Jive Interactive Intranet

Cloud Administrator Guide

Administering Community with the Simplified Admin Console

Notices

For details, see the following topics:

Notices

This document is proprietary and confidential to Aurea and is available only under a valid non-disclosure agreement. No part of this document may be disclosed in any manner to a third party without the prior written consent of Aurea. The information in these materials is for informational purposes only and Aurea assumes no responsibility for any errors that may appear therein. Aurea reserves the right to revise this information and to make changes from time to time to the content hereof without obligation of Aurea to notify any person of such revisions or changes.

You are hereby placed on notice that the software, its related technology and services may be covered by one or more United States (“US”) and non-US patents. A listing that associates patented and patent-pending products included in the software, software updates, their related technology and services with one or more patent numbers is available for you and the general public’s access at https://markings.ip-dynamics.ai/esw/ (the “Patent Notice”) without charge. The association of products-to-patent numbers at the Patent Notice may not be an exclusive listing of associations, and other unlisted patents or pending patents may also be associated with the products. Likewise, the patents or pending patents may also be associated with unlisted products. You agree to regularly review the products-to-patent number(s) association at the Patent Notice to check for updates.

Aurea and Aurea Software are registered trademarks of Aurea Software, Inc. in the United States and/or other countries. Additional Aurea trademarks, including registered trademarks, are available at: https://www.aurea.com/legal/trademarks/. Jive is a registered trademark of Jive Software, Inc. in the United States and/or other countries. Additional Jive trademarks, including registered trademarks, are available at: https://www.jivesoftware.com/legal/.

Third-party acknowledgments

The following third-party trademarks may appear in one or more Jive guides:

- Amazon is a registered trademark of Amazon Technologies, Inc.
- Apache and Derby is a trademark of Apache Software Foundation.
- Chrome is a trademark of Google Inc.
- Eclipse is a registered trademark of the Eclipse Foundation, Inc.
- HP-UX is a registered trademark of Hewlett-Packard Development Company, L.P.
- IBM, AIX, DB2, and WebSphere are registered trademarks of International Business Machines Corporation.
- Intel and Pentium are registered trademarks of Intel Corporation in the U.S. and/or other countries.
- JBoss is a registered trademark, and CentOS is a trademark, of Red Hat, Inc. in the U.S. and other countries.
- Linux is a registered trademark of Linus Torvalds.
- Microsoft, Active Directory, Internet Explorer, SharePoint, SQL Server, Visual Studio, and Windows are registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.
- Mozilla and Firefox are registered trademarks of the Mozilla Foundation.
- Oracle and Java are registered trademarks of Oracle and/or its affiliates.
- Progress and OpenEdge are registered trademarks of Progress Software Corporation or one of its subsidiaries or affiliates in the U.S. and other countries.
- Red Hat and Red Hat Enterprise Linux are registered trademarks of Red Hat, Inc. in the U.S. and other countries.
- SAP and SAP NetWeaver are registered trademarks of SAP SE in Germany and in several other countries.
- SUSE is a registered trademark of SUSE, LLC.
- Ubuntu is a registered trademark of Canonical Limited in the United States and/or other countries.
- UNIX is a registered trademark of The Open Group in the United States and other countries.

All other marks contained herein are for informational purposes only and may be trademarks of their respective owners.

Table of Contents

Aurea global support

If you encounter a problem while using an Aurea product or require assistance with downloading the software or upgrading a product release, please, try to:

- Search the articles on the Aurea Knowledge Base for solutions to your issues.
- Search the product documentation and other product-related information that are also available on Support Central.

If you still cannot find a solution, open a ticket on Aurea Support Central. Information about the support organization is available on Support Portal as well.

You can also find the setup files on Support Portal.

For information about purchasing an upgrade or professional services, contact your account executive. If you do not know who your account executive is, or for other queries, contact us through our website.

1

Overview

Supported languages

For a list of languages supported in the Jive user interface, see Supported languages on page 11.

Release notes

To learn more about changes in Jive with each release, including the release notes, see the Jive Cloud space on Worx.

Previous help versions

If you want to see previous versions of the documentation, take a look at the following help from previous cloud releases:

- 2018.1 Community Manager Help
- 2017.1 Community Manager Help
- 2016.3 Community Manager Help
- 2016.2 Community Manager Help
- 2016.1 Community Manager Help
- 2015.3 Community Manager Help

Beta features

Any feature labeled in this Jive Cloud Documentation as a "Beta Feature" is provided to you for non-production, evaluation, and testing purposes only. Beta features are provided "AS-IS," "AS AVAILABLE," AND WITHOUT WARRANTY OF ANY KIND, AND ARE EXCLUDED FROM ANY APPLICABLE SLAS AND SUPPORT SERVICES. Beta features may be subject to different security and privacy commitments. Beta features may or may not become GA features, and their implementation may change in backward-incompatible ways. We may change or discontinue beta features at any time and without notice. If you do not agree to these terms, do not enable any beta features.

Jive is a social business software that integrates the most powerful capabilities of collaboration, community, and social networking software. We hope you find this documentation useful as you set up, configure, and use your new Jive community. Thank you for choosing Jive!

For details, see the following topics:

Trying Jive

If you are trying Jive for the first time with a trial version, here is a quick introduction to get you started.

Welcome, Jiver!

Your free 30-day trial version of Jive includes the full Jive Platform (not just a lite version) for an unlimited number of users. Due to the capabilities of the cloud-delivered infrastructure, you can start with several users and scale to hundreds of thousands without ever moving to a different system.

Jive most powerful features include personalized attention streams, collaboration, and discussion features, decision-making badging, and the ability to bring virtually *any* web content into your community to discuss it with your team. With our native mobile apps, you can access your community on the go anytime from your mobile device.

You can learn more from an active and passionate group of Jive users in the Worx community, which you can find at https://community.aurea.com/welcome.

See what's new

Set up a News page for the users to see at a glance what's trending and happening in your community. The Activity streams let users see what's Top & Trending and Most Recent.

Create your own streams

Create your custom streams on the fly and filter out the excessive community activity. Your custom streams allow you to focus your attention on what matters: a particular topic, place, or team. For example, you might have streams for Executive Blogs, My Current Project, Posts from My Team, Water Cooler, and Email Watches. You can also follow your favorite tags in your streams.

To create a new stream, click **New Stream** in the main navigation of your News page and use the stream builder to drag and drop from a list of people and places suggested for you, or search for specific content items.

You can also add people, places, and content items to your streams whenever you're scrolling through any streams or when you're browsing through Content, People, or Places. In addition, the Recommended features that you can see throughout the application help useful content, people, and places *find you*. For more information, see Create a New Stream in the User Guide.

Learn how to use Jive effectively

Learn to use Jive more effectively with the Getting Started guides that walk you through typical Jive activities. Just click  next to your avatar and then **Get Started** in the left sidebar.

Collaborate on web content with Jive Anywhere

Bring virtually any web content quickly and easily into your community by clicking the **Jive Anywhere** button in your browser (learn how to set this up in the Jive Anywhere Guide). For example, you might want to discuss in Jive a specific record in a CRM system, a candidate's profile on LinkedIn, or a research report on the web. From any page, click the **Jive Anywhere** button, @mention the relevant folks, and then get down to social business. Stop the endless email chains and meetings.

You can also tie Jive Anywhere to more than one Jive community so that you're sharing your content with the right audience. For more information, see Adding Communities to Jive Anywhere in the Jive Anywhere Guide.

Drive business decisions

Turn a Jive conversation into a real business decision. Using actions, you can mark comments or replies as a Decision, Success, Final, or for Action. Marking for Action allows you to assign content items to yourself or others to review before Resolving the action. Content owners can mark an item as Official, Final, Success, for Action, or Outdated. Visual badges for these states help others quickly see what has been decided, assigned to someone, or finalized. Your community manager may need to enable this feature if you don't see it already in your community. For more information about this feature, see Marking Decisions in the User Guide.

Set up places

Create places in your community (if you have permissions) and choose from a list of preconfigured templates. Templates are designed to support real-world collaboration goals including a Vendor Collaboration place for partnering with an external talent team and a Support Team Backchannel for private discussions about customer cases. If you're looking for something more general, you can try the Team Collaboration place template.

You can also add new pages to any places that you own if your community manager has enabled this feature. New place pages are fully customizable with configurable tiles for greater design flexibility and utility.

Know your impact

The Impact Metrics feature provides insight into how documents, discussions, and blog posts are received by your community, including their Reach, Impact, and Sentiment. For more information about this feature, see Using impact metrics in the User Guide.

Share and extend the platform

Community managers can hook up Google Drive and Gmail, Salesforce, Facebook, and Twitter so you can see and discuss updates from those services right in your Jive community, and share your community content with external social channels.

Scale securely with Jive

With your trial version, you can start with a small team and scale to a massive global workforce without skipping a beat. Besides, you automatically get all the latest application features and innovations, while ensuring data security and compliance.

Unlike other services that commingle your data with other companies' data, your data is isolated when you use Jive. And while some vendors hold your data hostage until you pay, you always own your data with Jive. If you want to stop using Jive at any point, you can take your data with you.

Jive Cloud is based on the same platform that runs some of the biggest networks in the world and is proven to scale to tens of millions of users securely. For more information about security in Jive, see the Trust Jive article at http://www.jivesoftware.com/social-business-software/jive-security/.

Learn what's new in this release

You can learn about the latest features in What's new? on page 13.

