In the Create a Page popup, enter a name for your page.
3. Select the column layout you want for the new page.
4. Click **OK**.
5. Add and configure the tiles you want to appear on the new page.
6. Click **Save**.

To make additional changes, click **Edit page** in the upper right corner of the page. You can also **Delete** the page.

Note: If you reset the place's navigation (under Advanced Options) to Overview or Activity + Overview and save that change, you will no longer see the new page you just created. However, if you then *reset* the place's navigation to Activity + Pages and save *that* change, you will see your new page again. In other words, you don't actually lose any new pages you have created if you change the place navigation. You just don't see them when the place navigation is set to Overview or Activity + Overview.

Designing Activity Pages for Places

To customize a space, group, or project with a preconfigured set of content options designed for specific collaboration goals, select an Activity page as the landing page and then apply and configure a *Place Template*.

An Activity page shows a real-time activity stream of updates happening in the place, such as status updates and replies to content. Place templates are the starting point for setting up an Activity page: each template contains an activity stream, plus a configurable group of tiles that reflect typical collaboration goals. When you edit an existing place, create a group, start a project, or (if you have permission) create a new space, you'll choose from a list of pre-designed Place Templates. Just quickly set up a few key tiles to start collaborating in reality-tested environments such as:

- A Deal Room for building out a sales opportunity with your team
- A Vendor Collaboration place for partnering with external talent
- A private Pre-Hire Collaboration place for discussing potential job candidates

When you use a place template you can add and remove any of the tiles and move them around within the layout. Tiles are visual building blocks of information. They may dynamically pull data either from around your Jive installation or from a third-party service, or they may be configured with information you've hand-selected.

Assigning a Place Template

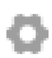
When you assign a Place Template to an existing project, space, or group, you get a preconfigured Activity page that contains the tiles and layout included in the template.

Assigning a Place Template to a place only affects the Activity page in that place. It changes the selection of tiles on the Activity page and the order they're displayed in.

Warning: When you assign a new Place Template to a place whose tiles have been configured, you lose any configuration in the tiles. For example, if you created a People list, it will be wiped out and replaced with empty, unconfigured tiles, even if the new Place Template includes a People tile. The exception is that Salesforce authentication will persist if you apply a different Place Template that uses a Salesforce connection.

To assign a new Place Template to an existing place:

1. Navigate to a place you have rights to modify.
2. Click **Manage** > **Settings** to enter the edit view of the place.
3. Once in edit view, you can click **Browse Templates** in the top left just under Home.
4. Choose a Place Template for this place. Place templates determine what tiles and streams will provide the layout and data for your group's Activity page. Choose the one that's right for the kind of collaboration that will happen here.
5. Click **Apply Template**.
6. Click

   and configure each tile that requires it.
7. Click **Apply** in the tile dialog.
8. Click **Save** to update the place with your changes.

Creating a New Place Template

You can create a new place template based on a currently configured place using the settings under Manage > Save as new template. Only edited templates have the option of being saved as new ones.

If you want to create a new Place Template, you can base one on the tiles included in an existing place you've configured and saved. For example, if you create a group using the General Collaboration template, but add and delete some tiles to include different information in that group, you can use **Save as new template** to save the layout of the tiles as a Place Template. Then you can assign that template to other places you create.

Note: If you have Community Manager rights, you can save Place Templates as Community templates so that other people in the community can use them. If you're not, only you will see your saved templates in My Templates.

A template saves the type, order, and layout of tiles for a place. It does not save the configuration of those tiles. If you've created lists of links using the Helpful Links tile, for example, and saved a template based on that place, places with that template assigned will have the Helpful Links tile in the same position. But they will not include the link list you created. This is true even if you later reassign that template to the same group.

To create a template based on an existing place:

1. Go to the place you want to base the template on. You need to have rights to a place to save it as a template.
2. Modify the current place's Activity page by selecting **Manage** > **Settings**. Make sure the tiles and layouts are customized the way you want them before you create a template.
3. If you've made revisions to the current place's template, click **Save** to save them to the current template.
4. In the Manage menu, click **Save as new template** and specify a name and description for the new template. You'll only see this option if you have customized the current template.
5. Provide a name and some tags for the new template. Tags will be used to populate the Similar Places tile.
6. Click **Save**.
7. If you want to apply the new template to a place, click **Manage** > **Settings**, and then select the new template from **Browse Templates** > **My Templates** to select and apply it.

Saving a Place Template Globally

If you have community manager rights, you can save a Place Template for other users to apply when they set up places.

Community managers can save Place Templates after they're customized. They'll show up in the Community Templates list when place owners are selecting a Place Template. New templates will be based on the configuration of an existing place.

To set up a new place template:

1. Go to the place you want to base the template on. Make sure the tiles and layout are customized the way you want them before you create a template.
2. Click **Manage** > **Save as Community template**.
3. Provide a name and some tags for the new template, and decide what category the template should be shown in. Tags will be used to populate the Similar Places tile.
4. If you want to apply the new template to this page, click **Manage** > **Settings** > **Browse Templates**. From here, you can select the category and template.

Deactivating a Place Template

If you want to limit the templates community users can select, you can activate and deactivate them in the template browser.

You may want to make some templates unavailable to your users. (For example, if you don't use Salesforce.com in your organization, you might want to hide the Deal Room template, which includes a Salesforce integration tile.) This prevents users from selecting the template from now on, but doesn't remove the template from any places where it's already in use. To make some templates invisible to users:

1. Navigate to a place.
2. Click **Manage** > **Settings** to enter the edit view of the place.

3. In the edit view, click **Browse templates** at the top of the place.
4. Select a template.
5. Next to the template description, click **Deactivate this template**.
6. Click **Save**.
7. To reactivate a deactivated template, just select **Reactivate this template** while browsing it. You won't be able to apply the template until you've reactivated it.

Managing Tiles and Templates

You can manage the categories of tiles and templates that are available when creating places, and create your own categories for displaying new templates and tiles.

You may find that you don't want to make the full range of templates or tiles available to users who create places, or you may have created some tiles and templates of your own that you'd like to organize in categories when they're displayed in the UI. You can use the admin console to create new categories for templates and tiles and to hide template or tile categories that you don't want users to see.

To manage template or tile categories:

1. In the Admin Console, go to **Add-ons** > **Place Template Management** or **Add-ons** > **Tile Categories**.
2. If you want to **create** a new category, click **Add a category** and type the name in the list.
3. If you want to **hide** a category from users who are creating new places, including all the tiles or templates it includes (unless they're also in another category), click **Hide Category**. For example, hiding the Places tile category will hide all the tiles that are unique to that category, and users won't see Places tiles as an option when they're adding tiles. However, they'll still see the Key Places and Content tile because it is also part of the Content category. You might find the Tile Reference helpful when thinking about this.

   Hiding a category has no effect on places that have already been created. Places that are already using tiles or templates in a category you've hidden will still use them, but they won't be selectable to users who are creating or modifying a place.
4. If you want to **delete** a category from the list (and make it invisible to users who are creating and editing places), click Delete Category. The category will be marked for deletion. (You won't be able to delete the built-in Jive categories, but you can still hide them if you don't want to use them.)

   Deleting a category has no effect on places that have already been created. Places that are already using tiles or templates in a category you've deleted will still use them, but they won't be selectable to users who are creating or modifying a place.
5. When your list of categories is the way you want it, click **Save** to apply your changes.

Place Template Reference

Each Place Template contains a unique selection of tiles customized for a specific collaborative activity, such as Sales or IT.

Templates are organized according to the kind of workgroup that typically uses them, but you can rename and customize any template. The right template contains more or less the tiles that you need. For example, if you want to set up a place to track items identified for quick follow-up, you could pick the Sales Answer

Desk template when creating the place, even if Sales isn't your main goal. This template includes a Featured People tile to identify people you can direct questions to, tracks items marked for Action and recent decisions, and surfaces popular content. For more information about data tiles and the information they're based on, see the Tile Reference.

It's possible to develop custom tiles that aren't included in the product, including tiles for third-party integrations. Check out developers.jivesoftware.com for the latest developer information and programming tutorials to get you started.

Note: You may not see events or ideas as feature options in a template if your community does not have these additional modules enabled. In addition, externally-facing communities (those serving customers, partners, and vendors), do not have the Corporate Communications, HR, IT, or R&D, or Sales templates. Internally-facing communities (those serving employees), do not have the Customer Service, Other, or Products templates.

General Place Templates

General Place Templates are useful for general collaboration cases not focused on a specific business function, and can easily be used as the base for custom templates.

Templates are organized according to the kind of workgroup that typically uses them, but you can rename and customize any template. The right template contains more or less the tiles that you need. For example, if you want to set up a place to track items identified for quick follow-up, you could pick the Sales Answer Desk template when creating the place, even if Sales isn't your main goal. This template includes a Featured People tile to identify people you can direct questions to, tracks items marked for Action and recent decisions, and surfaces popular content. For more information about data tiles and the information they're based on, see the Tile Reference.

Note: You may not see events or ideas as feature options in a template if your community does not have these additional modules enabled. In addition, externally-facing communities (those serving customers, partners, and vendors), do not have the Corporate Communications, HR, IT, or R&D, or Sales templates. Internally-facing communities (those serving employees), do not have the Customer Service, Other, or Products templates.

Table 16: Available in Internally-facing Communities

Place Template	Tiles	Features	Default Type	Default Tag(s)
Team Collaboration	Top Participants Key Content and Places Featured Content Recent Decisions Finalized Content	Videos Documents Discussions Ideas Polls Events Blogs Projects Status Updates (in groups only)	Open	—
Best Practices Sharing	Featured Content Popular Content Image Gallery Top Participants Key Dates	Videos Documents Discussions Ideas Polls Events Blogs Projects Status Updates (in groups only)	Open	best practice

Place Template	Tiles	Features	Default Type	Default Tag(s)
Customer 360	Gauge Featured Content Helpful Links Featured People Key Dates	Videos Documents Discussions Ideas Polls Events Blogs Projects Status Updates (in groups only)	Open	—
War Room	Gauge Finalized Content Action Items Top Participants Featured Content	Documents Discussions Projects Status Updates (in groups only)	Open	—

Table 17: Available in Externally-facing Communities

Place Template	Tiles	Features	Default Type	Default Tag(s)
Community Member Group	Key Content and Places Popular Content Top Participants	Videos Documents Discussions Ideas Polls Events Blogs Projects	Open	—

Place Template	**Tiles**	**Features**	**Default Type**	**Default Tag(s)**
Video Channel	Featured Video (3) Featured Content	Videos Discussions	Open	video
Blog Central	Top Participants Featured Content Popular Content	Blogs	Open	blogs

Corporate Communications Place Templates

Corporate Communications Place Templates include selections of tiles focused on sharing videos, live events, communications planning, and blogging.

Templates are organized according to the kind of workgroup that typically uses them, but you can rename and customize any template. The right template contains more or less the tiles that you need. For example, if you want to set up a place to track items identified for quick follow-up, you could pick the Sales Answer Desk template when creating the place, even if Sales isn't your main goal. This template includes a Featured People tile to identify people you can direct questions to, tracks items marked for Action and recent decisions, and surfaces popular content. For more information about data tiles and the information they're based on, see the Tile Reference.

Note: You may not see events or ideas as feature options in a template if your community does not have these additional modules enabled. In addition, externally-facing communities (those serving customers, partners, and vendors), do not have the Corporate Communications, HR, IT, or R&D, or Sales templates. Internally-facing communities (those serving employees), do not have the Customer Service, Other, or Products templates.

Place Template	**Tiles**	**Features**	**Default Type**	**Default Tag(s)**
Blog Central	Top Participants Featured Content Popular Content	Blogs Status Updates (in groups only)	Open	blogs

Place Template	Tiles	Features	Default Type	Default Tag(s)
Communications Planning	Key Dates Featured Content Action Items Recent Decisions Finalized Content Image Gallery	Videos Documents Discussions Ideas Polls Events Blogs Projects Status Updates (in groups only)	Private	corp comms
Live Event Activity Streaming	Top Participants Key Dates	Documents Status Updates (in groups only)	Open	event, stream

Customer Service Place Templates

Customer Service Place Templates include selections of tiles focused on finding information and supporting customers.

Templates are organized according to the kind of workgroup that typically uses them, but you can rename and customize any template. The right template contains more or less the tiles that you need. For example, if you want to set up a place to track items identified for quick follow-up, you could pick the Sales Answer Desk template when creating the place, even if Sales isn't your main goal. This template includes a Featured People tile to identify people you can direct questions to, tracks items marked for Action and recent decisions, and surfaces popular content. For more information about data tiles and the information they're based on, see the Tile Reference.

Note: You may not see events or ideas as feature options in a template if your community does not have these additional modules enabled. In addition, externally-facing communities (those serving customers, partners, and vendors), do not have the Corporate Communications, HR, IT, or R&D, or Sales templates. Internally-facing communities (those serving employees), do not have the Customer Service, Other, or Products templates.

Place Template	Tiles	Features	Default Type	Default Tag(s)
Knowledge Management	Key Content and Places Featured Content Finalized Content	Documents	Open	help, knowledge base, documentation
Customer Support	Featured People Action Items Recent Decisions Finalized Content Popular Content	Documents Discussions	Secret	—
Support and Community Team Backchannel (private discussions)	Featured Content Recent Decisions Top Participants	Documents Discussions Ideas	Secret	backchannel
Project Management	Gauge Key Dates Key Content and Places	Videos Documents Discussions Ideas Polls Events Blogs Projects	Secret	—

Human Resources Place Templates

Human Resources Place Templates include selections of tiles focused on HR team communications and pre-hire communication with future employees.

Templates are organized according to the kind of workgroup that typically uses them, but you can rename and customize any template. The right template contains more or less the tiles that you need. For example, if you want to set up a place to track items identified for quick follow-up, you could pick the Sales Answer Desk template when creating the place, even if Sales isn't your main goal. This template includes a Featured People tile to identify people you can direct questions to, tracks items marked for Action and recent decisions, and surfaces popular content. For more information about data tiles and the information they're based on, see the Tile Reference.

Note: You may not see events or ideas as feature options in a template if your community does not have these additional modules enabled. In addition, externally-facing communities (those serving customers, partners, and vendors), do not have the Corporate Communications, HR, IT, or R&D, or Sales templates. Internally-facing communities (those serving employees), do not have the Customer Service, Other, or Products templates.

Place Template	Tiles	Features	Default Type	Default Tag(s)
Best Practices Sharing	Featured Content Popular Content Image Gallery Top Participants Key Dates	Videos Documents Discussions Ideas Polls Events Blogs Projects Status Updates (in groups only)	Open	—
Pre-Hire Collaboration	Featured People Key Content and Places Helpful Links Action Items Key Dates	Videos Documents Discussions Ideas Polls Events Blogs Projects Status Updates (in groups only)	Private Externally-accessible	pre-hire

IT Place Templates

Information Technology Place Templates include selections of tiles focused on technology rollouts, helpdesk support, and upgrade planning.

Templates are organized according to the kind of workgroup that typically uses them, but you can rename and customize any template. The right template contains more or less the tiles that you need. For example, if you want to set up a place to track items identified for quick follow-up, you could pick the Sales Answer Desk template when creating the place, even if Sales isn't your main goal. This template includes a Featured People tile to identify people you can direct questions to, tracks items marked for Action and recent decisions, and surfaces popular content. For more information about data tiles and the information they're based on, see the Tile Reference.

Note: You may not see events or ideas as feature options in a template if your community does not have these additional modules enabled. In addition, externally-facing communities (those serving customers, partners, and vendors), do not have the Corporate Communications, HR, IT, or R&D, or Sales templates. Internally-facing communities (those serving employees), do not have the Customer Service, Other, or Products templates.

Place Template	Tiles	Features	Default Type	Default Tag(s)
Best Practices Sharing	Featured Content Popular Content Image Gallery Top Participants Key Dates	Videos Documents Discussions Ideas Polls Events Blogs Projects Status Updates (in groups only)	Open	best practice

Place Template	Tiles	Features	Default Type	Default Tag(s)
Technology Rollout and Support	Featured Video Featured Content Finalized Content Key Dates Helpful Links	Videos Documents Discussions Ideas Polls Events Blogs Projects Status Updates (in groups only)	Open	technology
IT Helpdesk Collaboration	Featured Content Popular Content Helpful Links Action Items Recent Decisions	Videos Documents Discussions Ideas Polls Events Blogs Projects Status Updates (in groups only)	Open	helpdesk

Place Template	Tiles	Features	Default Type	Default Tag(s)
IT Upgrade Planning	Key Dates Action Items Featured People Helpful Links Image Gallery	Videos Documents Discussions Ideas Polls Events Blogs Projects Status Updates (in groups only)	Open	it, upgrade
RFP Workgroup	Key Dates Popular Content Finalized Content Top Participants Key Content and Places Gauge	Documents Discussions Projects Status Updates (in groups only)	Private	request_for_proposal, rfp

Marketing Place Templates

Marketing Place Templates include selections of tiles focused on assembling marketing campaigns and collateral.

Templates are organized according to the kind of workgroup that typically uses them, but you can rename and customize any template. The right template contains more or less the tiles that you need. For example, if you want to set up a place to track items identified for quick follow-up, you could pick the Sales Answer Desk template when creating the place, even if Sales isn't your main goal. This template includes a Featured People tile to identify people you can direct questions to, tracks items marked for Action and recent decisions, and surfaces popular content. For more information about data tiles and the information they're based on, see the Tile Reference.

Note: You may not see events or ideas as feature options in a template if your community does not have these additional modules enabled. In addition, externally-facing communities (those serving customers, partners, and vendors), do not have the Corporate Communications, HR, IT, or R&D, or Sales templates. Internally-facing communities (those serving employees), do not have the Customer Service, Other, or Products templates.

Table 18: Available in Internally-facing Communities

Place Template	Tiles	Features	Default Type	Default Tag(s)
Event Planning	Key Dates Featured Content Gauge Popular Content Recent Decisions	Documents Discussions Ideas Projects Status Updates (in groups only)	Private	event
Customer, Partner, or Vendor Collaboration	Key Dates Top Participants Helpful Links Finalized Content Action Items	Videos Documents Discussions Ideas Polls Events Blogs Projects Status Updates (in groups only)	Private Externally-accessible	agency, customer, partner, vendor

Place Template	Tiles	Features	Default Type	Default Tag(s)
Campaign Planning	Top Participants Finalized Content Action Items Key Content and Places Key Dates	Videos Documents Discussions Ideas Polls Events Blogs Projects Status Updates (in groups only)	Private	assets, campaign
Customer Success Stories	Top Participants Featured Content Popular Content	Blogs Documents Status Updates (in groups only)	Open	success_stories, win

Table 19: Available in Externally-facing Communities

Place Template	Tiles	Features	Default Type	Default Tag(s)
Event Planning	Key Dates Featured Content Gauge Popular Content Recent Decisions	Documents Discussions Ideas Projects	Secret	event

Place Template	Tiles	Features	Default Type	Default Tag(s)
Customer, Partner, or Vendor Collaboration	Key Dates Top Participants Helpful Links Finalized Content Action Items	Videos Documents Discussions Ideas Polls Events Blogs Projects	Secret	partner
Customer Event	Key Dates Key Content and Places Top Participants	Events Blogs Documents Discussions	Open	—
Partner Enablement	Popular Content Key Content and Places Featured Video Featured Content Featured People	Videos Documents Discussions Ideas Polls Events Blogs Projects	Open	—

Products Place Templates
Products Place Templates include tiles for information used to launch and manage products.

Templates are organized according to the kind of workgroup that typically uses them, but you can rename and customize any template. The right template contains more or less the tiles that you need. For example, if you want to set up a place to track items identified for quick follow-up, you could pick the Sales Answer Desk template when creating the place, even if Sales isn't your main goal. This template includes a Featured People tile to identify people you can direct questions to, tracks items marked for Action and recent decisions, and surfaces popular content. For more information about data tiles and the information they're based on, see the Tile Reference.

Note: You may not see events or ideas as feature options in a template if your community does not have these additional modules enabled. In addition, externally-facing communities (those serving customers, partners, and vendors), do not have the Corporate Communications, HR, IT, or R&D, or Sales templates. Internally-facing communities (those serving employees), do not have the Customer Service, Other, or Products templates.

Place Template	Tiles	Features	Default Type	Default Tag(s)
Product Launch Planning	Top Participants Finalized Content Action Items Key Content and Places Key Dates	Videos Documents Discussions Ideas Polls Events Blogs Projects	Private	assets, campaign
Product Launch	—	Documents Discussions Blogs	Open	assets, campaign
Product and Services Feedback	Featured Content Action Items	Ideas Documents Discussions Polls Blogs	Open	feedback
Beta Testing	Featured Content Action Items Recent Decisions Top Participants	Ideas Documents Discussions Polls Blogs	Secret	—

Research and Development Templates

Research and Development Place Templates contain selections of tiles focused on innovation and collaboration R&D organizations, including FAQ and vendor collaboration.