I'm Convinced! Buy Jive application

So you've tried a Jive community and want to buy it? To get in touch, just send an email to sales@jivesoftware.com. Or contact your regional Sales office by phone: you'll find our locations around the world at https://www.jivesoftware.com/about-jive/contact.

And thanks for using Jive to change your work style.

Supported languages

The main application has been translated into a number of languages. Users with one of these languages set as their browser version automatically see the translated application. Users can also override their browser setting in their user preferences.

Supported languages

The main application supports the following languages:

- Arabic
- Chinese—Simplified
- Chinese—Traditional
- Czech
- Danish

- Dutch
- English
- Finnish
- French
- German
- Greek
- Hebrew
- Hungarian
- Italian
- Japanese
- Korean
- Norwegian
- Polish
- Portuguese—Brazilian
- Russian
- Spanish (Latin American, Neutral, International, Castilian)
- Swedish
- Thai

Jive supports right-to-left languages as described below.

Right-to-left language support

Jive includes Hebrew and Arabic translations of the interface and support for other right-to-left (RTL) languages as follows.

- The content editor accepts RTL text.
- When a right-to-left locale is selected, text in documents, discussion prompts, comments, replies, tiles, widgets, and in content of other types flows from right to left.
- The page flow is reversed. For example, controls and field labels are right-aligned rather than left-aligned.

Support includes the Core Jive web application displayed to end users, including the following:

- Responsive mobile on a mobile browser (but not the mobile apps)
- Search
- Analytics reporting and impact stats
- Events
- Video
- Gamification user UI

The following areas, integrations, and features are not supported:

- Document previews
- Jive mobile apps (but the responsive view of the application on a mobile browser is supported)
- Jive for Office and Jive for Outlook
- Jive Anywhere
- External storage provider solutions like Box, SharePoint, Google Docs, and Dropbox
- Spell checking

What's new?

The latest Cloud release includes significant new fixes and enhancements.

You can see the Jive Cloud space on Worx for details.

Note: For a list of updates in previous releases, see Previous help versions.

System requirements

Make sure these system requirements are met before using the application.

Supported browsers

Jive works with most current web browsers. Note that if you need to use Content Editor features, such as cut and paste, script access to the clipboard must be enabled.

- Microsoft Internet Explorer 11.

  Note: Compatibility mode is not supported.

- Microsoft Edge* (Chromium-based) and Edge Legacy* (HTML-based).
- Apple Safari* (on Macs only).
- Mobile Safari on iPhone and iPad for iOS 11 and later. (For a browser-independent native iOS phone app, be sure to look for the Jive Daily: Intranet on the go app, if your community uses it, in the App Store.)
- Mobile Chrome on Android devices for Android 8 and later. (For a browser-independent native Android phone app, be sure to look for the Jive Daily: Intranet on the go app, if your community uses it, in Google Play.)
- Mozilla Firefox*.
- Google Chrome*.

* Google Chrome, Mozilla Firefox, Apple Safari, and Microsoft Edge browsers are released frequently. Jive Software makes every effort to test and support the latest version.

Note: The recommended minimum screen resolution for desktop devices is 1024 x 768. Results may vary if you use zoom to adjust your view to levels other than 100%.

Important notes and restrictions:

- Chromebook is not supported.
- Beta versions of web browsers are not supported, but they are quickly added to the supported list after they're formally released.
- Apps are not supported on mobile devices. These features may not work correctly on mobile devices.

Required Jive domains and firewall rules

For the Jive application to function properly, it needs to connect to external domains from the client side outside the primary instance domain. This topic lists such external domains that require an active connection.

Note:

- Apps, add-ons, tiles, stream integrations, and other third-party integrations may require access to additional domains not listed here.
- When creating firewall rules, both ports `80 (HTTP)` and `443 (HTTPS)` must always be allowed for each domain, unless otherwise noted.

Jive Core application (Cloud only)

- https://assets.jiveon.com/
- https://assets2.jiveon.com
- https://static.jiveon.com/
- https://cdn.polyfill.io/

If your organization utilizes whitelisting to connect your Jive instance to your organization's services behind your firewall, you need to whitelist the following IPs. This may be required, for example, if your Jive community is configured for LDAP directory syncing, and you utilize a whitelist on your firewall to allow your Jive community to connect to it.

- AWS US-East-1 Region: 34.192.45.122, 34.198.91.162, 34.231.78.214, 34.225.172.123, 34.193.143.104, 52.55.123.87, 52.20.222.9, 34.230.231.2, 34.197.60.63, 52.207.30.159, 3.213.1.211
- AWS EU-West Region: 54.154.171.198, 108.129.50.14, 52.31.199.172, 34.247.7.187, 34.252.244.183, 52.211.222.108, 63.33.30.202

AWS CloudFront CDN for Jive Core (Cloud only)

Jive Core relies on Amazon Web Services CloudFront content delivery network (AWS CloudFront CDN) for content distribution. You can download the current list of AWS Cloud Front IP ranges in JSON format provided by AWS at http://d7uri8nf7uskq.cloudfront.net/tools/list-cloudfront-ips at any time you need.

For example, the list in December 2019 includes the following IP ranges (in JSON format):


```
{"CLOUDFRONT_GLOBAL_IP_LIST": ["144.220.0.0/16",
"52.124.128.0/17", "54.230.0.0/16", "54.239.128.0/18",
"52.82.128.0/19", "99.84.0.0/16", "204.246.172.0/24",
"205.251.192.0/19", "54.239.192.0/19", "70.132.0.0/18",
"13.32.0.0/15", "13.224.0.0/14", "13.35.0.0/16",
"204.246.164.0/22", "204.246.168.0/22", "71.152.0.0/17",
"216.137.32.0/19", "205.251.249.0/24", "99.86.0.0/16",
"52.46.0.0/18", "52.84.0.0/15", "204.246.173.0/24",
"130.176.0.0/16", "64.252.64.0/18", "204.246.174.0/23",
"64.252.128.0/18", "205.251.254.0/24", "143.204.0.0/16",
"205.251.252.0/23", "204.246.176.0/20", "13.249.0.0/16",
"54.240.128.0/18", "205.251.250.0/23", "52.222.128.0/17",
"54.182.0.0/16", "54.192.0.0/16"],
"CLOUDFRONT_REGIONAL_EDGE_IP_LIST": ["13.124.199.0/24",
"34.226.14.0/24", "52.15.127.128/26", "35.158.136.0/24",
"52.57.254.0/24", "18.216.170.128/25", "13.52.204.0/23",
"13.54.63.128/26", "13.59.250.0/26", "13.210.67.128/26",
"35.167.191.128/26", "52.47.139.0/24", "52.199.127.192/26",
"52.212.248.0/26", "52.66.194.128/26", "13.113.203.0/24",
"99.79.168.0/23", "34.195.252.0/24", "35.162.63.192/26",
"34.223.12.224/27", "52.56.127.0/25", "34.223.80.192/26",
"13.228.69.0/24", "34.216.51.0/25", "3.231.2.0/25",
"54.233.255.128/26", "18.200.212.0/23", "52.52.191.128/26",
"52.78.247.128/26", "52.220.191.0/26", "34.232.163.208/29"]}
```

	For more information, see *Locations and IP Address Ranges of CloudFront Edge Servers* in the Amazon CloudFront Developer Guide at https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/LocationsOfEdgeServers.html.
Jive Daily: Intranet on the go (Mobile app)	• `https://api.embed.ly` • `https://fabric.io` • `https://cdn.mxpnl.com/` • `https://api.giphy.com/` • `https://api2.appsflyer.com/` • `https://api.qordoba.com/`
Video module (Powered by Lexmark	• `https://video-svc.jivesoftware.com/` • `http://*.edgecastcdn.net/`

Perceptive Media (Perceptive)	• https://*.twistage.com/ • https://*.alphacdn.net • https://*.omegacdn.net • https://*.betacdn.net • https://i.embed.ly/
	Important: Jive is migrating from the Perceptive Media provider to the Jive video provider. Options and configuration relevant only for the Perceptive Media provider are marked with (Perceptive). They will be removed once the migration is finished.
Jive Rewards (Cloud only)	• https://rewards.jivesoftware.com • https://rewards.imgix.net/
New Relic (Cloud)	• https://js-agent.newrelic.com/ • https://bam.nr-data.net/
StreamOnce	• https://streamonce.prod.jivehosted.com

Cloud Search service	• US customers only:
	  • search-ingress-adapter.aws-us-east-1-prod.svc.jive-hosted.com
	  • search-query.aws-us-east-1-prod.svc.jivehosted.com
	• EU customers only:
	  • search-ingress-adapter.aws-eu-west-1-prod.svc.jive-hosted.com
	  • search-query.aws-eu-west-1-prod.svc.jivehosted.com

Cloud Analytics service	• US customers only:
	  • ca-ingress.aws-us-east-1-prod.svc.jivehosted.com
	  • ca-cmr.aws-us-east-1-prod.svc.jivehosted.com
	  • ca-query.aws-us-east-1-prod.svc.jivehosted.com
	• EU customers only:
	  • ca-ingress.aws-eu-west-1-prod.svc.jivehosted.com
	  • ca-cmr.aws-eu-west-1-prod.svc.jivehosted.com
	  • ca-query.aws-eu-west-1-prod.svc.jivehosted.com

2

Setting up community

This section introduces the basic configuration that is required to start using your Jive community site.