Templates are organized according to the kind of workgroup that typically uses them, but you can rename and customize any template. The right template contains more or less the tiles that you need. For example, if you want to set up a place to track items identified for quick follow-up, you could pick the Sales Answer Desk template when creating the place, even if Sales isn't your main goal. This template includes a Featured People tile to identify people you can direct questions to, tracks items marked for Action and recent decisions, and surfaces popular content. For more information about data tiles and the information they're based on, see the Tile Reference.

Note: You may not see events or ideas as feature options in a template if your community does not have these additional modules enabled. In addition, externally-facing communities (those serving customers, partners, and vendors), do not have the Corporate Communications, HR, IT, or R&D, or Sales templates. Internally-facing communities (those serving employees), do not have the Customer Service, Other, or Products templates.

Place Template	Tiles	Features	Default Type	Default Tag(s)
Best Practices Sharing	Featured Content Popular Content Image Gallery Top Participants Key Dates	Videos Documents Discussions Ideas Polls Events Blogs Projects Status Updates (in groups only)	Open	best practice
R&D Planning	Action Items Popular Content Top Participants Recent Decisions	Videos Documents Discussions Ideas Polls Events Blogs Projects Status Updates (in groups only)	Open	development, research

Sales Place Templates

Sales Place Templates include tiles for information used to plan and close deals, including some integrations with Salesforce.com.

Templates are organized according to the kind of workgroup that typically uses them, but you can rename and customize any template. The right template contains more or less the tiles that you need. For example, if you want to set up a place to track items identified for quick follow-up, you could pick the Sales Answer Desk template when creating the place, even if Sales isn't your main goal. This template includes a Featured People tile to identify people you can direct questions to, tracks items marked for Action and recent decisions, and surfaces popular content. For more information about data tiles and the information they're based on, see the Tile Reference.

Note: You may not see events or ideas as feature options in a template if your community does not have these additional modules enabled. In addition, externally-facing communities (those serving customers, partners, and vendors), do not have the Corporate Communications, HR, IT, or R&D, or Sales templates. Internally-facing communities (those serving employees), do not have the Customer Service, Other, or Products templates.

Place Template	Tiles	Features	Default Type	Default Tag(s)
Sales Home	Popular Content Key Content and Places Featured Video Featured Content Featured People	Videos Documents Discussions Ideas Polls Events Blogs Projects Status Updates (in groups only)	Open	sales
Sales Answer Desk	Popular Content Helpful Links Featured People Action Items Recent Decisions	Videos Discussions Blogs Documents Projects	Open	questions, sales

Place Template	Tiles	Features	Default Type	Default Tag(s)
Deal Room Generic	Top Participants Popular Content Action Items Finalized Content Key Dates	Videos Documents Discussions Ideas Polls Events Blogs Projects Status Updates (in groups only)	Open	deal_room, win
RFP Workgroup	Key Dates Popular Content Finalized Content Top Participants Key Content and Places Gauge	Documents Discussions Projects Status Updates (in groups only)	Private	request_for_proposal, rfp
Competition	Featured People Top Participants Featured Content Popular Content Key Content and Places	Documents Discussions Blogs Projects Status Updates (in groups only)	Secret	competition

Place Template	Tiles	Features	Default Type	Default Tag(s)
Customer 360	Gauge Featured Content Helpful Links Featured People Key Dates	Videos Documents Discussions Ideas Polls Events Blogs Projects Status Updates (in groups only)	Open	—

Designing Place Overview Pages

You can define the content and layout of place Overview pages for which you have administrator rights.

Places (social groups, projects, and spaces) become more inviting when you customize their overview pages to display the items members care about most. Depending on your overview page customization rights, you can easily get these pages to look the way you want by using widgets that help you choose and arrange content. Each widget displays content of a particular kind — for example, HTML, recent content, or feed subscription results — in a box that you can drag into position on a page. After you publish the page, you can always come back and update its content or design. A complete reference to available widgets can be found here. The steps for customizing overview pages are here.

This topic offers a few key guidelines for designing pages with widgets. A good starting point for thinking further about designing Overview pages is this blog post in the Jive Community: Extreme Makeover: Widget Edition.

Overview Page Best Practices

- What is the purpose of your site, space, or group? Make sure the widgets you choose help users identify the purpose of the place and quickly find the information they need.
- Keep in mind that with widgets, less is more. Highly complex pages can lead to performance challenges as well as user confusion. You should use only as many widgets as you need to provide key information for the place without overloading it.
- Make sure you also limit the number of images on the page. Loading many images on every page load can make your page slower and create visual clutter.
- Limit group and space ownership to one or a very few users to safeguard your design and protect security.

Setting Up a Place's Overview Page

To begin customizing the Overview page of a place, navigate there and click **Manage** > **Overview Page**.

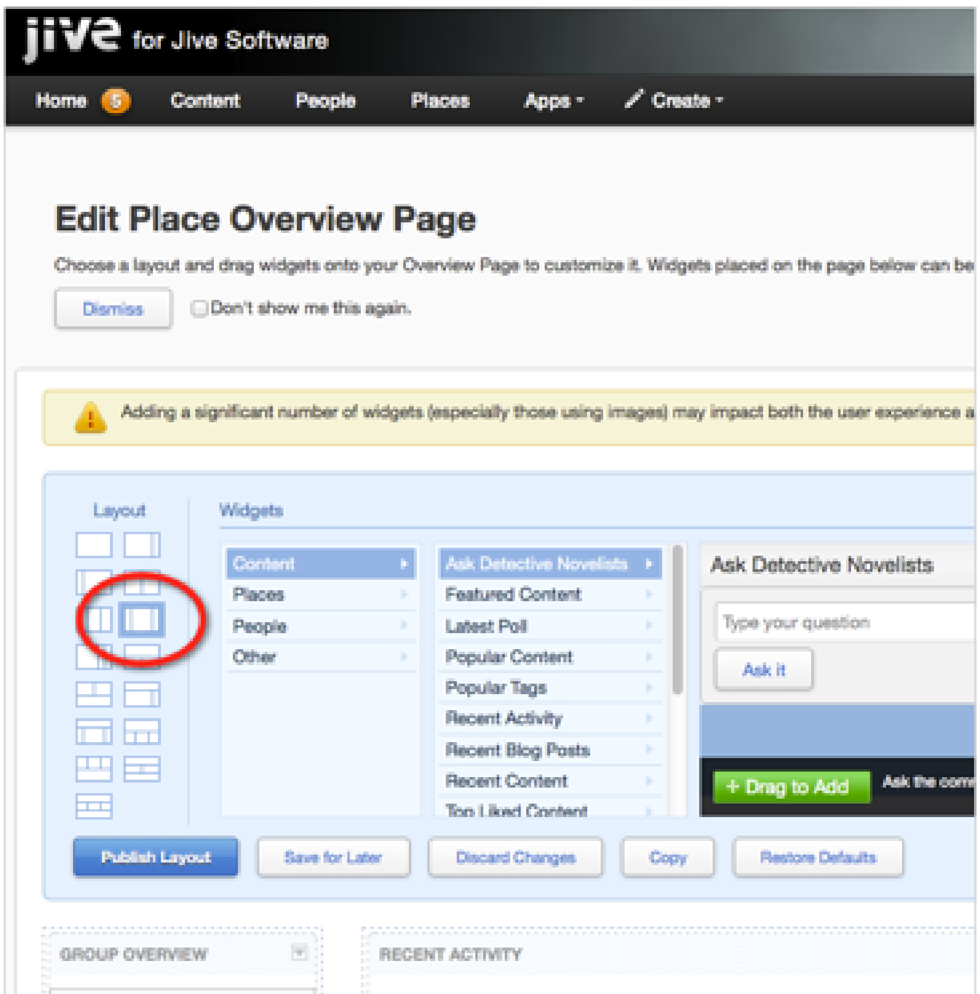
When you customize the Overview page for a place, you decide on a column view, then drag widgets into the layout. If you've chosen widgets that require further configuration, you'll then edit them to ensure the correct activity flows into them, or populate them with content.

Note: You can see the Overview page as an option in a place only if it is selected from the Advanced Options in the place's Settings (**Manage** > **Settings** > **Click the place's Name**).

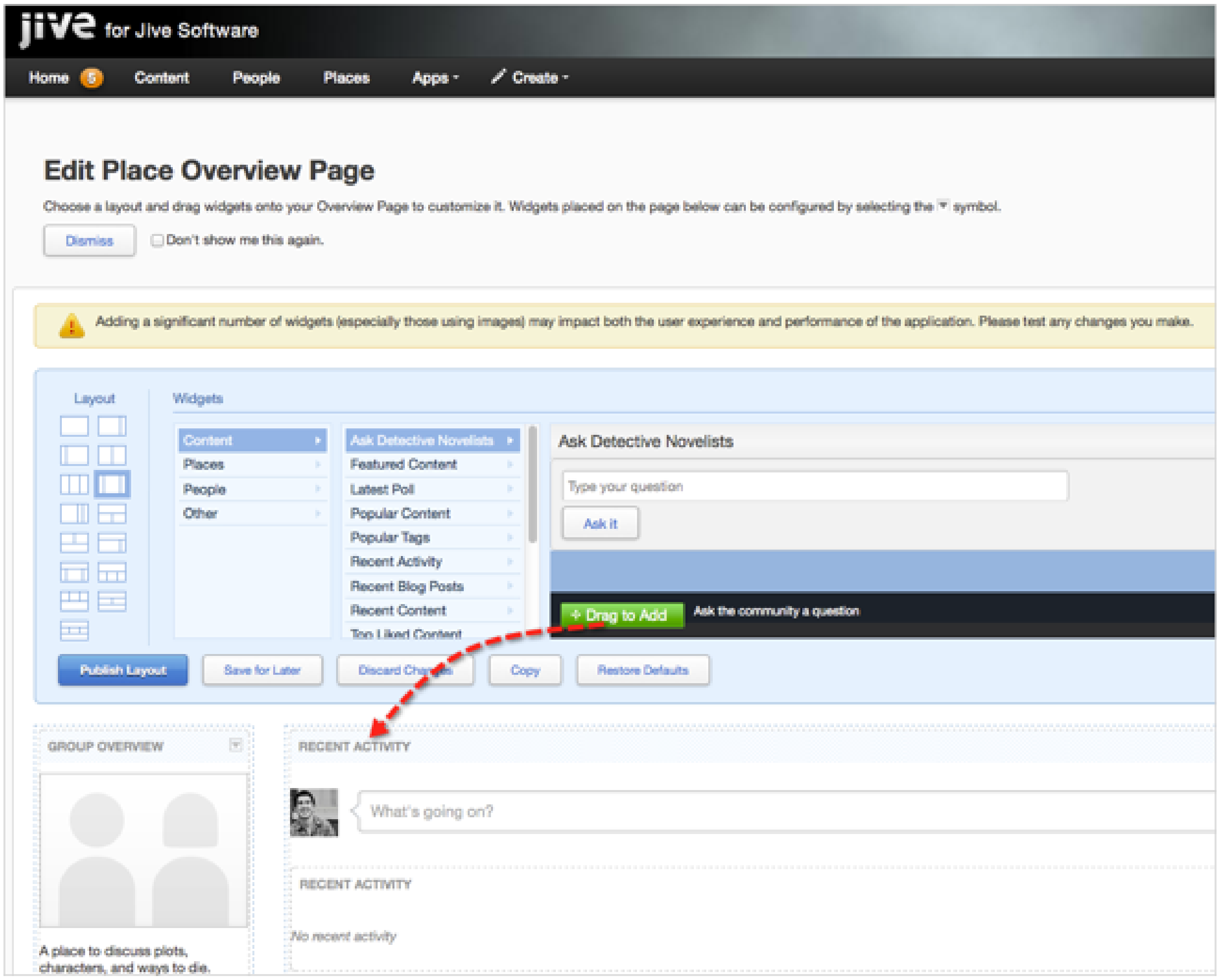
To customize the Overview page:

1. Go to the Overview page for the place you want to customize and click **Manage** > **Overview page**.

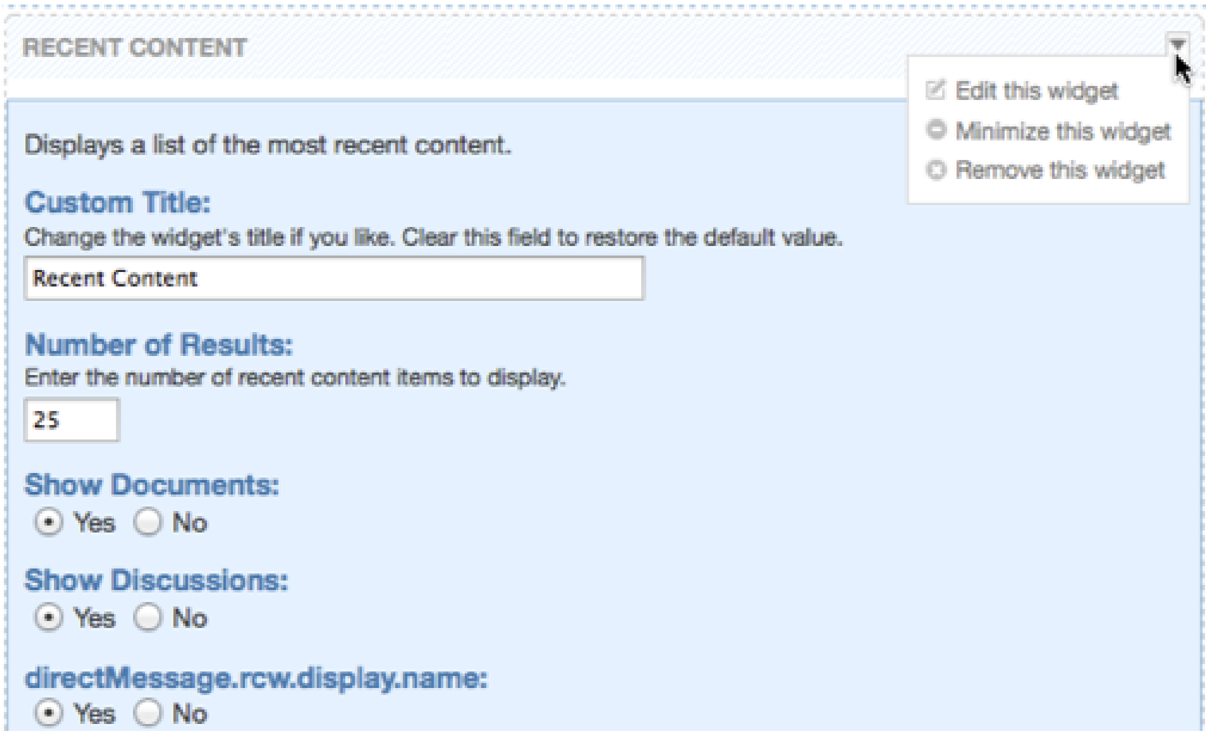
   You'll see a layout interface with the available layouts and widgets listed at the top.
2. Select a layout from the **Layout** column.



3. In the widgets list, find the widgets you want and drag them into the layout area.



4. After the widget is in the layout area, you can customize it by clicking the **Edit this widget** link (it's under the little arrow in the widget's upper right corner).



5. If you want to remove any widgets, click the **Remove this widget** link (it's under the arrow in each widget's upper right corner).
6. To save all your changes to the layout and make them visible to other users, click **Publish Layout**.

Updating Places That Have an Overview Page

Places created in an earlier version have an old-style Overview page, not a dynamic Activity page. You can easily change them to use an Activity page.

Existing places will keep their old-style Overview pages after an upgrade, but will also be assigned the **General** > **Team Collaboration** Place Template by default. However, you'll see this template only if you have set the Activity page to be displayed. If you want to keep the old Overview page and not display the Activity page, do nothing. If you want to create a new Place Template-driven Activity page, which leverages data streams and uses more performant data tiles, you can configure the Team Collaboration template to include the data you want to show, or choose a different one. See the instructions in this topic for showing and hiding the Overview and Activity Pages the way you prefer them. You can choose to show only one or both of these pages, but only one can be the default landing page (the place where visitors to the place land by default when they navigate to the place). For more about Place Templates, see Using Place Templates.

To set the visibility of the Activity Page as well as the old-style widgetized Overview Page for an existing place:

Note: If you use the checkpoint and status functionality for tracking project tasks, you may want to stick with the old-style Overview page rather than updating to the Place Template format. The widgets in the Overview page more effectively support Projects at this time.

1. Navigate to the place you own and click **Manage** > **Settings** to enter the edit view of the place.
2. Click the group name to open the Edit Group dialog.
3. Click **Advanced options** at the bottom.
4. Under **Enable**, click **Overview Page**, **Activity Page**, or **Both**. Selecting **Both** lets you show the Overview page alongside the Activity page. If you selected either **Activity Page** or **Overview Page**, that page will be the default home page, or the first page users see when they navigate to the place.
5. If you selected **Both**, you'll see an option to set the default landing page under **Set landing page**.
6. Click **OK** when you're finished. These changes won't take affect until you **Save** the changes you've made to the place.

Setting Up Image Navigation

You can configure any place's Overview page, including the community Home page, with image-based navigation to quickly direct your users to useful pages. First, you'll add the Image Navigation Widget to your place's layout, then add images and links to the widget.

Add the Image Navigation Widget to Your Place's Layout

1. Go to the place you own and click **Manage** > **Overview Page** to begin editing the place's Overview page. (If you're editing the community's Home page, you'll click your avatar in the upper right corner, and then **Manage** > **Overview Page**).
2. From the widgets list, select **Other** > **Image Navigation Widget**.
3. Drag the widget down into your layout area and drop it where you want it.
4. Click the small triangle in the upper right corner of the widget and select **Edit this widget**.
5. Change the widget's title or leave that field blank if you do not want any title.
6. Select whether you want the header and border to be displayed.
7. Click **Save Properties**.

Add Images to the Widget

After you've added the Image Navigation Widget to your place's layout, you'll add images and links to the widget, then publish the updated layout of the place.

1. Click the small triangle in the upper right corner of the Image Navigation Widget and select **Edit this widget**.
2. Click **Add a new image link**.
3. In the "Provide a Target Link" field, type in the URL that you want the image to link to.
4. Provide a caption for the image. You can use the caption Jive provides automatically, or overwrite it with your own.
5. Select the image you want to use for this link, and then click **Save**.
6. Repeat these steps until you have all the images you want to display in the widget. The limit is 8. You can move them around to change the order in which they are displayed by dragging and dropping them.
7. When you're finished, click **Publish Layout** on the editing page.

Setting Up the Search Widget

The Search widget allows your users to quickly search a specific space or group in your community, or the entire community.

1. Go to the place you own and click **Manage** > **Overview Page** to begin editing the place's Overview page. (If you're editing the community's Home page, you'll click your avatar in the upper right corner, and then **Manage** > **Overview Page**).
2. From the widgets list, select **Content** > **Search Widget**.
3. Drag the widget down into your layout area and drop it where you want it.
4. Click the small triangle in the upper right corner of the widget and select **Edit this widget**.
5. Use the title "Search Widget" or create your own, for example, "Search this Group" or "Search Me!"
6. Select the number of results to return in the search.
7. Select the place to perform the search. This can be any place in the community, or the entire community (which would be your "root" space).
8. Click **Save Properties**.
9. When you're finished making changes to your place's layout, click **Publish Layout**.

Setting Up the Ask Widget

The Ask (a place) widget allows users to quickly ask a question in a specific space or group in your community, or the entire community. After the user types a question into the Ask widget, the search function displays possible answers based on matching keywords. If the user doesn't see the correct answer in the results list, they can create a discussion right from the widget. This can be very helpful in places designed to support customers or employees.

1. Go to the place you own and click **Manage** > **Overview Page** to begin editing the place's Overview page. (If you're editing the community's Home page, you'll click your avatar in the upper right corner, and then **Manage** > **Overview Page**).
2. From the widgets list, select **Content** > **Ask (place)**.
3. Drag the widget down into your layout area and drop it where you want it.
4. Click the small triangle in the upper right corner of the widget and select **Edit this widget**.
5. Use the title "Ask (place)" or create your own, for example, "Ask Us a Question". You can also change the text that will be displayed on the actual Ask button, for example, instead of "Ask It," you might want "Submit Your Question".
6. Specify the place you want to perform the search. You can search in the current place, a single place that you specify, or all public places in the community (this would be your "root" space).
7. Select the number of results to return in the search.
8. You have some options for what will be displayed in the search results. You can select one, some, or all of these options:

Option	Description
All Questions	Displays in search results all questions that have been asked, whether or not they have been answered.
All Discussions	Displays only discussions in search results.
Answered Questions	Displays only Answered Questions in search results.
Documents	Displays only documents in search results.

9. Select the place you want questions posted to. This can be different from the place where the Ask widget is located. For example, you could put the Ask widget in an "Employee Questions" group, but post the questions to the "Employee Q&A" group.
10. Click **Save Properties**.
11. When you're finished making changes to your place's layout, click **Publish Layout**.

Setting Up the Answered Questions Widget

The Answered Questions widget allows your users to quickly see a list of questions that have been answered in a specific space or group in your community, or the entire community. Answered questions displayed in this widget are those that include a reply or comment marked as a "Correct Answer".

1. Go to the place you own and click **Manage** > **Overview Page** to begin editing the place's Overview page. (If you're editing the community's Home page, you'll click your avatar in the upper right corner, and then **Manage** > **Overview Page**).
2. From the widgets list, select **Content** > **Answered Questions**.
3. Drag the widget down into your layout area and drop it where you want it.
4. Click the small triangle in the upper right corner of the widget and select **Edit this widget**.
5. Use the title "Answered Questions" or create your own, for example, "Recently Answered".
6. Select the number of answered questions to display in the widget.
7. Select the order in which you want the answered questions to be displayed.
8. Specify the place you want to pull the answered questions from. Typically, you'll want this to be the current place, but it could be any other place in the community as well, or the entire community (this would be your "root" space).
9. Click **Save Properties**.
10. When you're finished making changes to your place's layout, click **Publish Layout**.

HTML and Formatted Text Widgets

The HTML and Formatted Text widgets are extremely flexible, but should be used carefully to ensure effective, performant pages.

The HTML and Formatted Text widgets are designed to display customized information on Overview places, including the community Home page. You can use them to embed all kinds of assets, including images. These widgets are often used to provide visual orientation or branding to the site or the place. The HTML widget also allows you to add JavaScript and CSS elements, with certain security limitations, which are described later in this topic.

Uploading Resources to a Widget

You can use the Formatted Text and HTML widgets to upload up to 10 file resources per place. (Spaces can include any kind of files: groups and projects are limited to GIF, JPEG, PNG and BMP files.) Files you upload will be stored as part of your community so you don't have to retrieve them from an external location, which can improve performance and saves you the trouble of hosting them elsewhere. You can then refer to these resources in any Formatted Text or HTML widget you have access to edit. For instructions, see Uploading Static Resources to a Widget.

> **Warning:** Keep in mind that resources you upload this way are posted on the Internet and can be viewed by anyone with access to the network. By design, they don't inherit the authentication requirements of your site or the permissions to the place where you upload them.

Managing Performance

Uploading resources is a good way to limit the performance impact of resource loading from your widgets: uploaded resources don't need to be authenticated on page load. However, you'll still want to consider user page loads when determining the number and content of widgets.

Managing HTML Widget Security

To ensure security and prevent problems that can corrupt your pages and keep them from loading, any HTML widget code that calls a `<script>` tag will be contained in an isolated iFrame. This is known as "safe mode." If you want to include CSS or other styling in the widget, you can include it in the same location as your HTML code. Isolation of the HTML widget also means that the widget can't borrow JavaScript from the Overview page, and that visual components cannot extend beyond the perimeter of the iframe. Simple HTML, JavaScript, and CSS continue to be supported.

In safe mode, you can still call the assets associated with the core Jive installation as follows:

```
<script src="/resources/scripts/jquery/jquery.js"></script> <link rel="stylesheet" href="/styles/jive.css" media="all">
```

It's possible for your site administrator to use a system property to override the default "safe mode" behavior (iFrame isolation) and allow external JavaScript access from the HTML widget. However, this approach requires caution and is not recommended. In previous versions, before the safe mode was implemented for widgets, it was possible for corrupted widget code to cause serious problems that affected the database.

Widget upload access should be limited to users you trust. Because any social group owner can upload resources to these widgets, it's possible for users to make incorrect judgments about appropriateness and security, so make sure group owners are carefully chosen.

Uploading Static Resources to a Widget

You can use the Formatted Text and HTML widgets to upload file resources into Jive, so you can link to them directly using a URL.

You can upload any kind of static file from a menu inside the Formatted Text and HTML widgets. You can also see the available uploaded resources and copy their URLs so you can use them in your widget code. You can upload up to 10 files per place.

Warning: Keep in mind that resources you upload this way are posted on the Internet and can be viewed by anyone with access to the network. By design, they don't inherit the authentication requirements of your site or the permissions to the place where you upload them.

To upload a static resource:

1. Go to any Overview page you have the rights to edit.
2. Click **Manage** > **Overview Page**
3. Under Layout, click **Widgets** > **Other** > **HTML** or **Widgets** > **Other** > **Formatted Text**.
4. Click **Manage Files**.
5. Click **Upload a File**. Keep in mind that only image files are supported in for upload in groups and projects.
   Your file will be added to the **Your uploaded files** list.
6. To copy the URL so you can use it to refer to the file in this or another widget, click **Copy to Clipboard**.
7. If you want to delete the file later, you can return to the Manage Files dialog and click the x next to a file name. Make sure you're not using the file in any widgets, because links and references to a deleted file will be broken.

Overview Page Customization Permissions

You can customize the Overview page of places. Here is a table that lists who can change what on place Overview pages.

Page	Description	Who Can Customize
Space Overview	Displayed on the Overview tab for space	An administrator for the space.
Project Overview	Displayed on the Overview tab for a project	The project's creator. Space and Group owners can edit the Projects that live in the space/group.
Group Overview	Displayed on the Overview tab for a group	All group owners.
Community Overview (Home)	Displayed on the front page of your community (if configured)	Your Community Manager.

Note: If your community is connected to another community (via what's called a "bridge"), then you might also be able to use widgets that live in the other community. Members of both the current community and the remote (or bridged) one can use remotely available widgets to enable viewing content and activity on the other community.

Available Widgets Reference

Different widgets are available in different types of pages.

The following tables show the types of widgets that can be used to customize place overview pages.

Table 20: Content Widgets

Name	Description	Used In
Answered Questions	Shows questions that have had a reply marked as the Correct Answer.	All
Ask (place)	Allows a user to ask a question while type-ahead search tries to answer it with a link to content in the place. If search does not find a match, it prompts the user to ask the question by creating a new discussion in the place.	All
Event Calendar	Displays upcoming events for the space or group in a calendar format. Note that you must have the Events plugin installed to see and use this widget.	Group Overview, Space Overview
Event View	Displays a specific event from any place. The event ID is located in the URL for the event, for example, "http://yourcommunity/version/events/1000". In this case, the ID is 1000. Note that you must have the Events plugin installed to see and use this widget.	All
Featured Content	Shows the featured content (place owners can designate content items to feature).	All
Featured Video	Shows a featured video. Note that you must have the Video plugin installed to see and use this widget.	Group Overview, Project Overview, Space Overview
Latest Poll	Shows the most recent poll created in the current place.	All
Popular Content	Shows the most liked content. Can be customized to show any combination of recent discussions, documents, polls, and/or blog posts from the current place.	All
Popular Videos	Shows the most liked videos. Note that you must have the Video plugin installed to see and use this widget.	All

Name	Description	Used In
Popular Tags	Shows the most commonly used tags in the current place.	All
Recent Activity	Displays a list of the most recent activity to show what people are doing.	All
Recent Blog Posts	Shows the first 200 characters of a specific user's blog posts, plus images from the blog.	All
Recent Content	Can be customized to show any combination of recent discussions, documents, polls, blog posts, and/or bookmarks from the current place.	All
Recent Ideas	Displays the place's recent ideas. Note that you must have the Ideation plugin installed to see and use this widget.	All
Recent Videos	Displays the place's recent videos. Note that you must have the Video plugin installed to see and use this widget.	All
Search	Allows user to search a place. Note that you can point this widget to any other place in the community, not just its containing space. For example, your Human Resources space could search the Wellness group from this widget.	All
Tagged Event	Displays the most recent event that uses a specific tag that you define. Note that you must have the Events plugin installed to see and use this widget.	All
Tasks	Displays the upcoming tasks in this project.	Project Overview
Top Ideas	Shows the top ideas in the community.	All
Top Liked Content	Shows the content with the most likes in the current place.	All
Top Rated Content	Shows the content with the highest rating in the current place.	All
Unanswered Questions	Shows discussions in the current place that have been marked as a question, but have not yet been marked Answered.	All

Name	Description	Used In
Upcoming Events	On the Home page, displays all visible upcoming events in the system. For all other places, displays the upcoming events for the place. Note that you must have the Events plugin installed to see and use this widget.	All
View Blogs	Shows blog post titles, a 200-character excerpt, or the full content of blog posts in a specified place.	All
View Document	Displays a document you select.	All
Watch a Tag	Shows community content that is tagged with the tag(s) that you specify when setting up this widget. This widget is keyed to the official Tag(s) of content; in other words, this widget does not show content with inline #hashtags or @mention text in the body of the content.	All

Table 21: Place Widgets

Name	Description	Used In
Featured Places	Shows a list of community places that you designate.	All
Groups	Shows similar groups to the current group.	All
Places	Shows the places around the community in a list view sorted by place type.	Home Page
Projects	Shows the place's associated projects.	Group Overview, Space Overview
Related Groups	Shows a list of groups similar to the current group.	Group Overview
Related Projects	Shows a list of projects similar to the current project.	Project Overview
Space Grid	Shows the sub-spaces of the current space in a grid view.	Home Page, Space Overview
Space Tree	Shows the sub-spaces of the current space in a tree view.	Home Page, Space Overview
Spaces	Shows the sub-spaces of the current space in a list view.	Home Page, Space Overview

Table 22: People Widgets

Name	Description	Used In
Featured User	Displays the selected user's profile image and basic information with an optional description.	All
Members	Shows the people who have joined the project.	Project Overview
Newest Members	Shows the people who most recently joined the community.	Home page
Recent Activity	Displays a list of the most recent activity to show what people are doing.	All
Recently Joined	Shows the people who most recently joined the group.	Group Overview
Top Participants	Show the people who created or replied to the most activity. (Note that a user's status points displayed in this widget refer to points earned in the given place only.)	All

Table 23: Other Widgets

Name	Description	Used In
Actions	Displays the Action links through which people can create content for a place.	All
Categories	Displays the administrator-defined categories for a place.	Group Overview, Project Overview, Space Overview
Checkpoints	Shows project milestones.	Project Overview
Formatted Text	Displays your text with formatting, links, and images.	All
Group Overview	Displays an image and description for the group.	Group Overview
HTML	Renders your HTML with JavaScript or even CSS. You can add custom buttons to this widget using the <button> class.	All
Image Navigation	Displays a clickable menu of images and captions linked to locations you select.	All
Project Calendar	Shows checkpoints and tasks due in coming weeks.	Project Overview

Name	Description	Used In
Project Overview	Shows the project's graphic, owner, and creation date.	Project Overview
Project Status	Shows an owner-determined status for a project.	Project Overview
Quick Tips	Displays a random quick tip about using the community.	Home page
RSS Subscription	Displays results of a feed from another part of the community or from another web site.	All
Slideshow Carousel	Embeds rich images and news content into a carousel widget.	All
Social Sharing	Allows one-click sharing of the place page in social media outlets. Note that Social Sharing must be enabled in the community by the community manager to see this widget.	All
Space Overview	Shows the space's graphic, description, tags, and creation date.	Space Overview

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:

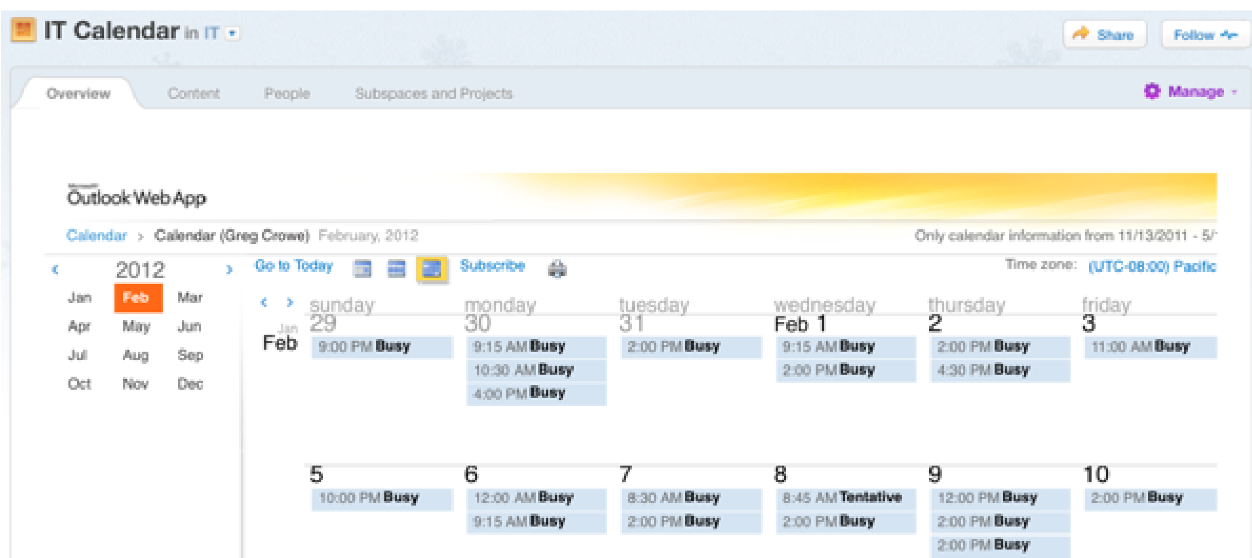
```
https://YOUR.MAIL.SERVER/owa/calendar/GUID@YOURDOMAIN.PUBLIC/
DIFFERENT_GUID/calendar.html
```

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:

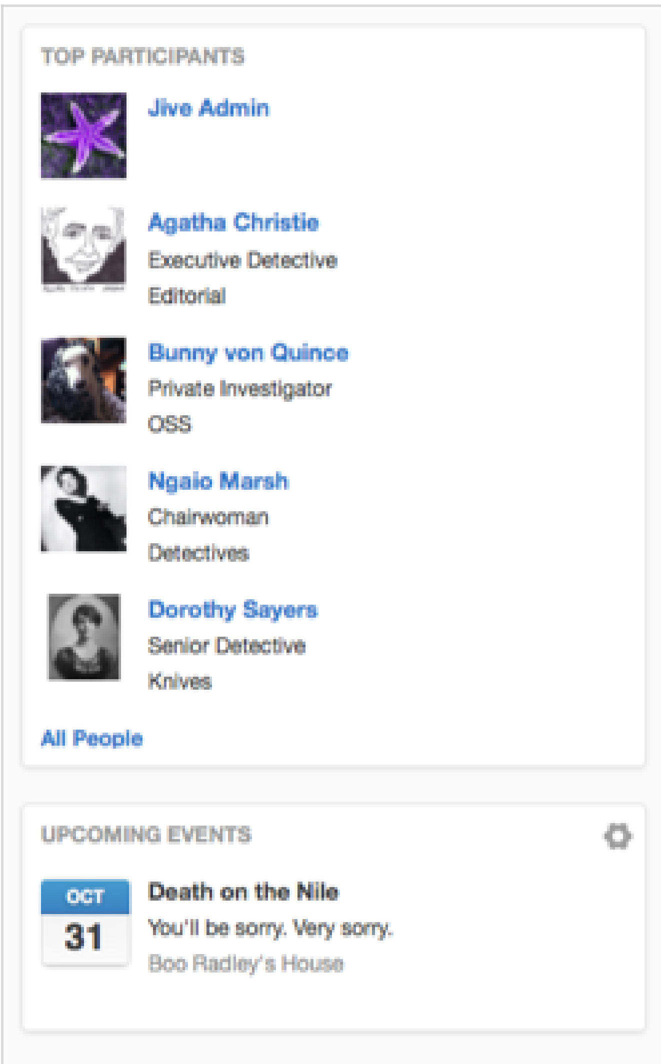


What is a Tile?

Tiles display useful information, such as Popular Content or Featured People.

You can use a tile as is or customize it to display specific information. Different tiles are available by default in different places (spaces, groups, Your View, and so on). For example, the HR Pre-Hire Collaboration place template includes the Helpful Links and Action Items tiles by default. If you own the place, you can choose not to show these default tiles, and instead select different tiles.

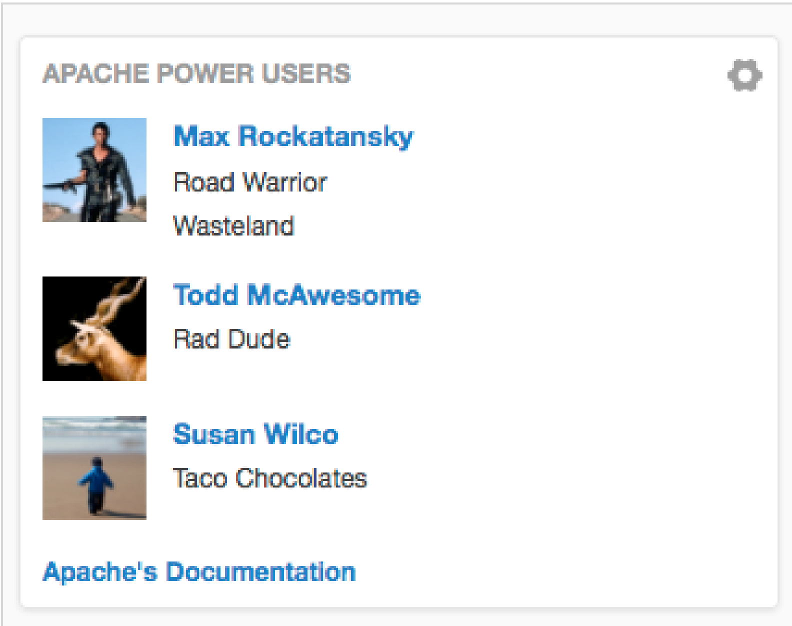
Here's an example of the Top Participants and Upcoming Events tiles:



Creating a Custom Tile

If you are a place owner, you can create custom tiles that include a list of links to helpful content, people, and places in your community, and even to links outside your community. Your custom tiles will be available to all of the places that you own. Community managers can create custom tiles and make them available to all places in the community.

A custom tile provides just the right links to content, people, or places. For example, a custom tile might be helpful for an HR group to list all of this month's new hires and include a link to the community's Onboarding group. An Engineering space might find it useful to have a list of the team's power users with a link to an external documentation site, like this:



To create a custom tile, first you'll create it, then configure it to include the links you want to feature.

Create a Custom Tile

1. Go to the place that you own and click **Manage** > **Settings** in the upper right.
2. Beneath the included default tiles on the right, click **Add a tile**.
3. Under Categories, select **Create New Tile**.
4. Choose the kind of tile you want:

Option	Description
Content/Place	Use this tile if you want to create links to specific content items and/or places in your community.
People	Use this tile if you want to create links to specific people in your community.

Configure Your Custom Tile

1. After you have created your custom tile, you'll see it immediately on your place's preview page. Click the new tile's gear icon

   to begin customizing it.

2. Give the tile a name, something that describes the tile's content, such as "Accounting Superstars" or "Engineering Docs."
3. Add the links to the content, people, or places that you want this tile to display.
4. Optionally, you can add a link to the bottom of the tile to an internal community page or an external URL.
5. Select the security type for this tile. Here are the options, which depend on your permissions (i.e., whether you're a place owner or a community manager):

Option	Description
Locked Tile	Locking the tile will make you the only person who can edit it. Other owners of the place can remove the tile from the place, but they cannot edit it. If you edit the tile, note that *all instances* of the tile (in other places that you own) will be updated. If you do not lock the tile, any changes that you or other place owners make to the tile will affect *all instances* of the tile. To paraphrase Voltaire, "With great power comes great responsibility."
Global Tile	Only users with Manage Community or Full Access permissions will see this option. All place owners in the community will be able to use this tile. If you lock the tile, all place owners will be able to use the tile but not edit it. If you do not lock the tile, all place owners will be able to edit the contents of the tile (but not its title). If other place owners edit the content of the tile, *all instances* of the tile in the community will be updated.

6. Click **Apply**.

Place Templates Tile Reference

Here's a complete list of the tiles available on the activity pages of the Place Templates. You may also see custom tiles not listed here that have been created by your community manager.

You should be able to satisfy most of your needs with the built-in tiles and the Create New Tile feature that allows you to create a custom tile. But it is also possible to develop tiles that aren't included in the product, including tiles for third-party integrations. Check out the Jive Developers' site to get started.

Note: You may not see events or tasks tiles if you have not enabled these optional features.

Table 24: Your Tiles

Tile	Description	Dependencies
Your Custom Tile Name	Any custom tiles you have created will be listed here.	You must first Create New Tile to see the Your Tiles option under Categories.

Table 25: Content Tiles

Tile	Description	Dependencies
Finalized Content	Shows content that has been marked "Final."	Relies on content being marked "Final."
Action Items	Track the content that needs follow-up action.	Relies on content being marked "Needs Action."
Recent Decisions	Shows the most recent items that were marked "Decision."	Relies on content being marked "Decision."
Featured Content	Shows content marked "Featured."	Relies on content being marked "Featured."
Document Viewer	Displays a document inside a tile.	Content added manually.
Popular Content	Shows content that's getting views and likes.	Relies on content getting viewed and liked.
Helpful Links	Build a list of key items for quick reference. Links can be internal to your community or external URLs.	Content added manually.
Key Content and Places	Displays a list of content and places that you can edit and manage yourself.	Content added manually.
Featured Video	Displays a video from anywhere on the Internet.	Content added manually.
Image Gallery	Create a slideshow of images and captions.	Content added manually.
Tagged Content	Displays content that matches specific tags.	Relies on content being tagged.
Expandable Sections	Shows links to community content under collapsible headings.	Content added manually. For more information, be sure to read Using Expandable Sections on page 244

Tile	Description	Dependencies
Content Sets	Shows community content inside a tile, in a browse sequence you design.	Content added manually. For more information, be sure to read Creating Content Sets on page 243.
Ask a Question	Find a previously asked or answered question, or ask a new one.	Content added manually.
Carousel	Link a rotating image carousel to key destinations.	Content added manually.
Answered Questions	Displays a list of questions that have been answered in the place.	Relies on discussions marked as questions that include a reply marked as the Correct Answer.
Unanswered Questions	Displays a list of questions that have not yet been answered in the place.	Relies on discussions marked as questions that do not yet have a reply marked as the Correct Answer.