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

For details, see the following topics:

- Required Jive domains and firewall rules
- Setting up your profile
- Starting the Admin Console
- Enabling Personal Insights
- Creating community structure
- Jive places: spaces, groups, and projects
- Planning customized community pages
- Theming community
- Managing Support Center
- Enabling new features in your community
- Renaming the root space
- Setting up locale and time zone
- Inviting people to community
- Customizing News page

Required Jive domains and firewall rules

For the Jive application to function properly, it needs to connect to external domains from the client side outside the primary instance domain. This topic lists such external domains that require an active connection.

Note:

- Apps, add-ons, tiles, stream integrations, and other third-party integrations may require access to additional domains not listed here.
- When creating firewall rules, both ports `80 (HTTP)` and `443 (HTTPS)` must always be allowed for each domain, unless otherwise noted.

Jive Core application (Cloud only)

- https://assets.jiveon.com/
- https://assets2.jiveon.com
- https://static.jiveon.com/
- https://cdn.polyfill.io/

If your organization utilizes whitelisting to connect your Jive instance to your organization's services behind your firewall, you need to whitelist the following IPs. This may be required, for example, if your Jive community is configured for LDAP directory syncing, and you utilize a whitelist on your firewall to allow your Jive community to connect to it.

- AWS US-East-1 Region: 34.192.45.122, 34.198.91.162, 34.231.78.214, 34.225.172.123, 34.193.143.104, 52.55.123.87, 52.20.222.9, 34.230.231.2, 34.197.60.63, 52.207.30.159, 3.213.1.211
- AWS EU-West Region: 54.154.171.198, 108.129.50.14, 52.31.199.172, 34.247.7.187, 34.252.244.183, 52.211.222.108, 63.33.30.202

AWS CloudFront CDN for Jive Core (Cloud only)

Jive Core relies on Amazon Web Services CloudFront content delivery network (AWS CloudFront CDN) for content distribution. You can download the current list of AWS Cloud Front IP ranges in JSON format provided by AWS at http://d7uri8nf7uskq.cloudfront.net/tools/list-cloudfront-ips at any time you need.

For example, the list in December 2019 includes the following IP ranges (in JSON format):


```
{"CLOUDFRONT_GLOBAL_IP_LIST": ["144.220.0.0/16",
"52.124.128.0/17", "54.230.0.0/16", "54.239.128.0/18",
"52.82.128.0/19", "99.84.0.0/16", "204.246.172.0/24",
"205.251.192.0/19", "54.239.192.0/19", "70.132.0.0/18",
"13.32.0.0/15", "13.224.0.0/14", "13.35.0.0/16",
"204.246.164.0/22", "204.246.168.0/22", "71.152.0.0/17",
"216.137.32.0/19", "205.251.249.0/24", "99.86.0.0/16",
"52.46.0.0/18", "52.84.0.0/15", "204.246.173.0/24",
"130.176.0.0/16", "64.252.64.0/18", "204.246.174.0/23",
"64.252.128.0/18", "205.251.254.0/24", "143.204.0.0/16",
"205.251.252.0/23", "204.246.176.0/20", "13.249.0.0/16",
"54.240.128.0/18", "205.251.250.0/23", "52.222.128.0/17",
"54.182.0.0/16", "54.192.0.0/16"],
"CLOUDFRONT_REGIONAL_EDGE_IP_LIST": ["13.124.199.0/24",
"34.226.14.0/24", "52.15.127.128/26", "35.158.136.0/24",
"52.57.254.0/24", "18.216.170.128/25", "13.52.204.0/23",
"13.54.63.128/26", "13.59.250.0/26", "13.210.67.128/26",
"35.167.191.128/26", "52.47.139.0/24", "52.199.127.192/26",
"52.212.248.0/26", "52.66.194.128/26", "13.113.203.0/24",
"99.79.168.0/23", "34.195.252.0/24", "35.162.63.192/26",
"34.223.12.224/27", "52.56.127.0/25", "34.223.80.192/26",
"13.228.69.0/24", "34.216.51.0/25", "3.231.2.0/25",
"54.233.255.128/26", "18.200.212.0/23", "52.52.191.128/26",
"52.78.247.128/26", "52.220.191.0/26", "34.232.163.208/29"]}
```

	For more information, see *Locations and IP Address Ranges of CloudFront Edge Servers* in the Amazon CloudFront Developer Guide at https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/LocationsOfEdgeServers.html.
Jive Daily: Intranet on the go (Mobile app)	• `https://api.embed.ly` • `https://fabric.io` • `https://cdn.mxpnl.com/` • `https://api.giphy.com/` • `https://api2.appsflyer.com/` • `https://api.qordoba.com/`
Video module (Powered by Lexmark	• `https://video-svc.jivesoftware.com/` • `http://*.edgecastcdn.net/`

Perceptive Media (Perceptive)	• https://*.twistage.com/ • https://*.alphacdn.net • https://*.omegacdn.net • https://*.betacdn.net • https://i.embed.ly/
	Important: Jive is migrating from the Perceptive Media provider to the Jive video provider. Options and configuration relevant only for the Perceptive Media provider are marked with (Perceptive). They will be removed once the migration is finished.
Jive Rewards (Cloud only)	• https://rewards.jivesoftware.com • https://rewards.imgix.net/
New Relic (Cloud)	• https://js-agent.newrelic.com/ • https://bam.nr-data.net/
StreamOnce	• https://streamonce.prod.jivehosted.com

Cloud Search service	• US customers only:
	  • search-ingress-adapter.aws-us-east-1-prod.svc.jive-hosted.com
	  • search-query.aws-us-east-1-prod.svc.jivehosted.com
	• EU customers only:
	  • search-ingress-adapter.aws-eu-west-1-prod.svc.jive-hosted.com
	  • search-query.aws-eu-west-1-prod.svc.jivehosted.com

Cloud Analytics service	• US customers only:
	  • ca-ingress.aws-us-east-1-prod.svc.jivehosted.com
	  • ca-cmr.aws-us-east-1-prod.svc.jivehosted.com
	  • ca-query.aws-us-east-1-prod.svc.jivehosted.com
	• EU customers only:
	  • ca-ingress.aws-eu-west-1-prod.svc.jivehosted.com
	  • ca-cmr.aws-eu-west-1-prod.svc.jivehosted.com
	  • ca-query.aws-eu-west-1-prod.svc.jivehosted.com

Setting up your profile

One of the first things you do as the community manager or administrator is setting up your user profile. By adding profile information, you create an example for other new users.

Fastpath: User interface: Your Avatar (in the upper right corner) > Edit Profile

- Add a photo to 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 is displayed next to items you are associated with, such as the content you create. Note that some images look better than others in small size.
- Add information about yourself. People are able to find yours and others profiles when they search for keywords, so it is a good idea to use words in your biography and expertise sections that people might search for.

For more information on setting up user profiles, see Set up your profile in the User Guide.

Starting the Admin Console

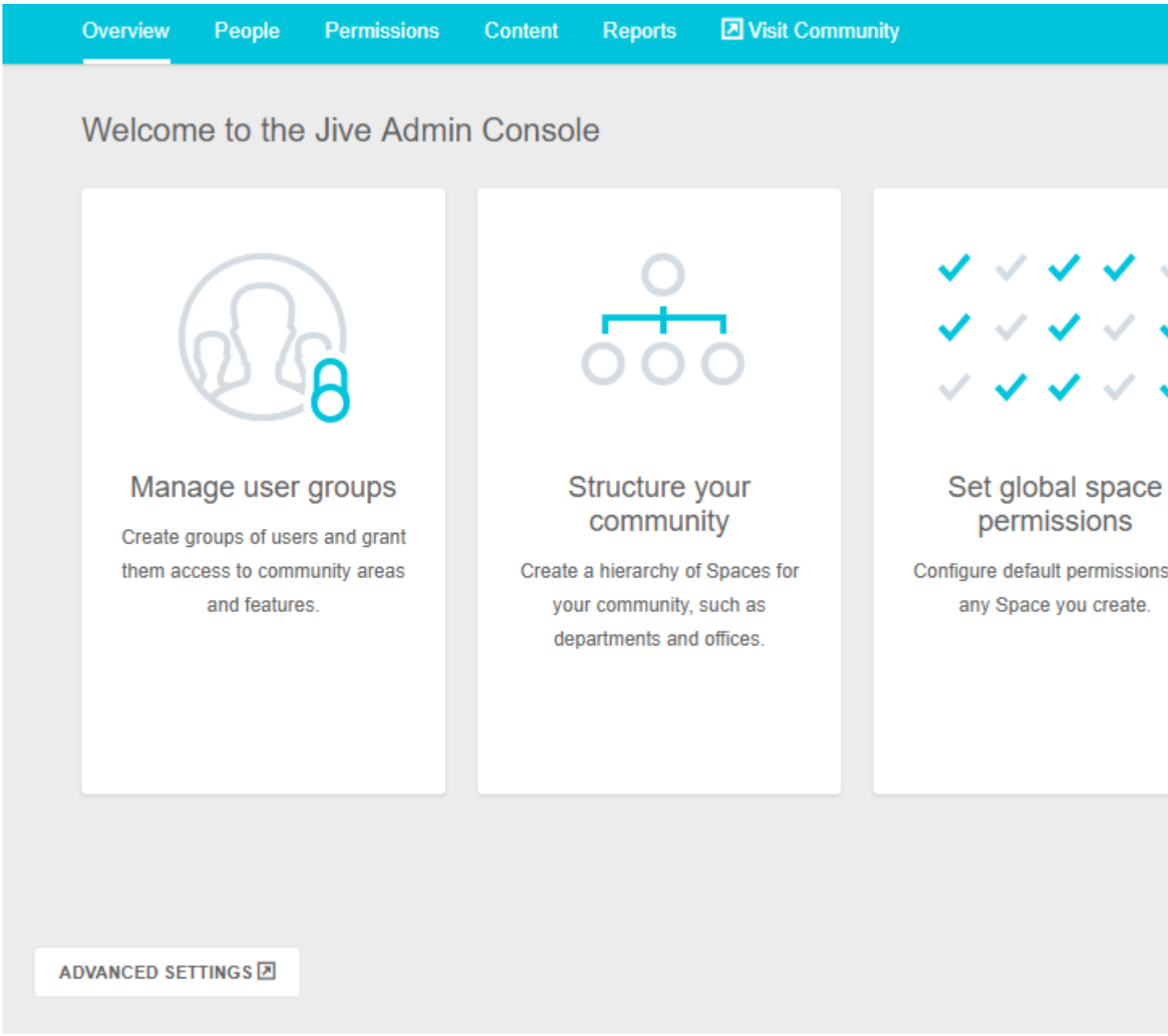
The Admin Console is an administration interface used to control and manage the Jive community site. As a community manager or administrator, you can access the