Table 26: People Tiles

Tile	Description	Dependencies
Featured People	Build a list of important people for your place.	Content added manually.
Top Participants	Shows frequent contributors to the place.	Populated when activity happens in the place. Note that this tile uses the same information as the status levels in your community.

Table 27: Places Tiles

Tile	Description	Dependencies
Key Content and Places	Displays a list of content and places that you can edit and manage yourself.	Content added manually.
Similar Places	Shows places with the same tags.	Relies on content being tagged.

Table 28: Sales Tiles

Tile	Description	Dependencies
Account Details	Pull in the details of an account from Salesforce. Requires a Salesforce account.	Pull in the details of an account from Salesforce. Requires a Salesforce account.

Tile	Description	Dependencies
Opportunity Details	Pull in the details of an opportunity from Salesforce. Requires a Salesforce account.	Pull in the details of an account from Salesforce. Requires a Salesforce account.
Probability Details	View the probability details of a Salesforce opportunity in gauge format. Requires a Salesforce account.	Pull in the details of an account from Salesforce. Requires a Salesforce account.

Table 29: Other Tiles

Tile	Description	Dependencies
Key Dates	Show selected dates for your team.	Content added manually.
Gauge	Show any kind of status on a gauge.	Set manually.
Featured People	Build a list of important people for your place.	Content added manually.
Key Content and Places	Displays a list of content and places that you can edit and manage yourself.	Content added manually.
Featured Video	Display a video from anywhere on the Internet.	Content added manually.
Image Gallery	Create a slideshow with images and captions.	Content added manually.
Carousel	Link a rotating image carousel to key destinations.	Content added manually.
Upcoming Events (Added Automatically)	Events creating in your place will automatically be added to this tile.	Relies on content from the Events plugin.
Featured Video (internal)	Display a video from your community.	Content added manually.
SharePoint Links	Display SharePoint links.	You must have a connection to a SharePoint site.
SharePoint Tasks	Display SharePoint tasks.	You must have a connection to a SharePoint site.
SharePoint Calendar	Display SharePoint calendars.	You must have a connection to a SharePoint site.
SharePoint Announcements	Display SharePoint announcements.	You must have a connection to a SharePoint site.

News Page Tile Reference

Here's a complete list of the tiles available on the News page.

> To learn more about using tiles, be sure to read Using Tiles.

Table 30: Your Tiles

Tile	Description	Dependencies
Your Custom Tile Name	Any custom tiles you have created will be listed here.	You must first Create New Tile to see the Your Tiles option under Categories.

Table 31: Content Tiles

Tile	Description	Dependencies
Document Viewer	Shows a full preview of a document you choose to display.	Content added manually.
Helpful Links	Build a list of key items for quick reference. Links can be internal to your community or external URLs.	Content added manually.
Key Content and Places	Displays a list of content and places that you can edit and manage yourself.	Content added manually.
Featured Video	Shows a manually selected video from an external, non-community source.	Content added manually.
Image Gallery	Create a slideshow with images and captions.	Content added manually.
Tagged Content	Displays content that matches specific tags.	Relies on content being tagged.
Expandable Sections	Shows links to community content under collapsible headings.	Content added manually.
Latest Blog Posts	Shows the newest blog posts in your community. (You won't see this tile if your community manager has disabled blogs in your community.)	Content added manually.
Carousel	Link a rotating image carousel to key destinations.	Content added manually.
Trending Content	Shows content that's attracting views and interactions. This tile appears by default on the News page. You can remove it by clicking the garbage can icon.	Relies on an algorithm.
Ask a Question	Find a previously asked or answered question, or ask a new one.	Content added manually.

Table 32: People Tiles

Tile	Description	Dependencies
Featured People	Build a list of important people for your place.	Content added manually.
Trending People	Displays the avatars of people trending in the community. This tile appears by default on the News page. You can remove it by clicking the garbage can icon.	Relies on an algorithm.

Table 33: Places Tiles

Tile	Description	Dependencies
Similar Places	Shows places with the same tags.	Relies on content being tagged.
Key Content and Places	Displays a list of content and places that you can edit and manage yourself.	Content added manually.

Table 34: Other Tiles

Tile	Description	Dependencies
Key Dates	Show selected dates for your team.	Content added manually.
Featured People	Build a list of important people for your place.	Content added manually.
Key Content and Places	Displays a list of content and places that you can edit and manage yourself.	Content added manually.
Featured Video	Shows a manually selected video from an external, non-community source.	Content added manually.
Image Gallery	Create a slideshow with images and captions.	Content added manually.
Carousel	Link a rotating image carousel to key destinations.	Content added manually.
Featured Video (internal)	Display a video from your community.	Content added manually.

Your View Tile Reference

Here's a complete list of the tiles available in Your View.

Table 35: Content Tiles

Tile	Description	Dependencies
Document Viewer	Shows a full preview of a document you choose to display.	Content added manually.
Featured Video	Shows a manually selected video from an external, non-community source.	Content added manually.
Expandable Sections	Shows links to community content under collapsible headings.	Content added manually.
Latest Blog Posts	Shows the newest blog posts in your community. (You won't see this tile if your community manager has disabled blogs in your community.)	Content added manually.
Trending Content	Shows content that's attracting views and interactions.	Relies on an algorithm.
Frequently Viewed	Shows the people, places, and content you visit most.	Relies on an algorithm.
Recently Viewed	Shows the people, places, and content you viewed recently.	Relies on an algorithm.

Table 36: People Tiles

Tile	Description	Dependencies
Frequently Viewed	Shows the people, places, and content you visit most.	Relies on an algorithm.
Recently Viewed	Shows the people, places, and content you viewed recently.	Relies on an algorithm.

Table 37: Places Tiles

Tile	Description	Dependencies
Frequently Viewed	Shows the people, places, and content you visit most.	Relies on an algorithm.
Recently Viewed	Shows the people, places, and content you viewed recently.	Relies on an algorithm.

Table 38: Other Tiles

Tile	Description	Dependencies
Featured Video	Shows a manually selected video from an external, non-community source.	Content added manually.

Setting Up the Questions Tiles

The Answered Question and Unanswered Questions tiles can be very useful in places where people ask questions and look for answers. These tiles help place visitors see at a glance what's been asked and answered.

The Answered Questions tile lists the place's recently answered questions (i.e., discussions marked as questions that include a reply marked as the Correct Answer). This tile can be helpful in places where people go to find answers, such as a Customer Support group or IT space. The Answered Questions tile also helps users understand that the place is active and effective -- questions are being asked and answered.

The Unanswered Questions tile is helpful for encouraging users to answer questions they see listed in the tile. You might also use the Unanswered Questions tile to determine upcoming work projects. For example, the manager of an accounting space might use the unanswered questions tile for project planning.

1. Go to the place that you own and click **Manage** > **Settings**.
2. In the editing interface, click **Add a tile**.
3. Under Content, select either the Answered Questions or Unanswered Questions tile.
4. If you don't want to use the default title of the tile, go ahead and change it. For example, in your place it might be more appropriate to call the tile "Correct Answers" or "Answered! Right On!"
5. Select whether you want the **newest** or **oldest** questions to display first in the list.
6. When you're finished configuring the tile, click **Save**. And don't forget to also **Save** your changes to the place.

Creating Content Sets

The Content Sets tile creates a browse sequence for key content on a custom Page in a place. It can connect any combination of content, as long as it's inside the place.

Using the Content Sets tile, you can create a named set of content inside a place. This content will be displayed in a linked browse sequence that indicates the order of reading. Content sets can include any kind of content that resides in the place where you're creating the set. Content sets are a powerful way to link and organize content within a place. For example, if you want to create a short guide that steps someone through a conceptual background, procedure, or other subject that requires a specific order, you can bring together documents, discussions, and status updates in a single presentation. Content sets are available only from a custom Page in a place. If you navigate to the same piece of content in a different way, for example if you find a document in a set by searching, you won't see it in the context of the set.

Building a Content Set

To begin creating a content set, you need to first make sure the content you want to include exists in the place where you're creating the set. If you're an administrator of the place, you can then add the Content Sets tile while adding or editing a custom page.

Removing Content in a Content Set

You can remove an item from a set by editing the content set, but deleting the content or moving it into a different place will also remove the content page from the set. If you delete all the content items in a section of a content set, the section will also be removed.

Content Sets or Expandable Sections?

When you configure them, the Content Sets tile looks very similar to the Expandable Sections navigation tile, which also shows a collapsible view of content links with descriptions and section headings. However, the Content Sets tile is designed as a portal for reading a group of linked items in sequence, while Expanded Sections presents an organized set of quick links from around the community. The two tiles have the following important differences:

	Content Sets	Expandable Sections
Content Source	Only content posted in the Place where the tile is.	Anywhere in the community, including personal or private content.
Navigation	Move from page to page in the set without leaving the content group or returning to the tile page.	One-way click-through from the tile page to each page in the set.
Location(s)	Custom pages and Activity pages.	Your View, custom pages, and Activity pages.

Using Expandable Sections

The Expandable Sections tile lets you create a collapsible list of content links inside a tile on a Place page, an Activity page, or your Your View page.

Using the Expandable Sections tile, you can organize content from around the community in an annotated list with headings. Your presentation of linked content will be displayed inside the tile. (Website developers sometimes call this presentation an "accordion.") Expandable Sections can include any content you can see, so you can include content in private or secret groups. (This makes the tile more useful in Your View.) Keep in mind that people who don't have access to the linked content won't see the links. They also won't see any sections that only contain links to content they can't see.

Removing Content

You can remove an item by editing the tile, but deleting the content will also remove the content page from the tile. If you delete all the content items in a section of a content set, the section will also be removed.

Content Sets or Expandable Sections?

When you configure them, the Content Sets tile looks very similar to the Expandable Sections navigation tile, which also shows a collapsible view of content links with descriptions and section headings. However, the Content Sets tile is designed as a portal for reading a group of linked items in sequence, while Expanded Sections presents an organized set of quick links from around the community. The two tiles have the following important differences:

	Content Sets	**Expandable Sections**
Content Source	Only content posted in the Place where the tile is.	Anywhere in the community, including personal or private content.
Navigation	Move from page to page in the set without leaving the content group or returning to the tile page.	One-way click-through from the tile page to each page in the set.
Location(s)	Custom pages and Activity pages.	Your View, custom pages, and Activity pages.

Managing Place Categories

You can create a list of categories for describing places. These categories can be used as a filter when browsing places.

Fastpath: Admin Console: System > Settings > Place Categories

Place categories provide a useful way for community managers to classify places, so users have an easier time finding them when searching and browsing. These categories are created in the Admin Console, and can then be applied to any place in the Create workflow or by clicking About in the banner while editing a place's settings. The Place categories are different from the categories used to classify content *inside* places (see Managing Content Categories on page 259). Up to 12 categories can be defined in your community.

To manage place categories:

1. In the Admin Console, go to **System** > **Settings** > **Place Categories**.
2. Create a list of categories by clicking **Add a category**, typing a category name in the field, and clicking **Save**.
3. If you want to hide a category from users who are creating and editing places, click **Hide**. Hiding a category also makes it invisible when browsing by category. If you choose to show the category later, it will become visible again in all these locations.
4. If you want to delete a category from the list permanently, click **Delete**.
5. When your list of categories is the way you want it, click **Save** to apply your changes.

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 the layout of a space's landing page. For more information, see Using Place Templates.
- 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 your community is create spaces and sub-spaces in a hierarchy that reflect your organization'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, such as Human Resources and Marketing.

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 Sales space for the Sales department, and 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.
- 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 drop-down lists) that display the names of all the spaces.

Changing the Name of the Root Space

You can change the name and description for the root space from the Admin Console. By default, the root space is named "Jive".

Fastpath: Admin Console > **System** > **Settings** > **Space**

Space Creation Options

Creating a space starts with clicking **Space** in the Create menu, but it helps to understand the options that can help your space do what you want it to.

I want to. . .	You should. . .	Can I change this later?
Design a landing page that's optimized for a specific work purpose.	Choose **Activity + Pages** or **Activity + Overview** from the Advanced Options during the initial setup, then choose and configure a Place Template customized for the kind of work you want to do. See Place Template Reference on page 201. Place Templates only apply to Activity pages, and not to Overview pages.	Yes, but if you start with Activity + Pages and change the setting later so Overview is enabled, any custom pages you created will be invisible.

I want to. . .	You should. . .	Can I change this later?
Design a landing page with widgets (but no additional pages)	Choose **Overview** or **Activity + Overview** from the Advanced Options during setup, and fill out a widget layout under **Manage** > **Overview Page** from the group page.	Yes.
Make more custom pages in the place for displaying information, not just a landing page.	Choose **Activity + Pages** from the Advanced Options during your setup, and then add the pages to your place afterward. See Adding a Custom Page to a Place on page 197.	Yes, but if you change the setting later so Overview is enabled, any custom pages you created will be invisible.
Integrate external streams from Facebook, Chatter, or any other apps your community admin has enabled.	Choose **Activity + Pages** or **Activity + Overview** from the Advanced Options during the initial setup, then click **Add a stream integration** when configuring the Activity page.	Yes, but keep in mind that some external stream types cannot be disconnected from the group except via a Support call.
Limit the kinds of content that can be included in this place.	During place setup, after you preview the group, edit the Features and Activity settings.	Yes.
Store this place's binary documents outside Jive, for example in Box or SharePoint.	During place setup, after you preview the topic, edit the Features and Activity settings. You'll only see options other than "No external storage" if your community admin has enabled another external storage type. See Groups with Box Storage.	Yes, but if the place is later disconnected from external storage, users will see references to documents that they can't access from Jive anymore.
Make sure people can find the place.	Add tags and/or categories in the About settings of your place.	Yes. Just remove the tags or categories.

Creating A New Space from the Admin Console

Creating several spaces quickly is easy from the Admin Console. You can apply place templates to them later from the user interface.

Fastpath: Admin Console > **Spaces** > **Management** > **Summary**

1. To create a new space, click the name of the space that will contain it, then click **New**.

2. Enter the space name to appear in the user interface.
3. Enter a description 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 the content types you want the space to support.
7. Click **Create**.

For information about using place templates, be sure to read Using Place Templates.

Creating A New Space from the User Interface

You can create spaces from the user interface or from the Admin Console. If you want to associate a place template with a space, you'll need to do that from the end user interface.

Note: Creating several spaces quickly is easier from the Admin Console; you can apply place templates to the Activity page for each space later, or create Overview pages for them if you choose. Tile Pages Versus Widget Pages on page 196.

1. In the user interface, click

   >

   Space and then type and select the place where you want to create the space. (If you want to create a sub-space, go to the parent space and click **Create a sub-space** in the Actions menu.)
2. In the Create Space window, enter the space name to appear in the user interface.
3. Enter a brief description to appear in the user interface. For example, a Marketing space might say "A home for all of our marketing teams."
4. Select tags that will often be used in this space. For example, a Sales space might use the following tags: RFPs, sales_videos, wins, and so on.
5. If you click through without selecting **Advanced Options**, your place will use an Activity page as its main page, with the option to add more custom pages. *We recommend using an Activity page because it can be displayed on mobile devices, and because it's more friendly to streaming content.* However, you may want to include an Overview page with widgets. You do this by clicking **Advanced Options** and choosing one of the two options that include an Overview page. If you select **Activity + Overview Page**, you'll need to specify which page will be the landing page for the place.
6. If you want to apply a customized place template to this place, click **Preview and browse templates**. If you don't choose a template, just click **Preview**: the space will use the default template, Team Collaboration. Place templates determine which tiles and streams will be included in your space's Activity page (which you can further customize). Choose the one that's right for the kind of collaboration that will happen in the place you're creating. You might want to read more about Using Place Templates.
7. Click **Banner Design** or **Place Image** in the banner to choose the colors or images for your place header. Banner Design controls the banner's background: Place Image is a small inset image displayed inside the banner. If you don't configure them, you'll get a generic background and a placeholder image.

8. When you're finished customizing the space, click **Create Space**.
9. Later, if you want to further customize the space, just click **Manage** in the banner.

Arranging Spaces

You can view and arrange the list of spaces in the Admin Console. You can also create spaces or edit their settings.

Fastpath: Admin Console > **Spaces** > **Management** > **Summary**

Drag a space up and down to reorder the list.

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).

1. Click **New** to create a space inside (hierarchically) the space you've currently selected.
2. Click **Edit** to edit the space's properties (see Setting Space Name, Locale, and Allowed Content Types).
3. 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**.
4. 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.

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 its display name, which is the name used in URLs that link to the space.

Fastpath: Admin Console > **Spaces** > **Settings** > **Space Settings**

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 behaviors. For more on how the locale is chosen for display to the user, see Locale 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).

Setting a Space's Allowed Content Types

You can set which content types a space supports, for example, discussions, videos, ideas, and so on.

Fastpath: Admin Console > **Spaces** > **Settings** > **Space Settings**

Spaces can support a variety of content types, which you can configure. For example, by clearing the Documents check box, you'll remove the Create > Document link from the space's Actions list. In addition, users won't be able to select that space from the place picker before posting a new document.

Caution: If users have created documents in the space already, 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).

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.

Fastpath: Admin Console > **Spaces** > **Settings** > **Document Settings**

Note: A space approver only approves documents in a space. If you want to control more than documents, use the moderation feature. To learn more about that, see the Moderation section.

Setting Space Approvers

To set space approvers, type the approver's 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

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 **Inbox**.
4. By clicking on the document from the Inbox, 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.
5. The author can edit and resubmit the document.

Note that a document can also have document-level approvers designated by the author when creating the document. To learn more about that, see Document Approval. All approvers must approve before the 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.

To set the threshold after which the offending content should be hidden until it can be reviewed by the moderator, 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.

Caution: Cloud instances do not have the Full Access role. Therefore, be sure that you assign more than one person to the Global Moderator role.

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 Moderator; if there is none assigned, it then looks for a Full Access moderator. To understand where you set these roles, see Moderator Roles and Where to Set Them. Click on an image to enlarge it.