Admin Console to manage your Jive community settings, permissions, content (such as documents, discussions, and blogs), and people.

The Admin Console has two interfaces:

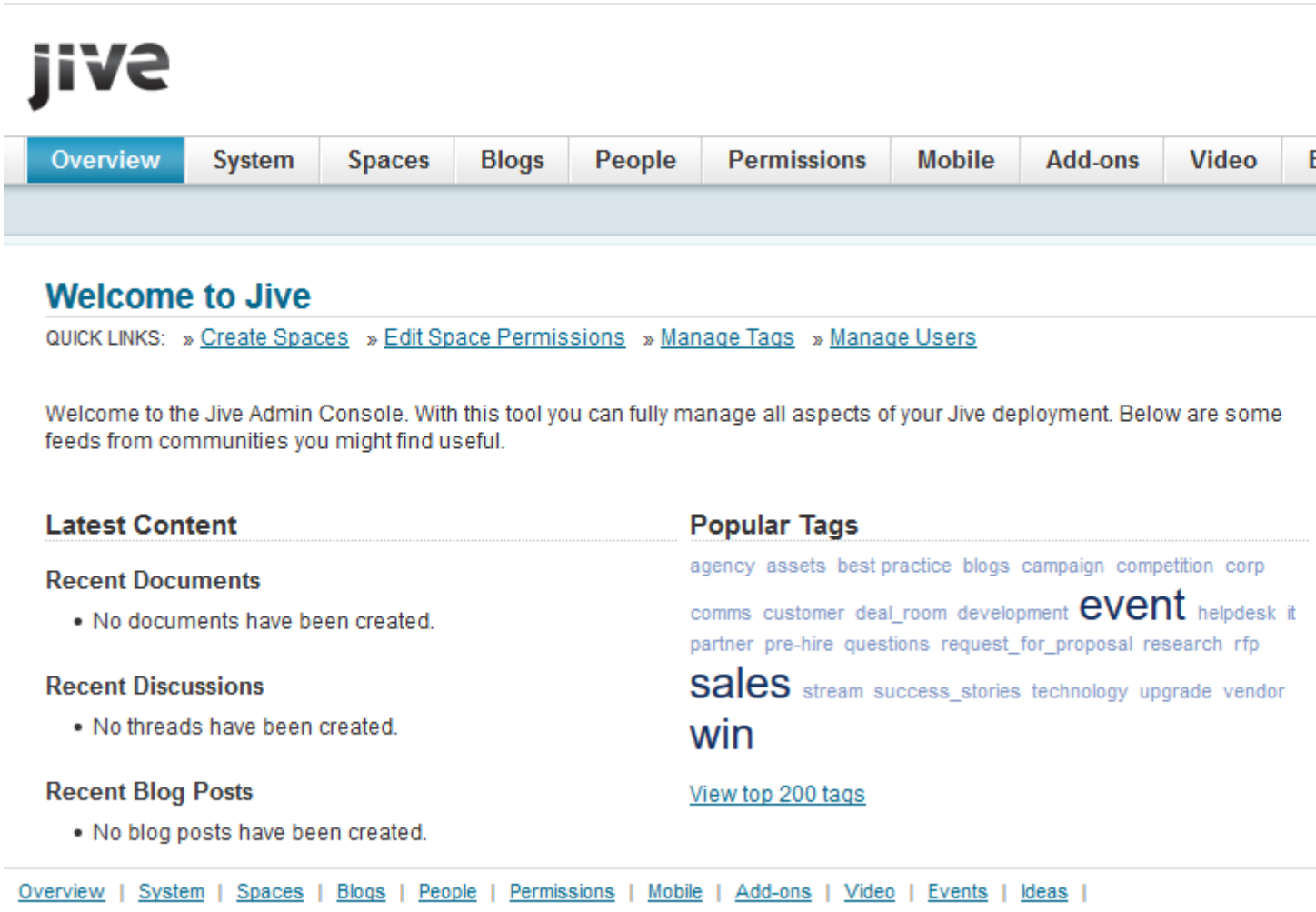
- Admin Console contains the most commonly used configuration options. It is the simplified subset of the Advanced Admin Console functionality.

Figure 1: The Admin Console



- Advanced Admin Console contains the all community configuration options.

Figure 2: Advanced Admin Console



Opening the Admin Console

To open the Admin Console from your community:

- To open the Admin Console, click your avatar in the upper right corner of the page and select **Admin Console** from the menu.

  Note that the Admin Console may be disabled for your community. In this case, this opens the Advanced Admin Console.

- To open the Advanced Admin Console from the Admin Console, click **Advanced Settings** in the bottom-left corner of the page.

To return to the user interface of your community:

- Click **Visit Community** in the main menu of the Admin Console.
- Click **Visit Site** in the upper right corner of the Advanced Admin Console).

Enabling or disabling the Simplified Admin Console

The feature option for enabling or disabling the simplified Admin Console interface is called **Simplified Admin Console**. For more information about enabling or disabling the feature, see Enabling or disabling the Simplified Admin Console on page 25.

Enabling or disabling the Simplified Admin Console

By default, the Simplified Admin Console is enabled in the community. If required, you can disable it.

Fastpath:

- **Admin Console** > **Overview** > **New Features Available**

For more information about the Admin Console interfaces, see Starting the Admin Console on page 22.

To disable or enable the Simplified Admin Console:

1. Go to the configuration page:
   - **Admin Console** > **Overview** > **New Features Available**
2. To disable the interface, select **Disabled** next to **Simplified Admin Console**.
3. To enable the interface, select **Enabled** next to **Simplified Admin Console**.
4. Click **Save**.

Enabling Personal Insights

Personal Insights help the community users to gain visibility into their contributions. With the feature enabled, users can learn how the community is responding to the content they created.

Fastpath: **Admin console: System** > **Settings** > **Analytics**

Note: Note that only the data of the current and previous two calendar years is available in Personal Insights. For more information, see Update to our Jive Analytics Data Retention Policy on Worx.

To enable Personal Insights:

1. In the Admin Console, go to **System** > **Settings** > **Analytics** , and then select the **Personal Insights** tab.

Note: You need at least the Manage Community administrative permission. For more information about permissions, see Overview of System Administration permission levels on page 114.

2. To enable Personal Insights on the profile page for all community members, select **Enabled** in **Personal Insights Settings**.
3. To **Allow everyone to view everyone else's Personal Insights**, select **Enabled** in the section.
4. Click **Save** to save the settings.

Creating community structure

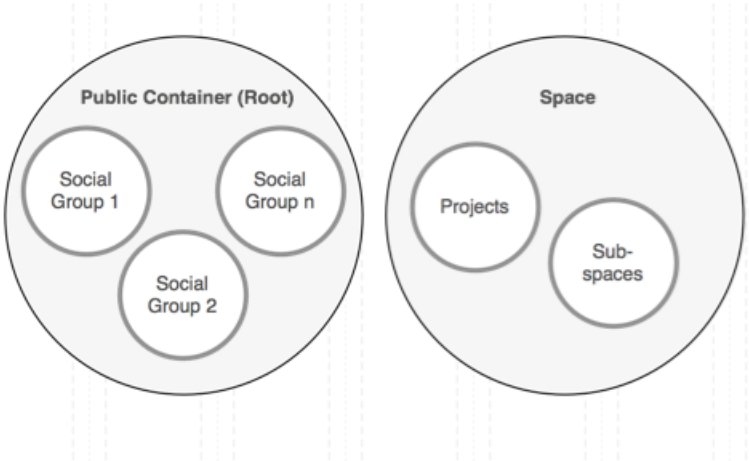
Creating a structure for content is one of the most important things you do to get your community started. Because people post content in various places, the places you create should help your users intuitively understand where to post (and find) content.

For example, you might organize the spaces to reflect the organization of the company itself including spaces like HR, Accounting, and Research.

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 do not have a hierarchical structure. Consequently, 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:



It is especially important when you are 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. The settings inherited at the time of creation are used as a starting point but can be modified later.

For more information about creating spaces, see Designing space hierarchies on page 145 and Creating new spaces from the Admin Console on page 150.