Abuse Rules and Notification Hierarchy for Contained Content Types

<table>
<tr><th></th><th></th><th colspan="8">Content Types</th></tr>
<tr><th></th><th></th><th>Announcements</th><th>Polls</th><th>Documents</th><th>Discussions</th><th>Blog Posts</th><th>Videos</th><th>Ideas</th><th>Status Updates</th></tr>
<tr><td rowspan="6">Containers</td><td>Root Container</td><td>Content Type Not Available Here</td><td>1. Global Moderator → 2. Full Access</td><td colspan="2">Content Type Not Available Here</td><td>1. Global Moderator → 2. Full Access</td><td colspan="2">Content Type Not Available Here</td><td>1. Global Moderator → 2. Full Access</td></tr>
<tr><td>Open and Member Social Groups</td><td>Content Type Not Available Here</td><td colspan="6">1. Global Moderator → 2. Full Access</td><td>Content Type Not Available Here</td></tr>
<tr><td>Private and Secret Social Groups</td><td>Content Type Not Available Here</td><td colspan="6">1. Full Access</td><td>Content Type Not Available Here</td></tr>
<tr><td>Space and Sub-spaces</td><td>Content Type Not Available Here</td><td colspan="6">1. Space Moderator → 2. Global Moderator → 3. Full Access</td><td>Content Type Not Available Here</td></tr>
<tr><td>Projects</td><td>Content Type Not Available Here</td><td colspan="6">1. Space Moderator → 2. Global Moderator → 3. Full Access</td><td>1. Global Moderator → 2. Full Access</td></tr>
<tr><td>Your Personal Content</td><td>Content Type Not Available Here</td><td colspan="3">If visibility = All, then 1. Global Moderator → 2. Full Access, otherwise 1. Full Access</td><td>1. Global Moderator → 2. Full Access</td><td colspan="2">If visibility = All, then 1. Global Moderator → 2. Full Access, otherwise 1. Full Access</td><td>Content Type Not Available Here</td></tr>
</table>

Abuse Rules and Notification Hierarchy for Content Comments

<table>
<tr><th></th><th></th><th colspan="7">Content Types</th></tr>
<tr><th></th><th></th><th>Poll Comments</th><th>Document Comments</th><th>Discussion Replies</th><th>Blog Comments</th><th>Video Comments</th><th>Idea Comments</th><th>Status Comments</th></tr>
<tr><td rowspan="6">Containers</td><td>Root Container</td><td colspan="7">1. Global Moderator → 2. Full Access</td></tr>
<tr><td>Open and Member Social Groups</td><td colspan="7">1. Global Moderator → 2. Full Access</td></tr>
<tr><td>Private and Secret Social Groups</td><td colspan="7">1. Full Access</td></tr>
<tr><td>Spaces and Sub-spaces</td><td colspan="6">1. Space Moderator → 2. Global Moderator → 3. Full Access</td><td>Content Type Not Available Here</td></tr>
<tr><td>Projects</td><td colspan="6">1. Space Moderator → 2. Global Moderator → 3. Full Access</td><td>1. Global Moderator → 2. Full Access</td></tr>
<tr><td>Your Personal Content</td><td colspan="3">If visibility = All, then 1. Global Moderator → 2. Full Access, otherwise 1. Full Access</td><td>1. Global Moderator → 2. Full Access</td><td colspan="2">If visibility = All, then 1. Global Moderator → 2. Full Access, otherwise 1. Full Access</td><td>Content Type Not Available Here</td></tr>
</table>

Abuse for Contained Content Types

Abuse Rules and Notification Hierarchy for Contained Content Types

Containers		*Content Types*							
		Announcements	**Polls**	**Documents**	**Discussions**	**Blog Posts**	**Videos**	**Ideas**	**Status Updates**
	Root Container	Content Type Not Available Here	1. Global Moderator → 2. Full Access	Content Type Not Available Here		1. Global Moderator → 2. Full Access	Content Type Not Available Here		1. Global Moderator → 2. Full Access
	Open and Member Social Groups	Content Type Not Available Here	1. Global Moderator → 2. Full Access						Content Type Not Available Here
	Private and Secret Social Groups	Content Type Not Available Here	1. Full Access						Content Type Not Available Here
	Space and Sub-spaces	Content Type Not Available Here	1. Space Moderator → 2. Global Moderator → 3. Full Access						Content Type Not Available Here
	Projects	Content Type Not Available Here	1. Space Moderator → 2. Global Moderator → 3. Full Access						1. Global Moderator → 2. Full Access
	Your Personal Content	Content Type Not Available Here	If visibility = All, then 1. Global Moderator → 2. Full Access, otherwise 1. Full Access			1. Global Moderator → 2. Full Access	If visibility = All, then 1. Global Moderator → 2. Full Access, otherwise 1. Full Access		Content Type Not Available Here

Abuse for Comments on Content

Abuse Rules and Notification Hierarchy for Content Comments

Containers		*Content Types*						
		Poll Comments	**Document Comments**	**Discussion Replies**	**Blog Comments**	**Video Comments**	**Idea Comments**	**Status Comments**
	Root Container	1. Global Moderator → 2. Full Access						
	Open and Member Social Groups	1. Global Moderator → 2. Full Access						
	Private and Secret Social Groups	1. Full Access						
	Spaces and Sub-spaces	1. Space Moderator → 2. Global Moderator → 3. Full Access						Content Type Not Available Here
	Projects	1. Space Moderator → 2. Global Moderator → 3. Full Access						1. Global Moderator → 2. Full Access
	Your Personal Content	If visibility = All, then 1. Global Moderator → 2. Full Access, otherwise 1. Full Access			1. Global Moderator → 2. Full Access	If visibility = All, then 1. Global Moderator → 2. Full Access, otherwise 1. Full Access		Content Type Not Available Here

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: Admin Console > **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 hierarchically), 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

Space administrators 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.

Moderators have the ability to edit and delete discussions in a space. To learn more about moderation, be sure to read the Moderation section.

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.
- 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 Content Categories

Categories are words or phrases an administrator provides for users to classify content in a place. (You can also assign categories to classify places themselves—see Managing Place Categories on page 245.) As an administrator, you define categories in a way that's meaningful *inside* the 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 to label content in the place will see the category's name highlighted. This is a cue to consider assigning the content to the category.

By managing the list of categories, you can help ensure that content is organized in the best way for people using the place. Spaces categories can be managed in the Admin Console, but groups and project categories are created by accessing **Manage** > **Categories**.

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.

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 permission 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, 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.

Default Permissions for Content Items

Here is a reference of the default permissions for content items.

Table 39: Internally-facing Communities

Content Item	All Registered Users Can:
Discussions	View Create Comment
Documents, Blog Posts, Events, Ideas, Polls, and Videos	View Create Comment
Avatars	Create up to 5
Profile Images	View Edit Create up to 10
User Profile Fields	Edit and View all fields except Mobile phone number *Mobile phone number: Edit and View, but Only Connections can view this by default.

Overview of Permissions by Place

Permissions are different depending on the place you assign them -- for example, in a space, blog, or social group.

System Administration

These permissions allow users administrative and moderation permissions to system-wide settings. Most of the permission levels available here provide access to the Admin Console. With the exception of the Full Access permission level, these don't provide access to content. You can't break out the bundled permissions in the administrative area (as you can with space permissions).

Spaces

These permissions allow users administrative or content moderation permissions in a space. Projects contained by a space inherit the permissions of their container space.

Blogs (global)	These permissions allow users to view, create, and comment on global blogs, such as system 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.
Social Groups	These permissions allow users to view and create social groups. Projects contained by a group inherit the permissions of their container group.
Home Page	These permissions allow users to create and interact with content that can appear on the community's home page and in the user container, including announcements, polls, and videos.

Overview of Assigning Permissions

When assigning permissions, you'll follow these basic steps.

While you can assign permissions to individuals, you'll most likely need to assign the same permissions to several users in the form of a user group. Each user group you create can represent a different category of people, from a permissions perspective. For example, 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 and its features.

1. Create user groups.
2. Add user groups to the different areas: system administration, spaces, social groups, blogs, and home page. For each user group you add, assign permissions for their access level.
3. Assign permissions in one of the following ways:
   a) **Assign a permission level.** Note that administrative permissions and spaces have several bundled permissions levels. You can also create custom space permission levels.
   b) **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 fine-grained options.
   c) **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.

Setting Permissions

You set permissions in the Admin Console to grant various levels of access to individuals or groups of users you define.

1. On the permissions 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.

Defining User Groups

You can define a set of users to quickly assign them a variety of permissions.

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 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: 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

The user groups that you set up will reflect your community's structure. There could be relatively few user groups, with separate groups for those who manage, moderate, and administer the community. Or there could be many, with groups representing departments in your organization, people with specific privileges (such as blogging), virtual teams within the organization, and so on.

Creating User Overrides

You can create user-by-user exceptions to permissions rules you've set up by creating user overrides. When you create a user override, you might be further limiting a user's access, but you could also be broadening it, for example, to add administrative abilities to the user.

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 a place, but isn't (and shouldn't be) a member of a permissions user group to which you've already assigned permissions for the place.
- A person is a member of a permissions user group to which you've assigned permissions for a place, but the person requires a different set of permissions than those received as a member of the place -- in other words, the person is an exception to the rule. For example, you might want to separately define the person's permissions to enhance or limit their access in the place.

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 user's name when you see it show up.
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

Use the System Administration permission levels to give users different kinds of control over administrative features in the application. Here are the System Administration permission levels you can assign, and what they will enable users to do.

Note: You can only use the following standard permission levels for System Administration permissions.

Full Access	This permission level allows 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	This permission level allows control over all technical aspects of the Admin Console. However, 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.
Manage Community	This permission level allows similar access as Manage System, plus the ability to create and manage spaces, space permissions, and system announcements. Users with this permission level can also view all space content, regardless of permissions, but they cannot view private groups and messages, nor personal container content.
Moderate Content	This permission level allows the user(s) to moderate social group content as well as perform global moderation duties across all spaces. This level does not enable Admin Console access. When this level is granted to a user group, all moderated content will pass through their queue before it appears in the community. For more about moderation, be sure to read the Moderation section.
Manage Users	This permission level allows the user(s) to manage the users of the application. For more about this, see Managing User Accounts and User Groups.
Manage Groups	This permission level allows the user(s) to create and manage user groups, such as for assigning permissions. For more about this, see Managing User Accounts and User Groups.

Manage News Streams	This permission level allows the user(s) to manage the News page, including creating and managing news streams for users and creating and configuring tiles on the News page.

How Admin Permission Levels Affect Your Access

Administrative permission levels control access to the Admin Console. The following tables list the sections of the console visible to users with different permission levels.

For example, a user who has been assigned the "Manage Users" permission level wouldn't typically need access to system-related areas of the Admin Console other than those for managing user accounts.

Note: You may not see all Admin Console sections and pages, depending on which optional modules you have installed in your community.

Note: Users with only Manage News Streams permissions cannot see the Admin Console.

Table 1. Overview Section

Console Page	Full Access	Manage Community	Manage System	Moderate Content	Manage Users	Manage Groups
Overview	✔	✔	✔	⊘	✔	✔

Table 2. System Section

Console Page	Full Access	Manage Community	Manage System	Moderate Content	Manage Users	Manage Groups
Management (all pages)	✔	✔	✔	⊘	⊘	⊘
Settings (all pages)	✔	✔	✔	⊘	⊘	⊘
Search	✔	✔	✔	⊘	✔	⊘
Spell Check	✔	✔	✔	⊘	✔	⊘
Plugins (all pages)	✔	✔	✔	⊘	⊘	⊘
Moderation						
Moderation Configuration	✔	✔	✔	⊘	✔	⊘
Config Spam Prevention	✔	✔	✔	⊘	⊘	⊘
Spam Link Domain WL	✔	✔	✔	⊘	⊘	⊘

Table 3. Spaces Section

Console Page	Full Access	Manage Community	Manage System	Moderate Content	Manage Users	Manage Groups
Management (all pages)	✔	✔	⊘	⊘	⊘	⊘
Settings (all pages)	✔	✔	⊘	⊘	⊘	⊘

Table 4. Blogs Section

Console Page	Full Access	Manage Community	Manage System	Moderate Content	Manage Users	Manage Groups
Management (all pages)	✔	✔	✔	⊘	⊘	⊘
Settings (all pages)	✔	✔	✔	⊘	⊘	⊘

Table 5. People Section

Console Page	**Full Access**	**Manage Community**	**Manage System**	**Moderate Content**	**Manage Users**	**Manage Groups**
Management						
User Search	✔	✔	✔	⊘	✔	✔
Create User	✔	✔	✔	⊘	✔	⊘
Group Summary	✔	✔	✔	⊘	⊘	✔
Create Group	✔	✔	✔	⊘	⊘	✔
User Relationships	✔	✔	✔	⊘	✔	⊘
Org Chart	✔	✔	✔	⊘	✔	⊘
Settings						
Avatar Settings	✔	✔	✔	⊘	⊘	⊘
Ban Settings	✔	✔	✔	⊘	✔	⊘
Delegated Authentication	✔	✔	⊘	⊘	⊘	⊘
Directory Server Settings	✔	✔	✔	⊘	⊘	⊘
Forgot Username	✔	✔	✔	⊘	⊘	⊘
Login Security	✔	✔	✔	⊘	⊘	⊘
Org Chart Settings	✔	✔	✔	⊘	⊘	⊘
Password Reset	✔	✔	✔	⊘	⊘	⊘
Profile Image Moderation	✔	✔	✔	⊘	⊘	⊘
Profile Settings	✔	✔	✔	⊘	✔	⊘
Registration Settings	✔	✔	✔	⊘	⊘	⊘
Single Sign On	✔	✔	✔	⊘	⊘	⊘
Status Level Settings	✔	✔	✔	⊘	⊘	⊘
Terms and Conditions	✔	✔	✔	⊘	⊘	⊘
User Status Update Settings	✔	✔	✔	⊘	⊘	⊘

Table 6. Permissions Section

Console Page	**Full Access**	**Manage Community**	**Manage System**	**Moderate Content**	**Manage Users**	**Manage Groups**
Permissions (all pages)	✔	✔	✔	⊘	⊘	⊘

Table 7. Add-ons Section

Console Page	Full Access	Manage Community	Manage System	Moderate Content	Manage Users	Manage Groups
Add-ons (all pages)	✔	✔	✔	⊘	⊘	⊘

Table 8. Jive Present Section

Console Page	Full Access	Manage Community	Manage System	Moderate Content	Manage Users	Manage Groups
Jive Present (all pages)	✔	✔	✔	⊘	⊘	⊘

Table 9. Ideas Section

Console Page	Full Access	Manage Community	Manage System	Moderate Content	Manage Users	Manage Groups
Ideas (all pages)	✔	✔	✔	⊘	⊘	⊘

Table 10. Events Section

Console Page	Full Access	Manage Community	Manage System	Moderate Content	Manage Users	Manage Groups
General	✔	✔	✔	⊘	⊘	⊘

Table 11. Mobile Section

Console Page	Full Access	Manage Community	Manage System	Moderate Content	Manage Users	Manage Groups
Mobile (all pages)	✔	✔	✔	⊘	⊘	⊘

Table 12. Video Section

Console Page	Full Access	Manage Community	Manage System	Moderate Content	Manage Users	Manage Groups
Preferences	✔	✔	✔	⊘	⊘	⊘

Setting Administrative Permissions for User Groups

You can assign groups of users system administrator permissions.

Fastpath: Admin Console > **Permissions** > **System Administration**

1. 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.
2. 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.

3. 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

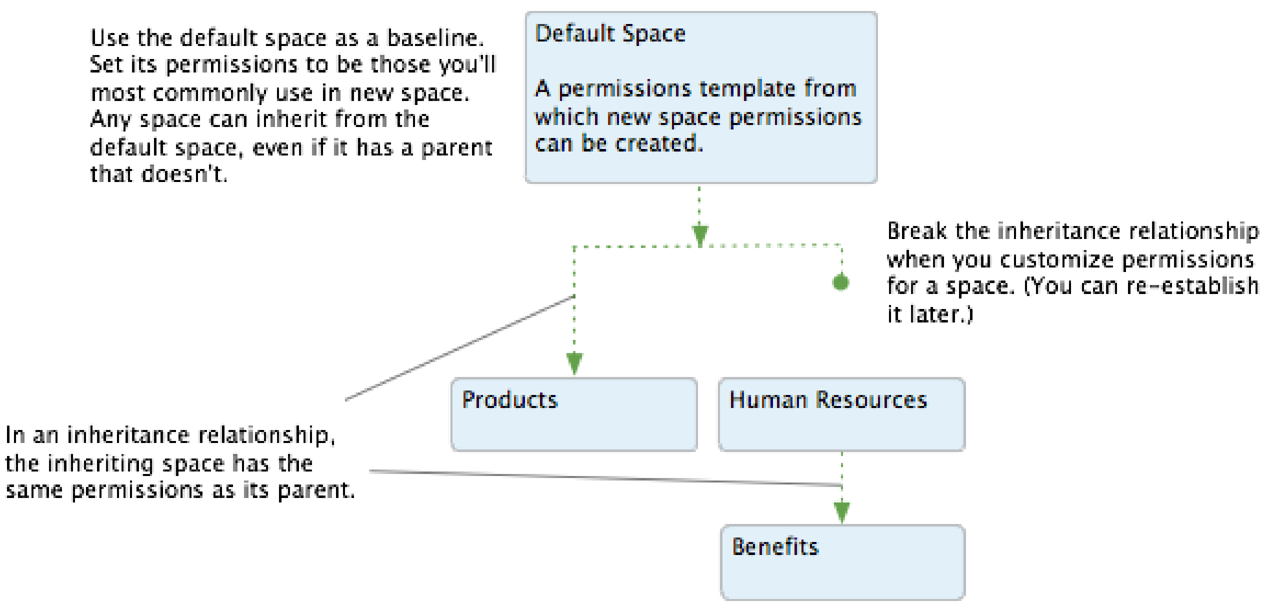
To make managing space permissions easier, an inheritance model provides a way to avoid (when you can) setting specific minute permissions for each new space. Spaces can inherit permissions from their parent or merely use those permissions as a starting point.

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** typically called "Jive" 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 a 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 spaces 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 community includes a default space, typically called "Jive". From there you can add more spaces to create a hierarchy.

The default space is the parent to all other spaces and 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. Click **Edit default space permissions**.
2. Configure the permissions for a group of users or individual users in the default space.

Setting Permissions for Spaces

You can assign individual users or groups of users various permission levels in a space.

To understand the different permission levels available for spaces and what they do, be sure to read Standard Space Permission Levels on page 273. You can also assign custom permissions levels.

To set permissions for people in a space:

1. In the Admin Console go to **Permissions** > **Space Permissions**.
2. Find and select the space you want to set permissions for.
3. On the page describing permissions for the space, assign permissions to a group of users or individual users.
4. To assign permissions to a group not yet listed:
   a) Click **Customize this space's permissions** > **Add group**and enter the name of the user group to add.
   b) Select a permission level from the drop-down menu.
   c) Click **Add Group**.
5. To edit permissions for a group of users already listed:
   a) Locate the user group in the list.
   b) Next to its permission level, click **edit**.
   c) Select a permission level from the drop-down menu.
   d) Click **Save**.

Creating User Overrides for Spaces

You can create an override for an individual user of a space.

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 a place, but isn't (and shouldn't be) a member of a permissions user group to which you've already assigned permissions for the place.
- A person is a member of a permissions user group to which you've assigned permissions for a place, but the person requires a different set of permissions than those received as a member of the place -- in other words, the person is an exception to the rule. For example, you might want to separately define the person's permissions to enhance or limit their access in the place.

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 user's name when you see it show up.
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: Projects inherit the permissions of the space that contain them. Social groups, on the other hand, are independent of spaces and projects. For more, see Managing Social Group Permissions.

Standard Space Permission Levels

Jive includes several predefined space permission levels that you can assign to individual users or groups of user you define, such as a space Administrator or Moderator.

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 40: 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 41: 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
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 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 42: Access Granted for Each Content Type Permission Level

Content Type Permission	View	Create	Reply	Comment	Rate	Vote
Create	Yes	Yes	Yes	Yes	Yes	Yes
Create (for discussions)	Yes	Yes	Yes	Yes	Yes	Yes
Contribute	Yes	No	Yes	Yes	Yes	Yes
View	Yes	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 43: Access Settings Available for Each Content Type

Content Type	View	Create	Reply	Comment/ Reply	Rate	Vote
Document	Yes	Yes	No	Yes	Yes	No
Discussion	Yes	Yes	Yes	No	No	No
Blog Post	Yes	Yes	No	Yes	No	No
Poll	Yes	Yes	No	Yes	No	Yes
Video	Yes	Yes	No	Yes	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 fail-safe 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 about this, be sure to read the Moderation section.

Creating a Custom Space Permission Level

You can create a custom space permission level that allows fine-grained control of a space. 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).

Fastpath: Admin Console > **Permissions** > **Space Permission Levels**

To create a custom space permission level:

1. From the **Custom Levels** tab, click **Create new permission level**.
2. In the **Create a Custom Permission Level** dialog box, enter a name and description for the permission level. These will help other administrators know the purpose of the new level.
3. Under **Access and administration,** select a category for the level, then choose from among the options in the category.
4. Click **Save**.

Now you can assign the custom level to an individual user or a user group, then configure the space's permissions to include that user or user group.

Managing Blog Permissions

This topic describes the permission settings for global blogs -- that is, blogs that aren't associated with a particular place. Global blogs 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 44: 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.

Blog Location	Permissions Management
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 view, create, and comment on global blogs.

You can only use the following standard permission levels for global blog permissions. Global blogs are those that are not associated with a specific space, group, or project.

Fastpath: **Admin Console** > **Permissions** > **Blogs**

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.

Setting Global Blog Permissions

You can set global blog permissions. Global blogs are those that are not associated with a specific space, group, or project.

Fastpath: **Admin Console** > **Permissions** > **Blog Permissions**

1. On the permissions 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 a place, but isn't (and shouldn't be) a member of a permissions user group to which you've already assigned permissions for the place.
- A person is a member of a permissions user group to which you've assigned permissions for a place, but the person requires a different set of permissions than those received as a member of the place -- in other words, the person is an exception to the rule. For example, you might want to separately define the person's permissions to enhance or limit their access in the place.

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 user's name when you see it show up.
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 Permissions

Social group permissions are designed 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.

Fastpath: Admin Console: Permissions > **Social Group Permissions**

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 permissions for social groups:

Permission	Access Granted
View social group	See the group feature 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.
Create group (private)	Create a new private or secret social group.
Manage social group	Allows users to manage any social groups.
Create externally accessible group	Allows users to create private and secret social groups accessible to invited external contributors.

Setting Social Group Permissions

Use this procedure to set up access to social groups.

You can set social group permissions in the Admin Console on the Social Group Permissions page. You can set the social group permission for either individual users (user override) or groups of users (user groups). For user groups permissions, the user group must exist before you can assign it permissions.

Fastpath: Admin Console > **Permissions** > **Social Group Permissions**

Setting a User Group Permission for Social Groups

1. On the permissions 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 a place, but isn't (and shouldn't be) a member of a permissions user group to which you've already assigned permissions for the place.
- A person is a member of a permissions user group to which you've assigned permissions for a place, but the person requires a different set of permissions than those received as a member of the place -- in other words, the person is an exception to the rule. For example, you might want to separately define the person's permissions to enhance or limit their access in the place.

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 user's name when you see it show up.
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.

Setting Up Non-member Content Editing

Community managers and people who have Create Group (Private) permissions can configure private groups so that group members can share specific documents and discussions with non-group members. This allows non-group members to help review and edit private group content, but does not allow them to see any other content items that live in the group.