Jive places: spaces, groups, and projects

A place in Jive is essentially a container that houses all the collaborative content for a certain subject or team. There are three types of places: **Spaces**, **Groups**, and **Projects**. The differences between them can sometimes be confusing, so here're the basics of each one.

Spaces

Spaces are built in a hierarchy, with the ability to have a network of multi-level sub-spaces underneath them. They also use permissions, set by community administrators, to define who can see and do different things in the space. Permissions get inherited by any sub-spaces unless they are customized for that space, so if a user can do something in one space, this user can do it in the sub-spaces as well (unless the permissions have been customized). Any type of content can be created in a space, unless it has been turned off for a particular space by community administrators. Due to their hierarchical nature, spaces are typically used to represent organizations and departments within a company, and other concepts that require a network of places linked together.

For more information about creating spaces, see Designing space hierarchies on page 145 and Creating new spaces from the Admin Console on page 150.

Social groups

Groups, or *social groups*, are isolated containers within a community; they have no ties to other places and cannot have sub-groups. Permissions are managed on a per-group basis by the original group creator or the admins selected for the group, or both. Groups can also house any type of content unless one or more is turned off by community administrators. Because they are a freely created containers, groups get used most often for topic-specific collaboration, rather than something general to a team. They also get used for collaboration between specific teams or different departments that often work together closely and rely on each other.

For more information, see Using content and Types of groups in the User Guide.

Projects

Projects can only reside within a space or a group; they cannot stand alone. However, they can still house any type of content unless one or more is turned off by community administrators. Permissions get inherited from the place in which the project was created. Projects also get created with a Start Date and an End Date and come with additional titles on their pages that display the progress being made in the project (if the project administrator keeps them up to date). Projects are generally used for short-term projects, which users need to collaborate on and house the content for in a single area.

For more information, see Using projects and tasks in the User Guide.

What to use

Use a space if you:

- Need to share information about your department, program or initiatives with the rest of the organization/larger audience
- Need to add permissions controlling who can create which kinds of content in your place
- Need to create a hierarchical set of places
- Need permissions for your place to be managed centrally

Create a group if you:

- Want to collaborate privately with your team or project team
- Want to invite individuals to collaborate, and don't need centrally managed permissions
- Want to invite people from outside the organization to access your place

Comparison of place properties

	Spaces	Groups	Projects
Hierarchical?	Yes	No	No
Can be private?	Yes, via permissions	Yes, via group settings.	Depends on parent place
Access permissions	Defined in the Admin Console. Inherited by sub-spaces	Defined in group settings. No inheritance	Inherited from containing place. Not customizable
Create permissions	Defined in the Admin Console. Inherited by sub-spaces	Any user	Inherited from containing place. Not customizable

	Spaces	Groups	Projects
Content allowed	Any; may be customized or restricted, or both by community administrators	Any; may be customized or restricted, or both, by community administrators	Any; may be customized or restricted, or both, by community administrators
Best uses	Large-scalecollaborative needs with sub-space ability, such as those of an entire department or office, or an expansive topic	Smaller-scale collaborative needs either by a specific audience or a more specialized topic	Short term area to collaborate on a finite topic

Planning customized community pages

There are several locations in Jive where you can customize a page with images and information, by using either tiles or widgets as building blocks.

You can customize pages in the following locations:

- The **News page** of the entire community. For more information, see Customizing News page on page 52.
- The **Home page** of the entire community, if it is enabled.

  Important: We do not recommend that you use widgets and widgetized Overview pages (including the Home page) in your community.

- The **Your View page**, if it is enabled in your community.
- The landing page of a place: an **Activity page** or an **Overview page** (place widgets must be enabled).

  Important: We do not recommend that you use widgets and widgetized Overview pages (including the Home page) in your community.

- A **custom page** added to a place if Pages are enabled in your community and the Overview page has been disabled for the place.

Tiles and widgets like content blocks help you lay out certain pages in your community. Tiles are the default way to do this, but if you have widgets enabled, you can choose them instead. Use the following table to determine which model is available for you to use.

The following table shows where you can use tiles, and where you can use widgets.

Page	Tiles	Widgets
Community Home Page		
Your View		
Place: Activity page		

Page	Tiles	Widgets
Place: Overview page		
Place: Custom pages		

Theming community

The Themes interface gives you the ability to create a professionally-designed community with just a few clicks. By using the interface, you can customize your community with your organization unique colors and logo, or use a predefined theme included with Jive, such as Bamboo or Winter. You can also export and import customized themes.

Fastpath: User interface: Your Avatar > Themes

Community managers and users with Customize Site permissions can use the out-of-the-box theming feature. These users have the Themes option available under their user menu in the upper right corner of the user interface.

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 various interface elements, such as text, background colors, and logo image. These changes affect all pages in your community.

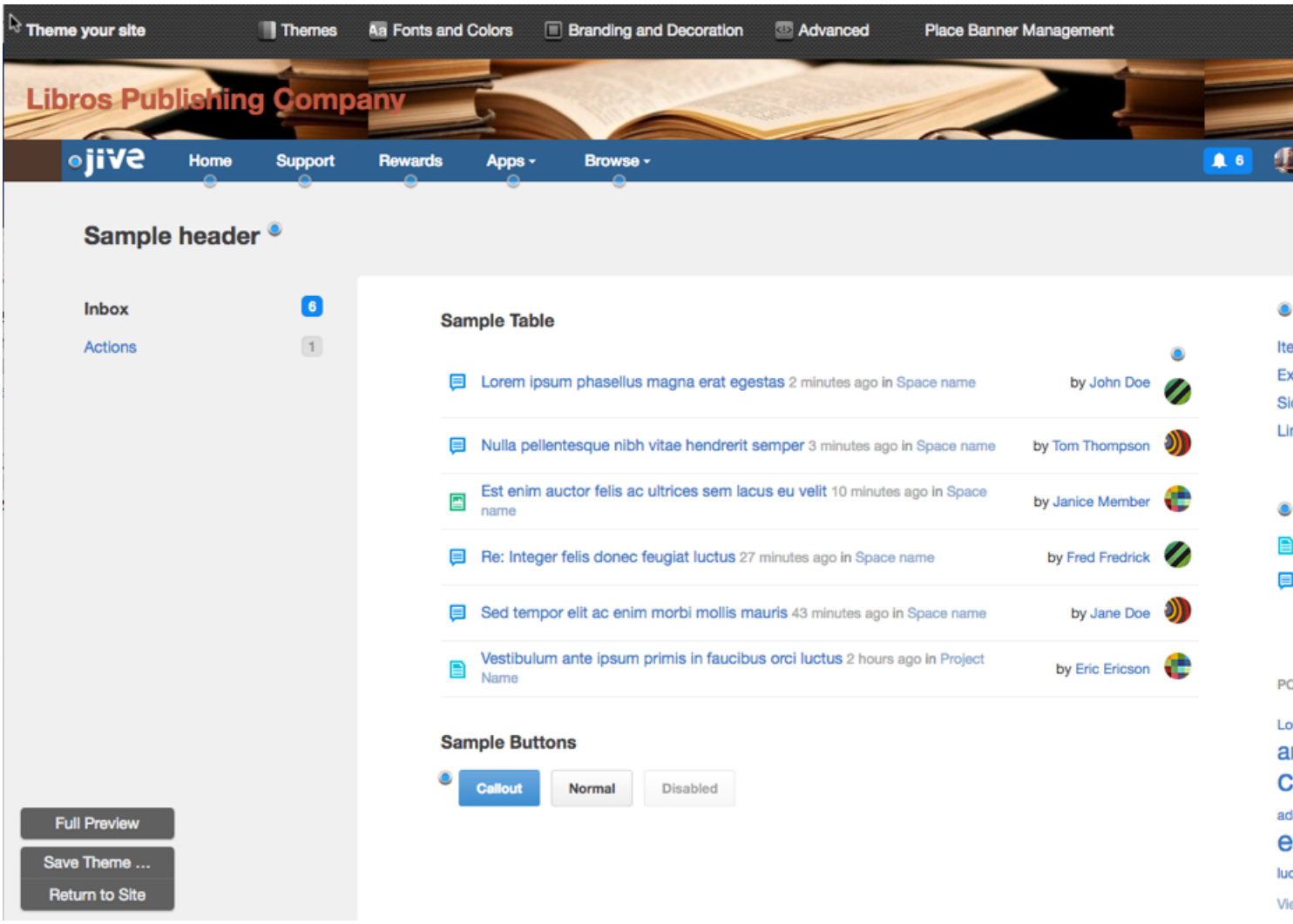
Note that only users with Manage Community or Customize Site permissions can see the Themes option under their user menu in the upper right corner of the user interface. You can review what you can change by using out-of-the-box theming in Theming options reference on page 33.

Fastpath: User interface > Your avatar > Themes

To open the theming interface:

- Click on your avatar in the upper-right corner and select **Themes**.

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



To customize your theme:

1. Make changes by clicking the blue dots next to interface components. You can see an instant preview of the updates.
2. Use predefined themes as templates by selecting a theme on the Themes tab. Then use the theme as-is or make further changes by clicking the blue dots next to interface elements. For more information, see Using predefined themes on page 32.
3. Use the Advanced tab to change your header and navigation style. Options include a thin navigation bar that stays pinned to the top while users scroll pages (Reduced), a more spacious navigation bar and header area combo (Basic), or a fully customizable header or footer (Custom).
4. Enable Custom Links to create custom navigation buttons in your navigation bar. For more information, see Creating custom links in the main menu on page 35.
5. Get a full preview at any time for a more thorough look at your changes. You need to save your changes before previewing.