To enable this for private groups in your community:

1. In the Admin Console, go to **System** > **Settings** > **Non-member Content Editing** and select **Enable non-member content editing**.
2. Click **Save**.

Owners of private groups will see the option to enable non-member content editing when they are editing the private group. People with Create Group (Private) permissions will see the option when creating (or editing) a private group. (Note that secret groups can't have this feature enabled, because it would expose the name of the group to users who were not aware of it.)

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. These 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. If you have enabled the Home page in your community, it can be 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 voting in polls, 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 status 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) Home page.
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.

Permission	Access Granted
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.
DM/Sharing user override	Allows users to override the DM/Sharing connection requirement.
Create attachments	Allow users to create attachments on content.
Insert images	Allows users to insert images into content.
Customize site	Allows users to customize site appearance (theming).
Manage Slideshow Carousel	Work with the multi-image slideshow widget used on the community's Home page and Overview pages.

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 permissions 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 the 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 a place, but isn't (and shouldn't be) a member of a permissions user group to which you've already assigned permissions for the place.
- A person is a member of a permissions user group to which you've assigned permissions for a place, but the person requires a different set of permissions than those received as a member of the place -- in other words, the person is an exception to the rule. For example, you might want to separately define the person's permissions to enhance or limit their access in the place.

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 user's name when you see it show up.
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 user name 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. 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.

Fastpath: **Admin Console** > **People** > **Management** > **Create User Group**

1. Enter a user group name and description. Choose something that will help you know at a glance what the user group is for and who's in it, for example, "HR_bloggers" or "Uber_admins".
2. Click **Enabled** if you want to use role badges. These are visual cues in the user interface that help people quickly identify community users and their responsibilities. You must also upload an image and select a role for this user group.
3. Upload a 16 by 16 pixel image to provide the visual cue you'll see next to those community users that will let others know their responsibilities.
4. Select the role for the users in this user group. You can choose from the following roles:
   - Administrator
   - Champion
   - Employee
   - Expert
   - Moderator
   - Support
5. Click **Create Group**.
6. Use the **Add Members** links to add user accounts for people who should be members of the new user group. For more information see Managing Group Membership.
7. Use the **Add Admins** links to add user accounts for people who will have permission to administer the account. If you use the badge roles, they will NOT be applied to the admins. For more information see Managing User Group Membership.

8. 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

Create user groups to assign permissions to groups of community users. You can add users as members and/or admins. Admins are responsible for administering the user group.

If you want admins to have the same permissions (if any) granted to a user group, then you need to also add them to the Group Member list. When admins are not added to the Group Members list, they only have permission to add or remove users from the Group Members and Group Admins lists, and they do not have the permissions (if any) assigned to the user group.

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 depending 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 admins 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. You may want to add this Admin to the Group Member list to grant them user group permissions, if any.
6. Click **Update**.

Editing User Group Settings and Properties

User group settings are simple, including the group's name and description, along with group properties.

You can edit a user group's settings in the Admin Console by going to **People** > **Management** > **User Group Summary** page, then clicking the group's name.

User group properties are simple name-value pairs that programmers can use to work with the group in their code. User 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.

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.

Visibility 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 a User Account

Add a new user to the community by creating their user account.

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). For more information about using LDAP or Active Directory with Jive, take a look at the LDAP and Active Directory Guide.

To create a new user account:

1. Navigate to **People** > **Management** > **Create User**.
2. Enter the user's basic information, including a username, email address, and password. Note that some communities are preconfigured to use a user's email address as their username.

   Note: A username may not contain any of the following characters: **, / ? & #**

3. You can choose to send the new user a welcome email. (For more about the template a welcome email is created from, see Editing Email Notification Templates.)
4. To create this new account and edit its properties now, click **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.
5. To create this account and move on to creating another (without editing account properties), click the Create & Create Another User button.

Deleting and Deactivating a User Account

You can deactivate or delete a user account when you want to remove the person's presence from the community.

Note: An administrator can also ban someone from being able to access to the community. For more information, see Banning People.

Deactivating a user account removes their access but keeps their content in the system. When you deactivate someone's account, Jive will replace their former avatar with a blank avatar; the word "Deactivated" 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 community 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 deactivating 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 deactivate a user account:

1. Go to **People** > **Management** > **User Search** .
2. Find the user account you want to delete in the list and click the **Delete** or **Deactivate** button.

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 they log in.
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 to make following easier. The relationships you define are optionally visible in people's profiles. Using these relationships can help community users stay on top of what specific other 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.

On the Admin Console's User Relationship Management page, you can create new relationships between users, or view or break (retire) existing relationships.

Creating Relationships

To create a friend relationship:

1. In the Admin Console, go to **People** > **Management** > **User Relationships**.
2. Enter the usernames of the people in the new relationship. If you can't remember the usernames, click the magnifying glass to browse and search a list of users; then, select the checkbox next to the one you want.
3. Click **Add** to create the relationship.

Viewing and Breaking Existing Relationships

To view or break existing relationships:

1. In the Admin Console, go to **People** > **Management** > **User Relationships**.
2. At the bottom of the page, you'll see a list of existing relationships. 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.

Configuring the Org Chart

You can enable or disable the Org Chart in the Admin Console. The Org Chart makes it easier for users to understand organizational relationships between people.

Internal communities	By default, internally-facing communities (those that typically involve only employees or other internal audiences) have the Org Chart enabled.
External communities	By default, externally-facing communities (those that typically involve customers, vendors, and other external audiences) have the Org Chart disabled.

To enable the Org Chart:

1. In the Admin Console, go to **People** > **Settings** > **Org Chart Settings** and select **Is org chart enabled?**
2. Select the additional options you want for the Org Chart, such as setting up an approval process for changes to Org Chart relationships.
3. Click **Save Changes**.
4. Next, set up the relationships for the Org Chart on the **People** > **Management** > **Org Chart Management** page.

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.

Configuring User Profiles

You can configure how users are allowed to set up their user profiles.

Letting Users Control Their Own Settings

You can let people control who sees their profile information 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 select a group of users who will see their name and email address.

The User Profile Fields and Other Options sections of the Profile Setting page enable 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, allow profile images or enable skills and endorsements. For information on customizing the user's profile fields using the Header Profile Fields and Other Profile Fields sections, see Configuring User Profile Templates.

Fastpath: **Admin Console** > **People** > **Settings** > **Profile Settings**

Setting	Description
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.
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.

Setting	Description
Allow Profile Images	Set to "Yes" to allow people to display an image (such as of themselves) on their user profile. You can also set the maximum number of profile images users can upload.
Show Full Name by Default	Set to "Yes" to have a person's full name displayed on their profile, as opposed to merely their user name. 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.
Skills and Endorsements	Select whether you want to enable both skills and endorsements, or disable both. You can also only enable skills and not endorsements. Skills are how users tag their own profile and endorsements are the tags others give users.

Configuring User Profile Templates

User profiles, like other content, can be found on searches. Because of this, what people say about themselves — including interests and areas of expertise — can be a great source of information for people looking to have a question answered.

A user's profile can include biographical and professional information, along with links to content they've contributed. Use the Profile Settings page to edit the fields that show up in profiles and set up visibility options.

On the Profile Settings page, you'll find the Header and Other Profile Fields sections, where you can define the exact profile template you want to provide users so they can complete their profile. You'll see the Header Profile fields highlighted in the top left of user profile if they are marked visible. The rest of the sections (User Profile Fields and Other Options) give you a way to let others control their own settings. For more on this, see Letting Users Control Their Own Settings.

Fastpath: Admin Console > **People** > **Settings** > **Profile Settings**

The application includes several commonly used fields by default, and you can add custom fields as well. Order the fields in the same order you want users to see them. 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 create a custom field, click **Create new field...**.

To change the behavior of a profile field, click the appropriate icon under Manage Properties. These icons define the field's 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.
- Users may edit -- People can edit their editable profile fields.
- User may configure visibility -- Enables users set this field to their own visibility preferences.

Create New 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 **Create 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 relationships 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.

Selecting Fields for Hover Cards

You can decide which of the short fields from people's profiles are displayed on the cards that are shown you hover over a person's name or avatar in the community.

Fastpath: Admin Console > **People** > **Settings** > **Hover Card Settings**

Your hover card fields are a subset of the Profile Fields you have defined in **People** > **Settings** > **Profile Settings**, and the visibility of each field is determined by what you've defined in Profile Settings. You can select up to five fields to be displayed on the hover card. The following field types can't be displayed on the hover card:

- Fields with the Large Text format (like Bio)
- Fields that are based on a multi-select option

You can change the order of the fields on the card from top to bottom by dragging and dropping. If your community is integrated with Lync or Webex, you'll see the associated links in a fixed location on the card. You also won't be able to move some other information, such as status levels and points.

Note that if a field you selected for the hover card does not contain any information, neither the field nor its label will be displayed.

To set the hover card fields:

1. Make sure the hover card fields you want have the correct visibility set in **People** > **Settings** > **Profile Settings**.
2. Go to **People** > **Settings** > **Hover Card Settings**.
3. Drag fields you want included on the hover card view from Available Fields to Hover Card Fields. Drag any of the fields you don't want included off the Hover Card Fields list.
4. Decide if you want the field names to show on the hover card as well as the field values. You can do this by toggling Show Label on and off. For example, if you want to the card to show Department: Manufacturing, keep the Show Label column checked, which is the default. If you want to just show Manufacturing, click the check mark in the Show Label column next to the Department field to remove it.

Moderation

Moderation allows you to designate one or more users to approve or reject documents, discussions, comments, and many other kinds of content before they are published in the community. You can set up moderation on nearly all types of content.

Note: Moderation is different from Document Approval. Document Approvers can only approve or reject documents in a space; moderators can approve or reject nearly all content types. To learn more about the document approval feature, see Setting a Document Approver in a Space.

Note: If you're trying to set up abuse reporting, see Setting Up Abuse Reporting.

What Is Moderation?

The moderation feature allows you to assign certain users to review and approve (or reject) content changes submitted by community users before they are published. You can designate one or several moderators and enable moderation for a variety of content types. You can also set up abuse reporting and moderate user registration.

For a complete list of content types that can be moderated and the places where you can enable moderation, see Who Moderates What?

The following types of moderation are available in the application:

Content moderation	You can enable content moderation in a space and the projects it contains, or in the root space and all social groups (because social groups are contained by the root space and inherit its moderation settings). You can designate one or several content moderators per place, as well as limit the type of content moderated in that place (documents, blog posts, discussions, and so on).
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.
User registration moderation	When you enable user registration moderation, registration requests are reviewed by a moderator(s) and then approved or rejected. You can blacklist email addresses from specific domains or auto-approve users if their email addresses originate from your community domain.
Profile image moderation	You can enable moderation for images that users upload to their user profile. This feature is either fully enabled for all users or fully disabled for all users.
Avatar moderation	You can enable moderation for every user-uploaded avatar image. For more information, see Setting Up User-Uploaded Avatar Moderation on page 310.
Abuse reporting	When users report abuse, the reports are sent to a moderator. For more information, see Setting Up Abuse Reporting.

Moderation Best Practices

Consider using these best practices if you enable moderation in your community.

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 and more than one global moderator. 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.

Moderator Roles and Where to Set Them

The following table lists the moderator roles and the location in the Admin Console where you assign a user(s) or group of users to the role.

Permission Level Name	Location of Setting
Space Moderator	**Permissions** > **Space Permissions** > **Moderate**
Global Moderator	**Permissions** > **System Administration** > **Moderate Content**

Permission Level Name	Location of Setting
Full Access	**Permissions** > **System Administration** > **Full Access**

Who Moderates What?

The following tables show the types of content that can be configured for moderation, who moderates them, and the order in which Jive notifies the moderator(s) about content submitted for moderation.

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 Space, Jive first looks for a Space Moderator; if there is none assigned, it then looks for a Global Moderator, and so on.

Caution: We strongly recommend designating more than one moderator per place and more than one global moderator. Refer to Moderation Best Practices for more information.

Click on an image to enlarge it.

Moderation Rules and Notification Hierarchy for the Creation of Contained Content Types

<table>
<tr><th></th><th></th><th colspan="8">Content Types</th></tr>
<tr><th></th><th></th><th>Announcements</th><th>Polls</th><th>Documents</th><th>Discussions</th><th>Blog Posts</th><th>Videos</th><th>Ideas</th><th>Status Updates</th></tr>
<tr><td rowspan="6">Containers</td><td>Root Container</td><td colspan="8">1. Global Moderator → 2. Full Access</td></tr>
<tr><td>Open and Member Social Groups</td><td colspan="8">1. Global Moderator → 2. Full Access</td></tr>
<tr><td>Private and Secret Social Groups</td><td colspan="8">Cannot be Moderated</td></tr>
<tr><td>Space and Sub-spaces</td><td colspan="7">1. Space Moderator → 2. Global Moderator → 3. Full Access</td><td>Content Type Not Available Here</td></tr>
<tr><td>Projects</td><td colspan="7">1. Space Moderator → 2. Global Moderator → 3. Full Access</td><td>1. Global Moderator → 2. Full Access</td></tr>
<tr><td>Your Personal Content</td><td>Content Type Not Available Here</td><td colspan="3">Cannot be Moderated unless Visibility = All, then 1. Global Moderator → 2. Full Access</td><td>1. Global Moderator → 2. Full Access</td><td colspan="2">Cannot be Moderated unless Visibility = All, then 1. Global Moderator → 2. Full Access</td><td>Content Type Not Available Here</td></tr>
</table>

Moderation Rules and Notification Hierarchy for Content Comments

		Content Types						
		Poll Comments	**Document Comments**	**Discussion Replies**	**Blog Comments**	**Video Comments**	**Idea Comments**	**Status Comments**
Containers	**Root Container**	1. Global Moderator → 2. Full Access						
	Open and Member Social Groups	1. Global Moderator → 2. Full Access						
	Private and Secret Social Groups	Cannot be Moderated						
	Spaces and Sub-spaces	1. Space Moderator → 2. Global Moderator → 3. Full Access						Content Type Not Available Here
	Projects	1. Space Moderator → 2. Global Moderator → 3. Full Access						1. Global Moderator → 2. Full Access
	Your Personal Content	Cannot be Moderated unless Visibility = All, then 1. Global Moderator → 2. Full Access			1. Global Moderator → 2. Full Access	Cannot be Moderated unless Visibility = All, then 1. Global Moderator → 2. Full Access		Content Type Not Available Here

Moderation Rules and Notification Hierarchy for System-wide Content Types

		Content Types		
		Avatar Image	**User Registration**	**Profile Images**
Containers	**Root Container**	1. Global Moderator → 2. Full Access		
	Open and Member Social Groups	Content Type Not Available Here		
	Private and Secret Social Groups	Content Type Not Available Here		
	Spaces and Sub-spaces	Content Type Not Available Here		
	Projects	Content Type Not Available Here		
	Your Personal Content	Content Type Not Available Here		

What Cannot Be Moderated?

You cannot moderate content created in private groups, secret groups, or content that has visibility limited to the author (Hidden) or to specific users.

Note: Externally-facing communities (those serving customers, partners, and vendors), do not have the Personal Content (Hidden) feature.

Moderation Inheritance in Groups and Spaces

Moderation inheritance works differently depending on the content's container.

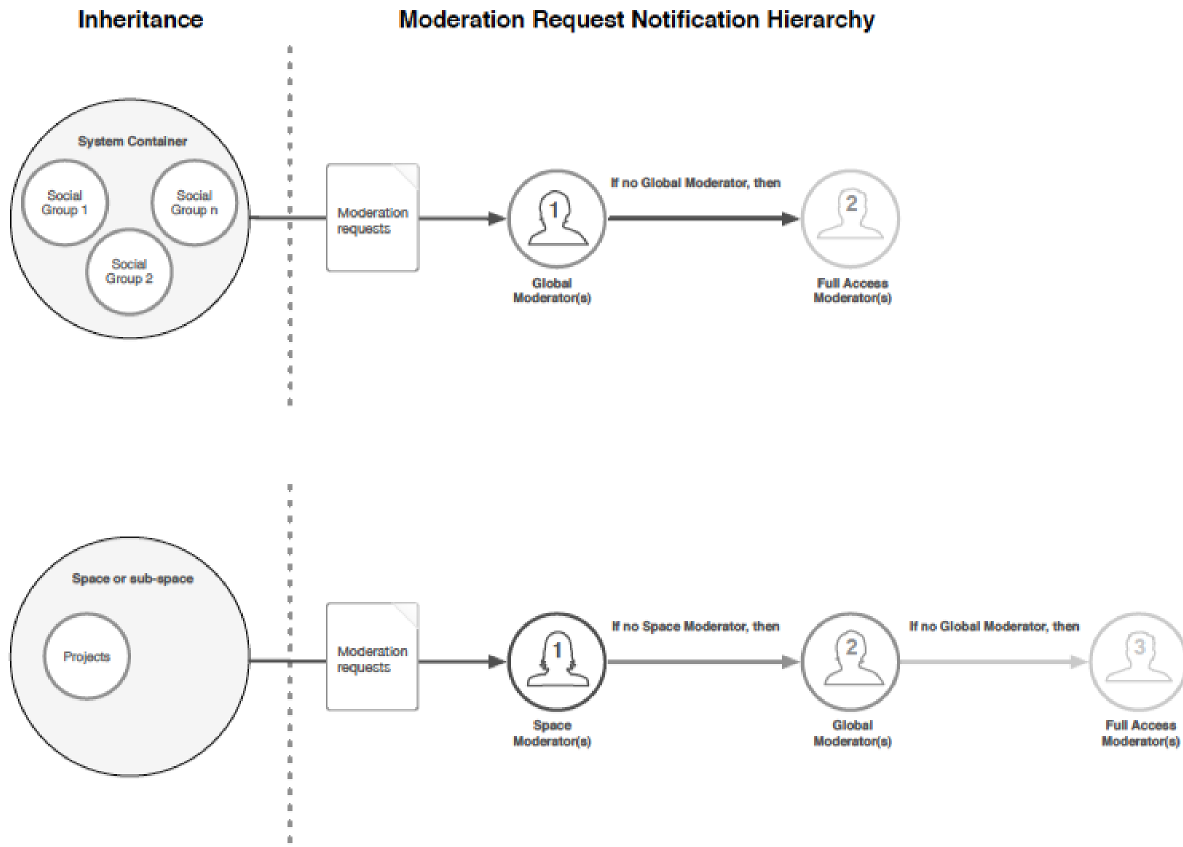
Here's how moderation inheritance works in places:

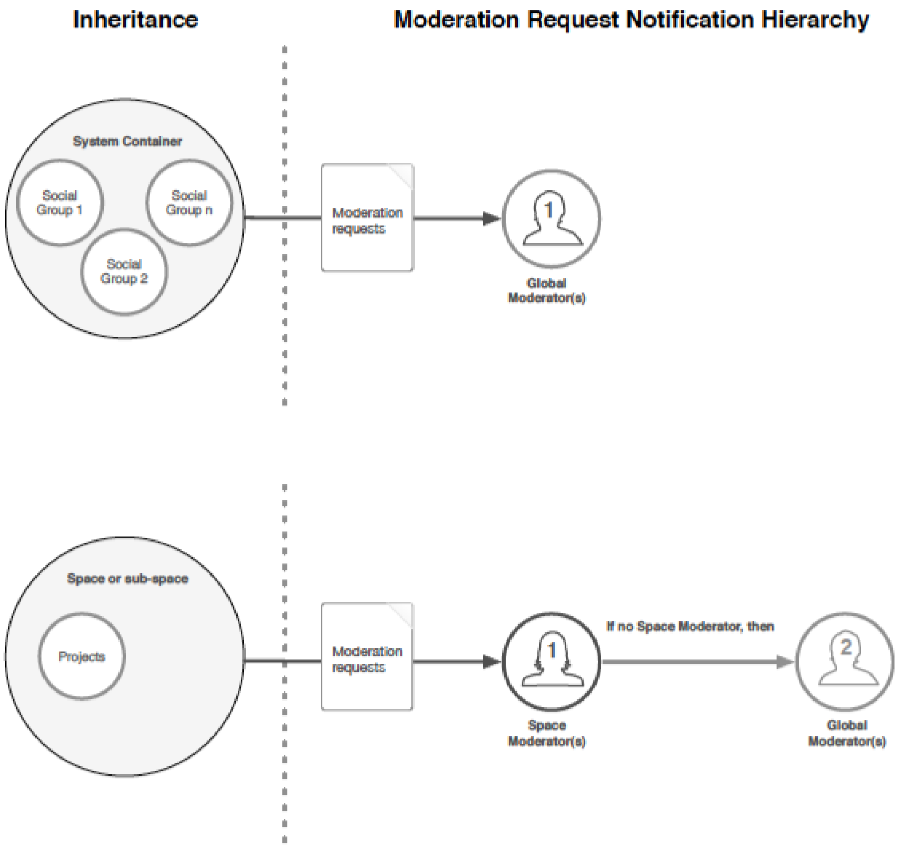
- Groups inherit the moderation settings of the system container (also known as the root container or the Jive Community) and are moderated by the Global Moderator(s), if there is one, and if not, by the Full Access user(s).
- Projects inherit the moderation settings of their container space or sub-space and are moderated by the Space Moderator(s), if there is one, and if not, by the Global Moderator(s). If there is no Global Moderator, the application will send the moderation request to the Full Access user(s).