6. Save your new theme as draft to continue working with it later by using the Save Theme option. This saves your work so that you can continue making theme changes later without affecting your current community.
7. Publish your saved theme when you are finished making changes to update your community immediately with the new theme. These changes affect all pages in your community.
8. Replicate saved themes by exporting them from one instance and then importing them to another instance by using the Import/Export link under Themes. For more information, see Exporting themes on page 37 and Importing themes on page 38.

Using predefined themes

By 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 users with Manage Community or Customize Site permissions can see the Themes option under their user menu in the upper right corner of the User interface.

2. Click **Themes** and select one of the **Predefined themes**, for example, Bamboo or Winter.
3. If required, customize your chosen theme by clicking the blue dots next to each component and making changes.

   As you make changes, you see an instant preview of the updates.
4. For a thorough look at your changes click **Full Preview**.

   You are required to save the changes before previewing.

5. When you are finished making changes, click **Save Theme**, then clear the **Publish theme on save** check box to save the theme, but not publish it. This saves your work so that you can continue making theme changes later without affecting your current community.

   Alternatively, you can save the theme and publish it by selecting the **Publish theme on save** check box and saving the changes, which updates your community immediately.

Theming options reference

You have many options for designing your site by using the theming interface.

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. For more information, see Importing themes on page 38, Exporting themes on page 37, Using predefined themes on page 32.
Fonts and Colors	From here you can set the font of all text elements. Also, you can customize the text color for these elements, such as links, hovers, and metatext.
Branding and Decoration	From here you can set the community page width, favicon, background color and image, and border style. Be aware that if you set your Background Attachment to Fixed, depending on the image size and width, browser scrolling may be slow.
Advanced: Header and Navigation Style	You can choose one 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). Additionally, you can choose to hide the header.

Field	Description
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 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 menu. You don't need to know any CSS or HTML to use this option. For more information, see Creating custom links in the main menu on page 35.

Table 2: More options ("blue dot" options)

These options vary depending on which Header and Navigation Style you select.

Field	Description
Branding Header and Navigation: Branding header	Sets the community logo and background color and image of this header area. You can upload an image to be used as the logo image and specify in the **Alternate Text** box the alternative text for the image if a user for some reason cannot view it.
Branding Header and Navigation: Main Navigation	Sets the link colors, background color and image of the main navigation menu. **Note:** You can also customize the actual buttons that appear in this navigation menu. For more information, see Creating custom links in the main menu on page 35.
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 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 main navigation menu.
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, for example, main navigation menu highlights.

Field	Description
Sample Widget	Sets the widgets elements, such as border style and header background.
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.

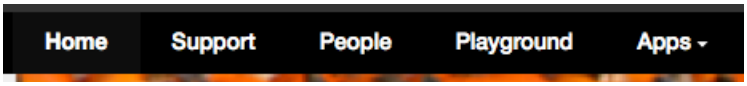
Creating custom links in the main menu

You can customize your main navigation menu so that users can quickly jump to your community's most popular or useful pages or external links by adding, editing, or deleting navigation buttons.

You can have a maximum of five buttons on the main navigation menu.

Here's an example of a customized navigation menu that includes a custom button: Playground.

Figure 3: Example of Custom Links



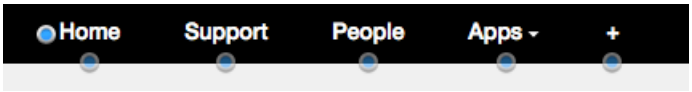
To create a custom link in the navigation menu:

1. In the user interface, go to **Your Avatar** > **Themes** > **Advanced** > **Custom Links** and select **Custom Links enabled**.

   Note that only users with Manage Community or Customize Site permissions can see the Themes option under their user menu in the upper right corner of the user interface.

   You should see blue dots under the main navigation buttons like this:

   Figure 4: Custom Links Navigation

2. From here, you have several options. Generally speaking, you can create navigation buttons that link to pages inside or outside of your community. Also, you can rename existing pages (for example, change News to 411 or People to Our Users), create drop-down menus of linked pages, rearrange the order of the navigation buttons, or even delete navigation buttons altogether. For details, see Custom Links Reference.
3. If you are creating a Single or Multiple custom link (not a Preset) and your community is set up for multiple languages, click **Provide other translations** for each navigation button you create, select the languages and provide translations for every language of the community.

For each new link you configured, you 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 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 finished customizing your navigation buttons, click **Full Preview** in the lower left corner to see how your changes look before publishing them.

Option reference of main navigation menu

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

Custom buttons

Customs buttons with 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 buttons, you need to provide translations if your community is delivered in multiple languages by clicking **Provide other translations** for each button that you add.

Table 3: Custom button options

Nav Bar Option	Links to
Single	Customizes a single link title and URL. For example, it might be helpful to your users to link to your CEO's Blog here. Alternatively, you could use this option to change the name of an existing Preset page. For example, you might rename the People button Our Users. Note that if you do this, the URL does not change, just the text in the navigation menu.
Multiple	Creates a drop-down menu with a unique title. For example, a Support button might drop down to Knowledge Base, File a Case, and Feedback. Or a Sales button might drop down to Create an RFP, Check the CRM, and Latest Wins.

Preset links

The Preset buttons 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 are 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 translations by clicking **Provide other translations**.

Table 4: Preset links options

Nav Bar Option	Links to
Content	`/content`
People	`/people`
Places	`/places`
News	`/news`
Support	`/support`
Apps	Opens up the Apps menu when clicked. The Apps navigation button is displayed outside of the theming interface only if the apps market is enabled (**Admin Console: Add-ons** > **Cloud Settings**) and the user is not anonymous.
Rewards	`/rewards` Opens up the community's Rewards global leaderboard when clicked.
Browse	Creates a drop-down menu that contains at least one of the following predefined links: Content (`/content`), People (`/people`), Places (`/places`).

System buttons

You can make some modifications to the following system buttons, 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 appears in the main navigation menu and takes users to the `/news` page by default. This button always appears as the left-most navigation item. Be aware that users have the option to pin any of their News streams to the Home button. For more information, see Pinning pages for quick access.
Create	The Create menu (as a button with the text "Create") appears in the main navigation when the Basic header is enabled (you may not see it in preview mode, but only after you publish). Otherwise, the Create menu appears in the secondary navigation area to the right as a pencil icon; if you use the Custom header, you have the option to use the text Create for the button instead of a pencil icon. For more details about the header options, see the Theming options reference on page 33.

Exporting themes

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

When you export a theme, the application creates a zip file that contains all of the theme's information, such as its customized colors and images. This zip file includes

any images you uploaded by using the Advanced theming interface. The theme file is encrypted for security reasons, so you cannot further customize its contents.

To export a theme:

1. Click on your avatar in the upper right corner and select **Themes**.

   Note that only users with Manage Community or Customize Site permissions can see the Themes option under their user menu in the upper right corner of the user interface.

2. From the theming page, select **Themes** > **Import/Export** .
3. Select **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 is downloaded to your local file system.

Now, you can import the zipped theme file to another Jive community, as described in Importing themes on page 38.

Importing themes

By using the **Themes** interface, you can import a theme to use it in your community.

When you import a theme, you add 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 exported a theme. This zip file includes all images that were uploaded by using the Advanced theming interface. For more information about exporting themes, see Exporting themes on page 37.

To import a theme:

1. Click on your avatar in the upper right corner and select **Themes**.

   Note that only users with Manage Community or Customize Site permissions can see the Themes option under their user menu in the upper right corner of the 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**.

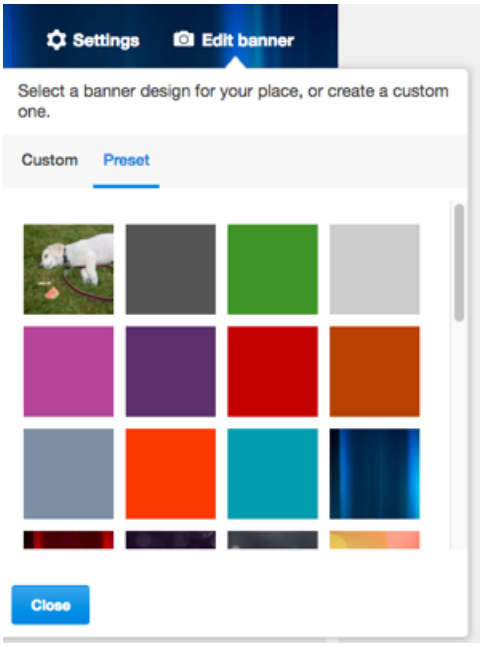
Now you should see the new theme in your list of saved themes. Click on it to see a preview of your community with that theme.

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: User interface: Your avatar > **Themes** > **Place Banner Management** > **Place Banner Presets**

Any changes you make to the place banner presets, such as adding a new banner preset, affects what place owners see when they edit the banner for their place. In the following image, the place owner sees a custom image that they can use as a banner because the community manager added this new image when they added a new banner preset:



For more information about adding images to banner presets, see Adding new images to place banner presets on page 40.

Note that the place owner can choose to upload another image for the banner by clicking **Custom**.

Replacing place template's default banner

You can replace the default banner image that appears in a place template (such as the Best Practices or another template) with your custom image. Additionally, 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 user interface, click **Your avatar** > **Themes** > **Place Banner Management** .