Note: Projects inherit the moderation settings of their container space or sub-space *except in the case of status updates posted in projects*, which are moderated the same way as status updates posted in a group.

For a complete list of content types and the places where you can and cannot enable moderation, see Who Moderates What? and What Cannot Be Moderated?

The following illustration shows how moderation inheritance works and the order in which moderators are notified:


Inheritance
Moderation Request Notification Hierarchy
System Container
Social Group 1
Social Group n
Social Group 2
Moderation requests
If no Global Moderator, then
Global Moderator(s)
Full Access Moderator(s)
Space or sub-space
Projects
Moderation requests
If no Space Moderator, then
If no Global Moderator, then
Space Moderator(s)
Global Moderator(s)
Full Access Moderator(s)



Setting Up Content Moderation

There are three steps to enabling content moderation in a place: selecting the place to be moderated, selecting the content types to be moderated in the place, and assigning the moderator(s) for the place.

Caution: You cannot moderate content created in private groups, secret groups, or content that has visibility limited to the author (Hidden) or to specific users.

Caution: Make sure you understand how moderation inheritance works before you enable moderation in a place.

Setting Up Moderation in the System Container and All Groups

When you enable moderation in the system container, you are enabling moderation there and in all groups (because they are contained by the system space and inherit its moderation settings). Moderation requests submitted in the system container or any group will be sent to the Global Moderator, if there is one, and if not, to the Full Access user(s).

To set up moderation in the system container and all groups:

1. In the Admin Console, go to **Spaces** > **Settings** > **Moderation Settings**.

2. Click **Change space** and select the top-level system container space (typically called "Jive" or "Default").
3. Select the content type(s) you want to moderate, for example, announcements, polls, documents, blog posts, and so on. You can choose one, several, or all. All content types will be moderated by the user(s) you will designate. In other words, you can't have Joey moderate documents in the place and Dee Dee moderate blog posts in the place.
4. Click **Save changes**.
5. Now go to **Permissions** > **Space Permissions**, and select the same place for which you just enabled moderation.
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 Moderation in a Space or Sub-space

When you enable moderation in a space or sub-space, you are enabling moderation in only that space or sub-space and its projects (because projects inherit the moderation settings of their container space or sub-space). Moderation requests submitted in the space will first be sent to the Space Moderator, if there is one, and if not, to the Global Moderator. If there is no Global Moderator assigned, the moderation request will go to the Full Access user(s).

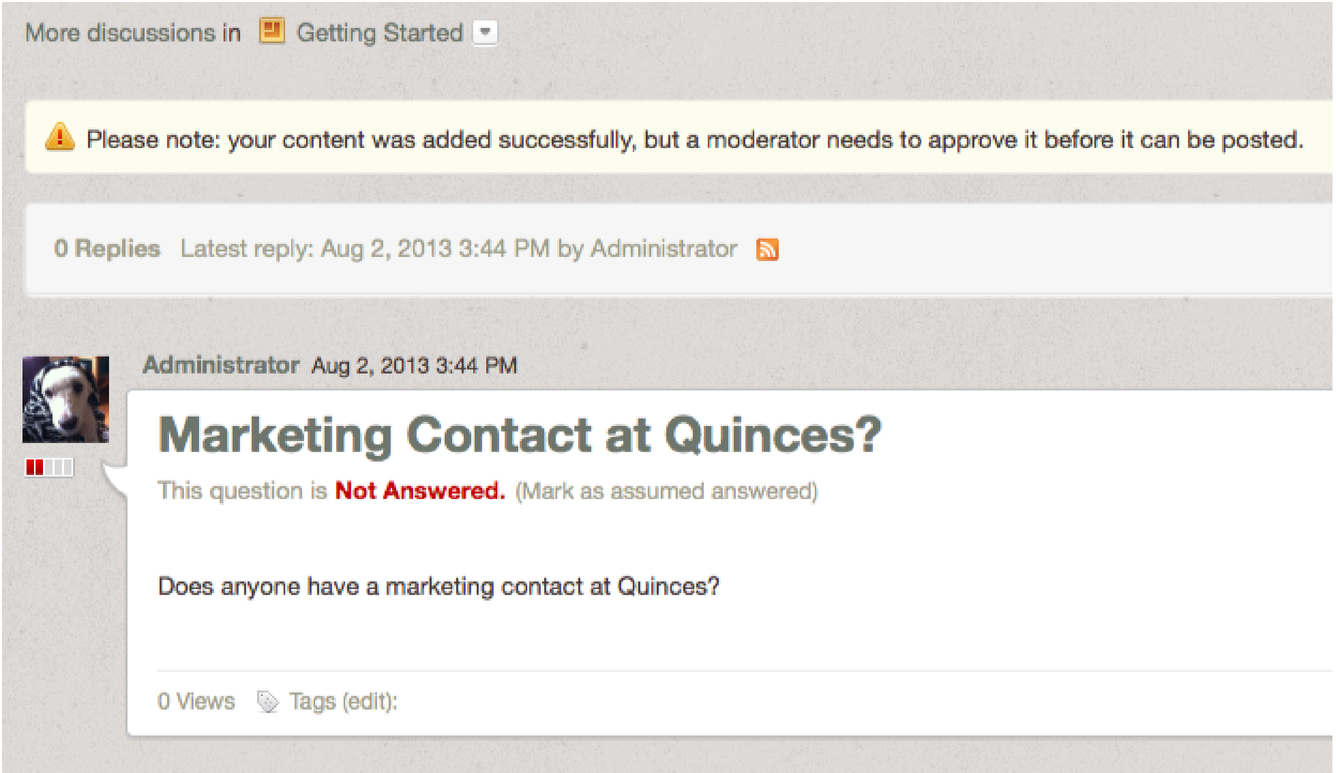
To set up moderation in a space or sub-space (and its projects):

1. In the Admin Console, go to **Spaces** > **Settings** > **Moderation Settings**.
2. Click **Change space** and select the Space you want to moderate.
3. Select the content type(s) you want to moderate, for example, announcements, polls, documents, blog posts, and so on. You can choose one, several, or all. All content types will be moderated by the user(s) you will designate. In other words, you can't have Joey moderate documents in the Space and Dee Dee moderate blog posts in the Space.
4. Click **Save changes**.
5. Go to **Permissions** > **Space Permissions**, and select the same space for which you just enabled moderation.
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**.

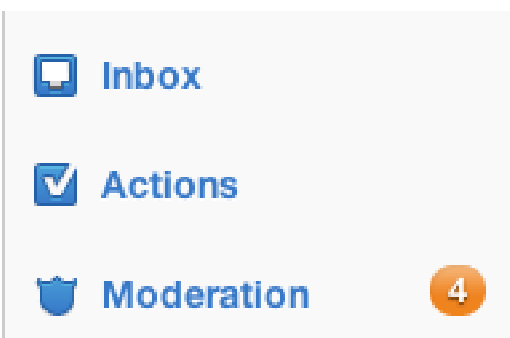
Reviewing Content Moderation Requests

If you are a moderator for a place, you'll have access to a list of requests for moderation.

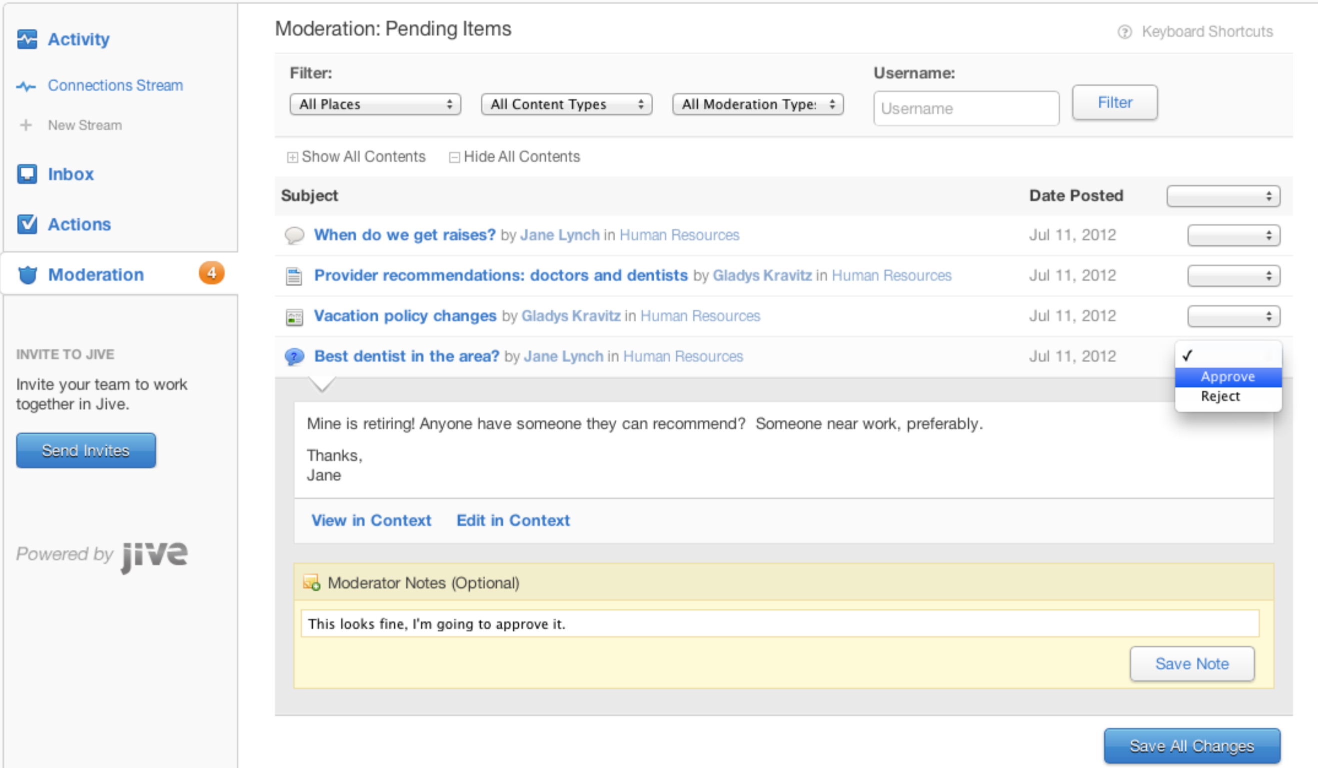
In places where content moderation is enabled, the author of a piece of content will see a note explaining that their content needs to be approved by the moderator before it will be published:



After the author submits the post, a moderation request will be sent to the moderator's Moderation queue for approval or rejection. (The community administrator sets up moderators for places. There can be more than one moderator in a place. For more about that, see Setting Up Content Moderation). Note that the author can still access the submitted content by going to **Content** > **Drafts**, where they can continue to make changes. The moderator will see only one item to moderate, no matter how many changes the author makes.



If there is more than one item awaiting moderation, you'll see a list in your Moderation queue. 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 your community administrator. The following example shows a variety of items awaiting moderation:



Notice that at the top of the page, you can filter the content listed. Filtering can be helpful when you've got a very long list.

To moderate, simply click on an item and make a decision to:

- **Approve the content.** This will publish the content in the community. You will no longer see the item in your moderation queue.
- **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. If you (or another moderator) reject the 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. Once something has been rejected by you or another moderator, you can still see the item in the Admin Console under **Spaces** > **Management** > **Document/Discussion Management**. From there, you can edit the item by clicking the pencil icon next to it and then publish the item if you've changed your mind about it. Remember that all social groups are contained by the system (root) space, so you will see content items here from groups.
- **Leave a note.** This note 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 User Registration Moderation

You can set up moderation for new user registrations if you've set up the application to allow people to register on their own. A community manager or system administrator enables both user registration and moderation for new registration requests.

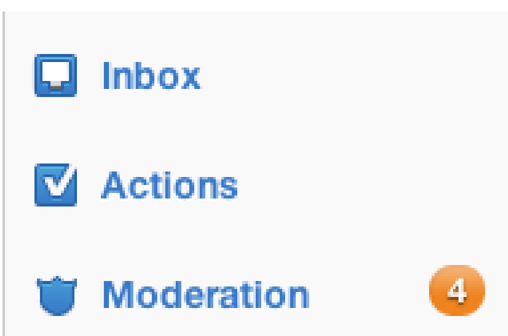
To set up new user registration moderation:

1. Enable user self-registration by going to **People** > **Settings** > **Registration Settings** and select **Enabled** under "Allow user-created accounts." This allows users to create their own account from the login page. To learn more about the options on this page, see Configuring User Registration.
2. On the same page, under "Registration Moderation," select **Enabled**. This turns on the moderation feature for all new user registrations.
3. You can select **Only for addresses matching the blacklisted domain list** to limit registration moderation to those email address originating only from the domains that you blacklist. Alternatively, you can block registrations entirely from those you list in the blacklist box by selecting **Always block registrations from blacklisted domains**. To block or moderate all addresses from a domain, use an asterisk before the domain, e.g., ***@domain.com**.
4. Make sure you have designated a Global Moderator(s). The application will send new user registration moderation requests to that user(s) first. If you don't have one, the application will send the request to the Full Access user(s).

Moderating New User Registrations

If you are the moderator for new user registration, you will approve or decline new registration requests. Here's how it works:

1. When someone submits a new registration, you will see an alert on your Moderation tab in the end user interface. Click it.



2. On the Pending Items page, you will see the request (or a list of requests). Click the person's name to view their profile page with the information they entered.
3. Then **Approve** or **Reject** the registration request. If you reject, you can enter your reason before finishing.

Setting Up Profile Image Moderation

You can enable moderation for images that users upload for use in their user profile.

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

This feature is either fully enabled for all users or fully disabled for all users.

1. Enable profile image visibility by going to **People** > **Settings** > **Profile Settings** and selecting **Yes** in the Allow Profile Images field.
2. Go to **People** > **Settings** > **Profile Image Moderation** and select **Enable moderation of new user profile images**, then **Save**.
3. Make sure you have a Global Moderator(s) assigned at **Permissions** > **System Administration** > **Moderate Content**. The application will send profile image moderation requests to that user(s). If it does not find a Global Moderator, the request will go to the Full Access user, which is assigned at **Permissions** > **System Administration** > **Full Access**.

Setting Up User-Uploaded Avatar Moderation

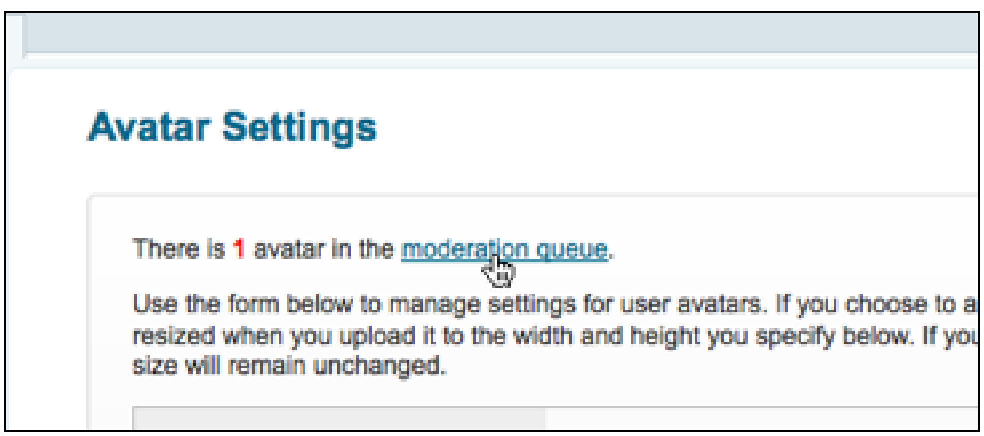
You can have every user-uploaded avatar image added to a moderation queue for approval or rejection.

Fastpath: Admin Console: People > Settings > Avatar Settings > Moderate uploaded user avatars

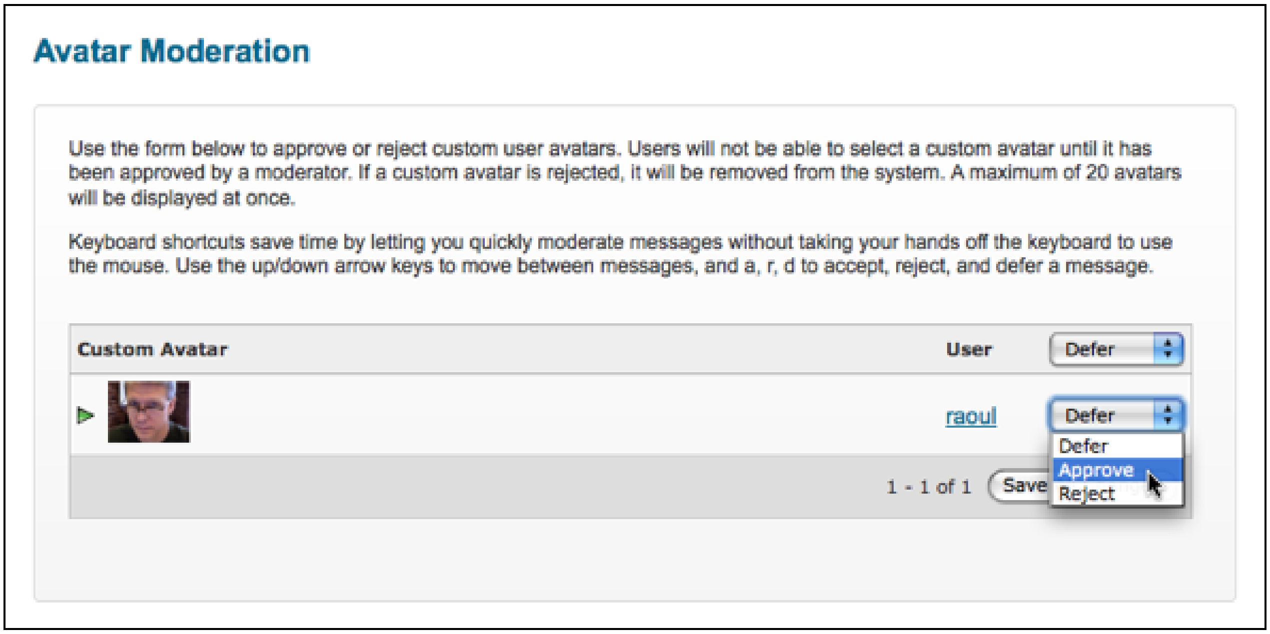
When you choose to have avatars moderated, a user uploading an avatar will be told by the interface that their avatar choice is pending approval. Once approved, the avatar will be available for the user to designate it (or others) as their primary avatar. It will not become the user's primary avatar until the user manually selects it after moderator approval.

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

Note: The avatar moderator will see the link only when there are images in the queue waiting to be moderated.



The moderator will then select **Defer, Approve, or Reject** for images listed in the avatar 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 the bottom of that page, under User Avatars, you can view and delete their uploaded avatar images.

Moderation: Frequently Asked Questions

Here are answers to some frequently asked questions about moderation.

How is moderation in groups different from moderation in spaces?

You can enable moderation on some spaces and sub-spaces, but not others. For each space or sub-space with moderation enabled, you can designate a different user to be the Space Moderator. Projects inherit the moderation settings of their container/parent space or sub-space.

Groups are contained by the system container (also called the root container or Jive Community) and inherit its moderation settings. Therefore, if you enable moderation in the system container (root), moderation is enabled *for the system/root container and all groups*. You cannot enable moderation on an individual group. All moderation requests in the system (root) container and groups will be sent to the Global Moderator(s), if there is one, and if not, to the Full Access user.

Can I moderate the creation of groups?

There is no specific setting to set up moderation for the creation of groups. However, you can implement a workaround by limiting the permissions of group creation to one group of users. Regular users would then have to request the creation of a new group from the group with permission.

How does moderation inheritance work?

We explain this with handy drawings in Moderation Inheritance in Groups and Spaces.

What kinds of content can be moderated?

Nearly all content types can be moderated. For a full list, see Who Moderates What?

You cannot moderate content created in private groups, secret groups, or content that has visibility limited to the author (Hidden) or to specific users.

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 Space Moderator(s) is specified, who would get moderation notifications?

The Global Moderator(s) (assigned here: **Permissions** > **System Administration** > **Moderate Content**). If there is no Global Moderator assigned, then moderation requests in that space would be sent to the Full Access user (assigned here: **Permissions** > **System Administration** > **Full Access**).

See Who Moderates What? and Moderation Inheritance in Groups and Spaces to understand how the application notifies moderators.

How are moderators notified that they have content pending moderation?

The alerts displayed on the Moderation icon show the number of unacknowledged moderation alerts. 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 set by place. So, if you create a document in a place that has moderation enabled, the moderator for that place can edit any and all documents submitted for publication in that place.

If I save a document as Hidden, can it be moderated?