   Note that only users with Manage Community or Customize Site permissions can see the Themes option under their user menu in the upper right corner of the user interface.

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 remains unchanged.

7. Click **Save**.

Adding new images to place banner presets

You can add custom presets with your images to the existing set of banner designs available in a place template.

To add a new custom preset with your image:

1. In the user interface, click **Your Avatar** > **Themes** > **Place Banner Management** > **Place Banner Presets** > **Add new banner preset** .

   Note that only users with Manage Community or Customize Site permissions can see the Themes option under their user menu in the upper right corner of the 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 can see this image in their Banner Design options.

Optimizing themes for mobile browsers

When planning your community theme, note 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.
- 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.

To add a logo that is compatible with a narrow-screen view:

1. Click **Your avatar** > **Themes** .

   Note that only users with Manage Community or Customize Site permissions can see the Themes option under their user menu in the upper right corner of the user interface.

2. Once you are 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. In **Alternate Text**, specify the alternative text for the image if a user for some reason cannot view it.
7. Click **Save Theme** > **Save and Publish** .

Managing Support Center

The Support Center streamlines how users find answers by dedicating a path to just that.

The Support Center provides a user experience focused on enabling self-help and community support with the goal of reducing the number of new support cases being created.

The Support Center:

- Helps users quickly find their answers by using predictive search and providing official answers.
- Discourages users from cluttering up the community with already-answered questions by providing a configurable layout so you can surface targeted topics and common answers.
- Gives users a place to easily ask the community a question if an answer doesn't exist.
- Lets you adjust the layout and style to reflect your organization's content and branding.

Here's a sample of how you might set up Support Center for an internal community for a space exploration company.

About Support Center

For an internal community, the Support Center saves time for all employees, those seeking answers and those providing them.

You could use the Support Center to collect answers that were previously scattered throughout your community, and pull them into one place. Employee service departments such as IT, HR, and Facilities, would find this feature useful for reducing the time spent answering common employee questions. The following list suggests content an employee support center might need:

- Onboarding guides and employee handbooks
- Benefits booklets
- IT troubleshooting topics
- Mobile phone access for your community
- Maintenance requests
- How to access a printer

Note: To enable the Support Center, you need to file a case with Support. For more information, see Getting started with the new Jive Support Portal on Worx.

Enabling Support Center

If you see Support in the main navigation menu of your community, then you have the Support Center enabled. Otherwise, you need to enable it.

Fastpath:

- **Admin Console** > **Content** > **Support Center**

To enable the Support Center:

1. Go to the configuration page:
   - **Admin Console** > **Content** > **Support Center**
2. Select **Enabled**.
3. Click **Save**.

This enables the Support Center in your community. Now you need to enable custom links and add the Support Center button to the main navigation menu. For more information,see Adding Support link on page 44.

Adding Support link

By using the theming tool, you can add the Support link to the main navigation so users can access the Support Center.

Fastpath: Your avatar > Themes

To add the Support link to your community:

1. In the user interface, click **Your avatar** > **Themes** . If you already have Custom Links enabled, skip to Step Step 5 on page 44.
2. Click **Advanced** > **Custom Links** .
3. Select the **Custom Links Enabled** check box.
4. Click back to the main theming page.
5. Click the blue dot under the **+** mark.

   If you don't see a blue dot, you may have used all of the preset options, and you need to edit an existing one by selecting **Preset** > **Support** . (You can also rename it, as described in Remove or rename Support link on page 44).

6. Click **Save Theme**.
7. Click **Publish Theme on Save**.
8. Click **Save and Publish**.

Now you are ready to assign Support Center permissions to the person or group you want to design and maintain it. For more information, see Assigning Support Center permissions on page 45.

Remove or rename Support link

By using the theming tool, you can remove or rename the Support link.

Fastpath: Your avatar > Themes

Perform these steps to rename or remove the Support link from the main menu:

1. In the user interface, click **Your Avatar** > **Themes** . If you already have Custom Links enabled, skip to Step Step 5 on page 44.
2. Click **Advanced** > **Custom Links** .
3. Select the **Custom Links Enabled** check box.
4. Click back to the main theming page.
5. Click the blue dot under the Support button. You can:

   - **Delete navigation item** to remove the button from the navigation ribbon, or
   - Rename the Support button by selecting **Single** and then typing in the new name. For example, type `Support Ya!`, and then enter `/support` in the URL field, with the forward slash (`/`).

6. Click **Full Preview** to see how the change is going to look.

   When prompted to save the changes, give this new theme a name, such as Jive with Support Ya! or Jive without Support.

7. Click **Publish Now** or **Edit more** depending on what you want to do next.

Assigning Support Center permissions

You can assign Manage Support Center permission to the users who need to design and maintain the Support Center.

Fastpath:

- **Admin Console** > **Permissions** > **System Administrators**

If it makes sense for your organization, you can give certain people the responsibility of managing the Support Center. If you want only certain users to manage the Support Center, create a user override or a user group and assign them the Manage Support Center permission. Note that the System Administrator and users assigned the Full Access permission also have management rights.

To assign permission to a user or user group:

1. Go to the configuration page:
   - **Admin Console** > **Permissions** > **System Administrators**
2. Assign the **Manage Support Center** permission to either a user group or a user.
   - Assign this permission to a user by setting a user override. For more information, see Creating user overrides on page 113.
   - Assign this permission to a user group by creating a group and setting this permission. For more information, see Setting up administrative permissions for user groups on page 119.

After assigning this permission, any user with this permission can design the Support Center. For more information about designing the Support Center, see Designing Support Center on page 45.

Designing Support Center

Before you publish the Support Center to your community, you need to design it. It not only means choosing the colors and fonts you like but also adding content in the form of sections and places.

When you design the Support Center, think about how you can categorize the information you want users to see up front. Users can browse documents or requests in the places you added to the Support Center. Use sections to group these places and present essential topics in the order you find helpful.

You can change the background colors and images and also change the header text.

To configure the Support Center:

1. Click **Support** in the main menu.
2. Click **Configure** in the upper-right corner.

   You must have **Manage Support Center** permissions to see this option.

3. Once you are in edit mode, you can edit some colors and text. Click any blue box with a gear icon. Here's what you can do:

Options	Description
Background	Here you can edit the color of the Header text and the background. You can also upload a background image.
Header Text	Here's where you add the text that is the Support Center header.
Body Header Text	The body header text has two lines that you can add to the main part of the Support Center. It's a good place to talk about how people should use the sections you've set up.
Header Text for Support Channels	Here you can add a title to your Support Channels. You can use something like Still need help?, More ways to contact us or Let us know how we are doing.

4. Click **Add a Section** to create a new category for places in Support Center.

   Make the title describe the content users can find there, for example, Getting Started, Check on Your Orders, or Troubleshooting Tips.

5. Click **Add a Place** to add places to a section.

   Add places that belong to the section category. Keeping sections organized helps users find what they need, quickly. You can make it easy for a user to glance at a section and find the topic they've been looking for.

   Note: To learn about how to choose the five leading content items, see Designing Support Center.

   ---

6. Click **Add a Support Channel** at the bottom of the page.
7. Select **Publish Support Center on save** to make the Support Center visible to all end users.
8. Click **Save**.

Adding sections and places

Add places and sections to the Support Center so you can gather, in one location, topics that might help users.

Sections let you organize content from Jive places so users can easily find what they need. Add places to a section so users can see their featured, trending, or recent content. For example, you can create a Knowledge base section and add a space that contains knowledge base articles. If you don't have the Featured Content tile set up, then users see either Trending or Recent Content.

Setting up content

The Support Center displays the five most recent content items unless you have set up Trending Content or Featured Content.

Prepare content for the Support Center by deciding how you want the Support Center to display content. The order of precedence is Featured Content, Trending Content, and then Recent Activity. By default, the Support Center shows the five most recent content items for a place. Feature any content items, and you'll see them in the top five list for a place. Once content begins to trend by being liked or bookmarked, you'll see Trending Content instead of Recent Activity.

Adding other support channels

Add support channels so you can give your customers or users other avenues to contact you for Support if they need it.

Support channels provide ways for users to ask their questions when the answers are not in your community already. From creating a support request in your community to tweeting you, to calling or emailing, you can lay down the options you want users to take. It is also a great way to promote your social channels.

Enabling new features in your community

Some releases may include features that may or may not become part of the community features. You can enable or disable these features from the Admin Console.

Fastpath: Admin Console: System > **Settings** > **New Features**

We've added the following options to the New Features page.

Simplified Admin Console	Jive now includes the option to use a simpler admin console that we've redesigned based on real-world feedback from Jive community managers. With the Simplified Admin Console enabled, you see only the typically required settings grouped together in a more intuitive way.