No. Your Hidden documents cannot be 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 group to a space and both are moderated, items 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 place, items that were already awaiting moderation will remain in moderator queues, but the item will appear to community users as if it were already approved.

Moderation for Contained Content Types

Moderation Rules and Notification Hierarchy for the Creation of Contained Content Types

<table>
<tr><th></th><th></th><th colspan="8">Content Types</th></tr>
<tr><th></th><th></th><th>Announcements</th><th>Polls</th><th>Documents</th><th>Discussions</th><th>Blog Posts</th><th>Videos</th><th>Ideas</th><th>Status Updates</th></tr>
<tr><td rowspan="6">Containers</td><td>Root Container</td><td colspan="8">1. Global Moderator → 2. Full Access</td></tr>
<tr><td>Open and Member Social Groups</td><td colspan="8">1. Global Moderator → 2. Full Access</td></tr>
<tr><td>Private and Secret Social Groups</td><td colspan="8">Cannot be Moderated</td></tr>
<tr><td>Space and Sub-spaces</td><td colspan="7">1. Space Moderator → 2. Global Moderator → 3. Full Access</td><td>Content Type Not Available Here</td></tr>
<tr><td>Projects</td><td colspan="7">1. Space Moderator → 2. Global Moderator → 3. Full Access</td><td>1. Global Moderator → 2. Full Access</td></tr>
<tr><td>Your Personal Content</td><td>Content Type Not Available Here</td><td colspan="3">Cannot be Moderated unless Visibility = All, then 1. Global Moderator → 2. Full Access</td><td>1. Global Moderator → 2. Full Access</td><td colspan="2">Cannot be Moderated unless Visibility = All, then 1. Global Moderator → 2. Full Access</td><td>Content Type Not Available Here</td></tr>
</table>

Moderation for Comments on Content

Moderation Rules and Notification Hierarchy for Content Comments

<table>
<tr><th></th><th></th><th colspan="7">Content Types</th></tr>
<tr><th></th><th></th><th>Poll Comments</th><th>Document Comments</th><th>Discussion Replies</th><th>Blog Comments</th><th>Video Comments</th><th>Idea Comments</th><th>Status Comments</th></tr>
<tr><td rowspan="6">Containers</td><td>Root Container</td><td colspan="7">1. Global Moderator → 2. Full Access</td></tr>
<tr><td>Open and Member Social Groups</td><td colspan="7">1. Global Moderator → 2. Full Access</td></tr>
<tr><td>Private and Secret Social Groups</td><td colspan="7">Cannot be Moderated</td></tr>
<tr><td>Spaces and Sub-spaces</td><td colspan="6">1. Space Moderator → 2. Global Moderator → 3. Full Access</td><td>Content Type Not Available Here</td></tr>
<tr><td>Projects</td><td colspan="6">1. Space Moderator → 2. Global Moderator → 3. Full Access</td><td>1. Global Moderator → 2. Full Access</td></tr>
<tr><td>Your Personal Content</td><td colspan="3">Cannot be Moderated unless Visibility = All, then 1. Global Moderator → 2. Full Access</td><td>1. Global Moderator → 2. Full Access</td><td colspan="2">Cannot be Moderated unless Visibility = All, then 1. Global Moderator → 2. Full Access</td><td>Content Type Not Available Here</td></tr>
</table>

Moderation for System-Wide Content Types

Moderation Rules and Notification Hierarchy for System-wide Content Types

		Content Types		
		Avatar Image	**User Registration**	**Profile Images**
Containers	**Root Container**	1. Global Moderator → 2. Full Access		
	Open and Member Social Groups	Content Type Not Available Here		
	Private and Secret Social Groups	Content Type Not Available Here		
	Spaces and Sub-spaces	Content Type Not Available Here		
	Projects	Content Type Not Available Here		
	Your Personal Content	Content Type Not Available Here		

Jive Security

Jive's security and privacy features are designed to meet the requirements of the most tightly regulated global industries and government agencies.

Jive Software makes every effort to protect the confidentiality, integrity, and availability of its cloud-based, hosted, and on-premise communities, as well as its cloud-delivered services. Jive Software continually evaluates the security of current and past product versions to protect your organization's data. This section provides a brief overview of Jive's security features and some suggestions about the configuration features you can use to protect your community and its information. For more information about Jive's security architecture and practices, see the Jive Security whitepaper on the Jive Community. A more detailed version is available under NDA from Sales or Support.

Note: This security section only describes the Jive application. It does not describe the security features of third-party products that integrate with Jive.

In-product Security Features

Several built-in security features allow you to configure your Jive community for the appropriate level of security for your organization.

Authentication Features

Login Security	Using the Admin Console, you can configure Jive to strongly discourage automated (computer-driven) registration and logins. Automated registration is usually an attempt to gain access to the application for malicious reasons. By taking steps to make registering and logging in something that only a human being can do, you help to prevent automated attacks. We recommend using the following tools, all of which are available as options in the Admin Console: • Login Throttling: Enabling login throttling slows down the login process when a user has entered incorrect credentials more than the specified number of times. For example, if you set the number of failed attempts to 5 and a forced delay to 10 seconds and a user fails to log in after more than 5 attempts, the application would force the user to wait 10 seconds before being able to try again. • Login Captcha: Enabling login Captcha will display a Captcha image on the login page. The image displays text (distorted to prevent spam registration) that the user must enter to continue with registration. This discourages registration by other computers 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 cannot

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 is 6, which is long enough to make the image useful, but short enough to make it easy for real humans.

- Password Strength: You can choose to enforce strong passwords via the Admin Console. The following options are available out of the box:
  - a minimum of 6 characters of any type
  - a minimum of 7 characters including 2 different character types (uppercase, lowercase, number, punctuation, and/or special characters)
  - a minimum of 7 characters including 3 different character types
  - a minimum of 8 characters, including all 4 character types

To learn more about configuring login and password security, see Configuring Login Security and Configuring User Registration.

Session Timeout

By default, Jive passes a token that persists the user session for 30 minutes from the last request. If you have a specific need to modify this limit (for example, if you need to make your Jive session timeout match the timeout of your identity provider when configuring SSO), you can use the auth.lifetime system property to set a new session timeout period in minutes. Keep in mind that increasing session duration increases security risks such as session hijacking and unattended workstation tampering. You should consult your organization's security team before you modify this value.

Email Validation

You can configure Jive to require email validation for all new accounts. This setting helps to prevent bots from registering with the site and then automatically posting content. When you configure email validation, Jive will require a new user to

	complete the registration form and retrieve an email with a click-through link to validate their registration. To learn how to enable this setting, see Configuring User Registration.
Account Lockout	Jive does not offer account lockout as an out-of-the-box feature. However, you can configure Jive to authenticate against a third-party SSO that will perform account lockout.
SSO	Jive includes support for SAML out of the box and can also be implemented as a customization from Jive's Professional Services team, a Jive partner, or an engineer of your choice. Be sure to read Getting Ready to Implement SAML SSO.
Delegated Authentication	When delegated authentication is enabled and configured, Jive makes a simple Web Service call out to the configured server whenever a user attempts to log in. This allows administrators to control the definition of users outside of the community. To learn more about this, see Configuring Delegated Authentication.

Authorization Features

Jive includes powerful built-in end user and admin permissions matrices, as well as customizable permissions. Depending on the assigned role, users can see or not see specific places and the content posted there. In addition, administrative permissions can be used to limit the access level of administrators. Jive administrators control user and admin permissions through the Admin Console. To learn more about how permissions work, see Managing Permissions.

Moderation and Abuse Features

Moderation	Jive administrators can enable moderation so that designated reviewers view and approve content before it is published in the community. This can be useful for places that contain sensitive information. In addition to content moderation, administrators can enable moderation for images, profile images, avatars, and user registrations. For more about moderation, see the Moderation section.
Abuse Reporting	Administrators can enable abuse reporting so that users can report abusive content items. To learn

	more about abuse reporting, see Setting Up Abuse Reporting.
Banning Users	Administrators can block a person's access to Jive so that they are no longer able to log in to the community. For example, if someone becomes abusive in their messages (or moderating their content is too time-consuming), administrators may choose to ensure that the user can no longer log in. Users can be banned through their login credentials or their IP address. Be sure to read Banning People for more information.
Interceptors	Interceptors can be set up to perform customizable actions on incoming requests that seek to post content. Administrators can set up interceptors to prevent specific users from posting content or to filter and moderate offensive words, anything from specific IP addresses, or the posting frequency of specific users. To learn more about how interceptors work, see Configuring Interceptors.

Encryption

HTTPS	HTTPS encryption is required for running Jive. Jive supports TLS 1.0 and up.
Encryption at Rest	Encryption at rest is available to North American customers as an addition.

Cookies

Jive uses HTTP cookies in several places in the application to provide a better user experience. To learn more about how the application uses cookies, be sure to read Jive and Cookies.

Note: The Jive Professional Services team can deliver security customizations if the out-of-the-box security features do not meet the specific requirements of your organization.

Jive and Cookies

Jive uses HTTP cookies in several places in the application to provide a better user experience.

Jive does not set third-party cookies as part of the core product offering; however, it is possible for you to configure the application so that third-party cookies are set. For example, you can configure the application to use a Web-tracking tool such as Google Analytics or WebTrends, each of whom may set a third-party cookie. To see a list of those cookies that may be set, be sure to read Other Cookies.

Jive does not set the "domain" attribute of an HTTP cookie.

Out of the box, Jive is configured to send only allowed, secure cookies. If your installation is not using secure cookies for some reason, see Setting Up Secure Cookies on page 323.

All Jive cookies that are set by the server (not via the client or browser) have the HttpOnly flag.

Jive sets the following cookies.

Note: Except where noted, none of the following cookies contains user-identifiable information. This behavior meets European Union privacy laws.

anonymous

Used only by the Gamification module. Tracks if the user is authenticated or not.

- Possible values: true or false.
- Expiration: one year.
- Encryption: none.
- Example: anonymous="false"

BIGipServer

Cookies prefixed with BIGipServer help to efficiently route internal traffic, and contain encoded addresses of internal Jive servers. These addresses are strictly internal, and cannot be used to connect to internal servers from the Internet. Altering the values of the cookie will not have any effect. For more information about these cookies, see the article Overview of BIG-IP persistence cookie encoding on the F5 Support site.

clickedFolder

This cookie is used in the Admin Console to persist the open/closed status of the current folder as used in various tree-view portions of the Admin Console.

- Possible values: string, true, or false.
- Expiration: at session end.
- Encryption: none.
- Example: clickedFolder="true"

highlightedTreeviewLink

This cookie is used in the Admin Console to persist the current folder as used in various tree-view portions of the Admin Console.

- Possible values: integer, the DOM ID of the clicked folder.
- Expiration: at session end.
- Encryption: none.

	• Example: highlightedTreeviewLink="23"
jive-cookie	This cookie is used in the Admin Console to temporarily persist an encrypted username/password when creating a bridge between two sites. The information in the cookie is first encrypted with AES/256 encryption and then Base64 encoded. • Possible values: string, Base64 encoded, encrypted username/password of remote site. • Expiration: at session end. • Encryption: yes. • Example: jive-cookie="YWFyb246MTMxNTU4MjUzNTI3MDoyZDUyODNmZj
jive_default_editor_mode	This cookie is used on the front-end for guest/anonymous users who choose to use an editor mode other than the default editor mode. • Possible values: string, advanced. • Expiration: 30 days. • Encryption: none. • Example: jive_default_editor_mode="advanced"
jiveLocale	This cookie is used on the front-end for guest/anonymous users who choose a locale setting. • Possible values: string, locale code. • Expiration: 30 days. • Encryption: none. • Example: jiveLocale="en_US"
jive.login.ts	Stores the time stamp of the user's last login. • Possible values: epoch time in ms • Expiration: at session end. • Encryption: none. • Example: 1387387736841
jive.mobile.redirect	This cookie retains the user's selection for opening content in the Jive Mobile Web app or the Jive Native App when using a mobile device. Currently supported for iOS devices only. • Possible values: WEB, NATIVE.

	• Expiration: one month. • Encryption: none.
jiveRegularLoginUserCookie	This cookie is used to auto-redirect the login screen to the built-in authentication page (if the value exists and is set). • Possible values: true. • Expiration: one month. • Encryption: none.
jive.saml.passive.tried	This cookie is used to mark when SAML passive authentication has already been attempted. • Possible values: true. • Expiration: 3600 seconds (one hour). • Encryption: none. • Example: jive.saml.passive.tried="true"
jive.security.context	This cookie is the authentication context for the user. • Possible values: the user's encrypted security context. • Expiration: 30 minutes unless refreshed. Same as the standard servlet container session timeout. • Encryption: AES 256. • Example: jive.security.context="SdRw2i/HXoh1+LwTBLFy3Q==.MzA3OQ=="
jive.server.info	This cookie is used on the front-end in combination with Content Distribution Networks (CDN) like Akamai to associate the user with a specific server (also known as "session affinity"). • Possible values: string, a combination of the serverName, serverPort, contextPath, localName, localPort, and localAddr. • Expiration: at session end. • Encryption: none. • Example: jive.server.info="serverName=community.example.com:server

jiveSSOLoginUserCookie	This cookie is used to auto-redirect the SSO screen to the built-in authentication page (if the value exists and is set). • Possible values: true. • Expiration: one month. • Encryption: none.
jiveTimeZoneID	This cookie is used on the front-end for guest/anonymous users who choose a timezone setting. • Possible values: string, timezone ID. • Expiration: 30 days. • Example: jiveTimeZoneID="234"
jive.user.loggedin	This cookie is used on the front-end in combination with Content Distribution Networks (CDN) to denote the status of the current request. • Possible values: string, true if the current request originates from a browser where the user is logged in. • Expiration: at session end. • Encryption: none. • Example: jive.user.loggedin="true"
jive_wysiwygtext_height	This cookie is used on the front-end to persist the height of the editor window across sessions. • Possible values: integer, the height in pixels of the editor after the user chooses to expand the editor window. • Expiration: one year. • Example: jive_wysiwygtext_height="500"
JSESSIONID	This cookie is used on the front-end and the Admin Console to identify a session. It is part of the Java Servlet specification. • Possible values: string, the unique token generated by Apache Tomcat. • Expiration: at session end. • Encryption: none. • Example: JSESSIONID="1315409220832msB9E3A98AA1F2005E61FA9

linkedin_oauth_	This cookie is used to communicate and authenticate with LinkedIn.
place_info	This cookie is used to temporarily store the tile configuration information when a user is configuring a tile that integrates with a third-party system, such as Salesforce. After the user clicks **Save** in the place template editing interface, the cookie is destroyed. • Expiration: after place template changes are saved. • Encryption: none. • Example: place_info="placetype %3A700%26placeid%3A5758"
skin.palette.preview	This cookie is used to preview the site with an unpublished template. • Possible values: ID (long value) of the template. • Expiration: long lived. 30 days. • Encryption: none. • Example: skin.palette.preview="1001"
SPRING_SECURITY_REMEMBER_ME_COOKIE	This cookie is used on the front-end as part of the security authentication process to denote whether or not the user wants to have their credentials persist across sessions. It is part of the Spring Security specification; details are available here. • Possible values: string, the Base64 encoded username and expiration time combined with an MD5 hex hash of the username, password, expiration time, and private key. • Expiration: defaults to 14 days. • Encryption: none. This is an MD5 hex hash. • Example: SPRING_SECURITY_REMEMBER_ME_COOKIE="YWFyb24

Setting Up Secure Cookies

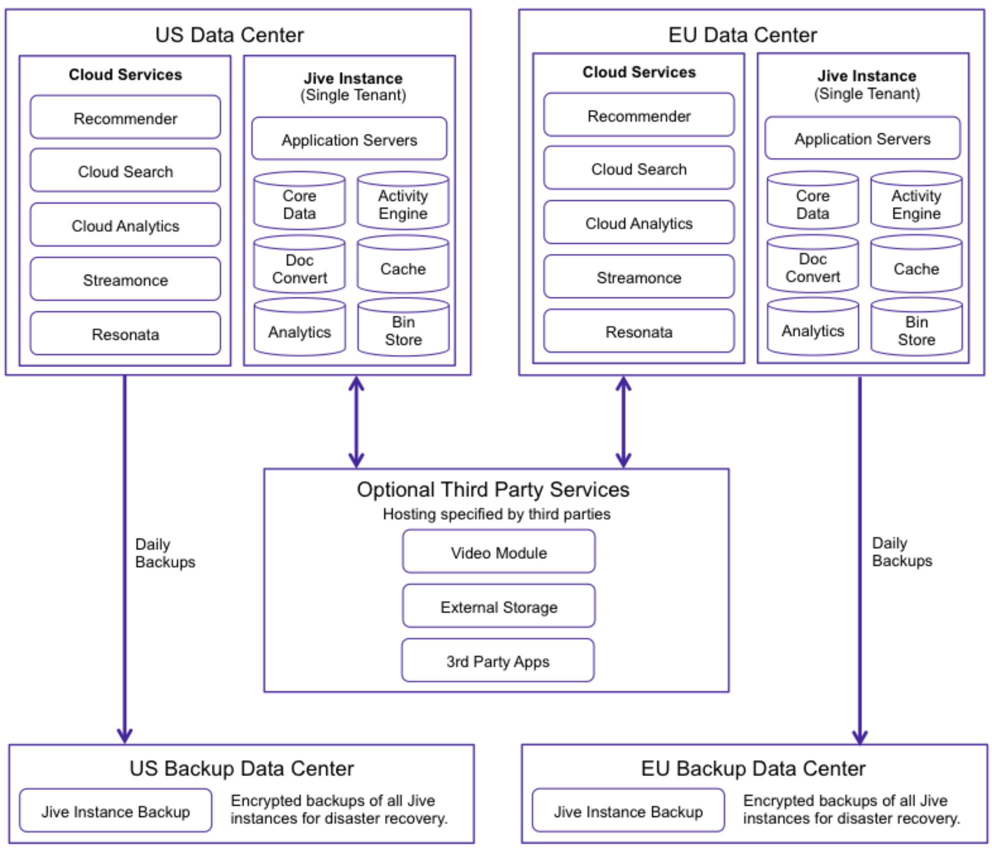
Out of the box, Jive sets the "secure" attribute for cookies that should only be sent via HTTPS connections. If your installation is not configured this way, here's how you can configure Jive to send only allowed, secure cookies.

1. Set the Jive system property "jive.cookies.secure" to the value "true". This results in all Jive-specific cookies (not including JSESSIONID) having the "secure" attribute set on the cookie (**Admin Console: System** > **Management** > **System Properties**).
2. Configure both Apache and Tomcat to only allow HTTPS connections. To understand these configurations, see Configuring SSL on the Load Balancer.
3. Configure Tomcat with the "secure" attribute set to "true" in the `server.xml` configuration file, specifically the "server/connector" element.

Security of Cloud-Delivered Services

A number of key Jive services, such as Search, Recommender, and Analytics, are cloud-delivered to your instance.

The architecture of these services is shown in the diagram below. For detailed information about how each service is secured, see the public and NDA versions of the Jive Security whitepaper.



Security Recommendations

These security recommendations depend on your community's specific configuration.

Caution: Each community can be configured differently. Because of this, not all of these recommendations apply to all communities. If you have any questions about these recommendations, please contact your Jive Software representative.

Security Recommendation:	Applies to:	Description:
Configure user login security	Jive-x	Login security can include throttling, Captcha, and password strength requirements. **For implementation details:** See Configuring Login Security and Configuring User Registration.
Enable SSO	Jive-n	A single-sign on solution can help you provide a consistent login experience for your users while providing identity management for your organization via a third-party vendor. Jive Software strongly recommends using a single sign-on solution for access to internal communities. In addition to the out-of-the-box SSO options in the application, our Professional Services team can create customizations to meet almost any single sign-on requirement. **For implementation details:** See the Single Sign-On section, or, if you need an SSO customization, contact your Jive Software account representative.
IP Whitelisting	Jive-x and Jive-n	IP address whitelisting is available for restricting access to either the entire site, or just the administration console. You can also use whitelisting to restrict access to certain locations, such as corporate offices. To access this feature, contact Support.

Security Recommendation:	Applies to:	Description:
Prevent spam in your community	Jive-x	Everyone hates spam, and it can also present security risks. Limit it in your community as much as you can. **For implementation details:** Preventing Spam includes several suggestions for dealing with spammers and preventing spam in your community, including a spam plugin that can connect to a third-party spam filtering tool. We also recommend reading the Spam Prevention Best Practices Guide in the Jive Customers group in Jive Community. (If you're a customer, we recommend joining this private group for useful community management content from Jive and fellow customers.)
Understand administrative permissions and how they work	Jive-x and Jive-n	Administrative permissions can be a powerful tool for limiting who can make changes to your community. **For implementation details:** See the Managing Administrative Permissions section.
Enable Anti-Virus Checking	Jive-x and Jive-n	Cloud communities automatically include a module that checks files for viruses before they can be uploaded to the community; for Hosted communities, this is an optional purchase.
If higher data security is needed, enable Encryption at Rest	Jive-x and Jive-n	Jive's Encryption at Rest module (an optional purchase) is our recommended solution for customers who need additional encryption to meet their security requirements. Complete infomation is available from Sales.