Image Browse and Collections	Jive places now include an Images page where users can view images and organize them into collections to share with other community members. Place owners are also able to save and display collections for place members to view and share later. This feature is enabled by default, but you can disable it.
Group Membership Evolution	With this option enabled, social groups more closely reflect customer usage of group membership, as follows: • Open groups have been renamed to Public. • Public groups no longer have a concept of joining or invitation. All content in them is open for viewing and editing, unless any content item has been individually restricted. • Members Only groups have been renamed to Public (Restricted). • Public (Restricted) groups now allow non-members to create discussions, questions, and ideas, and to reply or comment on any content in the group. However, they cannot invite new members or create any other content types. • Members have the additional ability to invite more members, and to create all allowed content types. • Private groups have the same name and functionality as before. • Secret groups have been renamed to Private (Unlisted). • The group creation workflow has been changed to reflect the broader categories of Public and Private, with additional subtype selection. • The new naming conventions be reflected in place browsing and search.
Events Browse	With Events Browse enabled, places include an Events page where users can view a listing of the place's events, as well as filter them by tag, category, type, and date to view related events together. This feature is enabled by default, but you can disable it.
Profile Evolution	With Profile Evolution enabled, you see more relevant information at a glance. You see an optional banner at the top of your profile page now. Photos are now down the page in a Photos section. Your avatar is now your profile image. For more details, see the Onboarding Guide for this release on Worx.
Keywords in Content URLs	With this feature enabled, words from the title field of any newly created or updated content item are included as keywords in the content URL. This change improves SEO for Jive-x communities. Original title keywords are always used in the title no matter how much you edit the title. If you want to change the original title and

	keywords in the content URL, you need to delete the content item and create a new one. **Note:** After enabling Keywords in URLs you need to edit and then save existing content for it to begin using keywords in its URLs. Links to the original URLs continue to work.
HTML5 Document Previews	With this feature enabled, you can see document previews for uploaded files without using Flash. This feature supports the following formats: Microsoft Word, Excel, PowerPoint, and PDF. **Note:** HTML5 previews do not currently support inline comments or document search.

Renaming the root space

You can change the name and description of the root space from the Admin Console. By default, the root space is named `community`.

Fastpath:

- **Admin Console** > **Permissions** > **Spaces**

To change the name of the root space in the Admin Console

1. Go to **Admin Console** > **Permissions** > **Spaces** .
2. Click  > **Edit general information** next to the name of the root space.
   The root space is the top one in the list; it's called `community` by default.
3. In **Name**, enter the community name.
4. Optionally, in **Description**, enter the community description.
5. Optionally, in **Locale**, specify the default community locale.
   The default locale is `Inherit [English]`.
6. Click **Save Changes**.

The root space becomes available under new name throughout the application, for example, when you need to select a place.

Setting up 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.

Fastpath:

- **Admin Console** > **People** > **Locale and Language**
- **Admin Console** > **Permissions** > **Spaces** , then  > **Edit general information** , then **Locale**

A 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 and what the character encoding is. 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.

Note: Only a subset of the languages listed is 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 locale preferences, which take precedence. Here's 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 overrides global settings you make for another locale.

3. Locale set at the space level. For more information, see Setting Space Name, Locale, and Allowed Content Types.

   - **Admin Console** > **Permissions** > **Spaces** , then  > **Edit general information** , then **Locale**

4. Locale set at the root space (global) level.

   - **Admin Console** > **People** > **Locale and Language**

Inviting people to community

As a community manager, you can invite people to join the community. Informing people about the community site is rather simple: you provide them with a direct link to the site either from the community itself or by using any other communication channel.

On the community site, you can send invitations to people by using the Send Invites dialog box, as described Step below. You can also send an invitation when creating a user account in the Admin Console or configure the system to automatically send invitations to self-registered users, as described in Creating user accounts with the Admin Console on page 69 and Configuring self-service user registration.

Community managers or users can also invite external contributors to join the community. For more information, see Adding external contributors on page 155.

After receiving the invitation, people can join the community by using the available methods, for example, self-registration or SSO. For more information, see the following sections: Setting up LDAP and Active Directory on page 84 and Setting up Single Sign-On on page 91.

To invite people to join the community by using the Send Invites dialog box:

1. In the user interface, click **People** > **Send Invites** .
2. In the **Send Invites** dialog box, enter the email addresses of people you want to invite.

   When selecting people to invite, you can also do the following:

   - To invite several people from your email address book or the user management system, browse contacts by clicking the browse icon. Select the people or groups of people you want to invite, and then click **Add selected people**.
   - To invite people from an existing email list, export the list of addresses from your email application, then copy and paste it in. The addresses in the list must be comma-, space-, or semicolon-delimited.

3. If necessary, edit the message you want potential group members to see with their invitation.
4. Click **Send Invitation**.

The people you invite receive emails with the invitations to join the community.

Customizing News page

The News page features a variety of streams (News streams) designed to direct users to content, people, and places of their interests. For example, it includes an All Activity stream, which shows the recent activity from all over the community depending on user permissions. Additionally, it also displays the latest updates in specific streams that a particular user may be following or any custom streams that the user may have created.

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

For more information on using the News page and News streams, see Using News in the User Guide.

Tips for creating News streams

Before you create a News stream, consider the following questions.

Does absolutely everyone need this information?	News streams created for everyone display information 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 is relevant to all of these users, follow the instructions in Creating News streams for everyone on page 53.
How much traffic is generated by the place or blog I want to share content from?	The place you select for a News stream should not be 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 needs this News stream?	You can define audiences by selecting individual people, by filtering on profile fields, or by selecting a user permissions group that is defined in Jive. The last two choices may require some preparation on your part: to make sure you're using profile fields consistently or to create any permissions groups you need for targeting an audience. Note that the system-defined groups in Jive (under **Admin console: People** > **Management** > **User Group Summary**) cannot be used to target audiences. You can use any custom-defined groups shown on the page. These groups may be created manually or synced from an SSO provider.

What are some examples of News streams I might create?	For a detailed example of how you might create News streams for your community, see All About the News Feature on Worx.

Creating News streams for everyone

Users see News streams listed across the top of the News page. As a community manager, you can create and manage the streams for all registered users to see to the News page.

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

You can create up to 10 News streams to be displayed on the News page in the order listed under **News Stream** when you edit the News page.

To create News streams for everyone in the community:

1. In the user interface, go to the **News** page and click **Manage the News page** icon ( ) next to **News** to create a new stream.
2. Under **Create custom streams for**, select **Everyone**.
3. In **News Stream Title**, enter the stream title, for example, CEO's Blog.

   This is the stream name users see on the News page.
4. In **Places/Blogs**, specify the place or blog from which you want the stream to pull content.

   Tip: If you see both a place and the place blog listed, note that selecting the blog would post less content in the stream. In other words, selecting a place means *any* new content created there shows up in the stream. Selecting the blog means only blog posts show up.
5. Under **Audience**, select 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 **Notify Users**, 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: In general, we recommend setting this to **Off**. However, you may likely want to enable notifications on the most important content that your users cannot miss. Note that if notifications get noisy, users may stop reading the content.
7. Click **Save** to save the stream configuration.

You can create up to 10 News streams and reorder the list by dragging streams to new positions.

8. When you finished adding streams, click **Publish Layout**.

For a detailed example of how you might create News streams, see All About the News Feature on Worx. You must be a registered community user to see this content.

Creating News streams for specific users

Users see News streams listed across the top of the News page. As a community manager, you can create and manage the streams to show a different selection of content to different audiences on the News page.

Attention: 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 see content relevant to them:

1. In the user interface, go to the **News** page and click **Manage the News page** icon ( ) next to **News** to create a new stream.
2. Under **Create custom streams for**, select **Specific Users**.

   This opens the **Edit News Stream** page.
3. In **News Stream Title**, enter the stream title, for example, My Team News.

   This is the stream name users see on the News page.

   Tip: Make the stream title work for every rule you are going to create for this stream.

4. Select **Create Stream Rule**.

   This opens the **Create a Stream Rule** page.
5. Specify stream rules to filter users. For each rule, do the following:
   a) Under **Places/Blogs**, enter or select the place or blog from which you want the stream to pull content.

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

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

For more information on user groups, see Managing user groups on page 65.

You also have the option to select **Create profile filter** so that you can filter your audience based on a combination of profile fields. For more information on filtering based on a profile field, see Creating an Audience-Specific News Stream in All About the News Feature on Worx.

c) Click **Save** to save the stream filter and return to the stream rules configuration page.

You can create up to 100 rules for a stream.

6. Under **Notify Users**, 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: In general, we recommend setting this to **Off**. However, you may likely want to enable notifications on the most important content that your users cannot miss. Note that if notifications get noisy, users may stop reading the content.

7. Click **Save** to save the stream configuration.
8. When you finished adding streams, click **Publish Layout**.

As an example, you could create a stream called Management Ideas, and then create different rules that direct new content from Finance groups to the Finance managers and blog posts from the Technical Managers group to Engineering managers. 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.

For a detailed example of how you might create News streams, see All About the News Feature on Worx. You must be a registered community user to see this content.

Turning off or on Top and Trending

Users with the Full Access permissions can toggle the **All Activity: Top & Trending** stream for the community.

Fastpath: Advanced Admin Console > **System** > **Settings** > **News**

To toggle **All Activity: Top & Trending** stream for the community:

1. Go the configuration page:
   - **Advanced Admin Console** > **System** > **Settings** > **News**
2. In **Enable or disable top and trending content on news page**:
   - To turn on **Top & Trending**, select **Enabled**.

- To turn off **Top & Trending**, select **Disabled**.

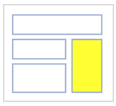
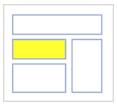
3. Click **Update**.

News page tile reference

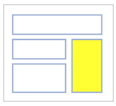
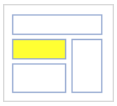
Here is a complete list of the tiles available on the News page of your community.

Tiles are split by category, similar to tiles arrangement in the UI. Some tiles can be available in more than one category.

Collaboration tiles

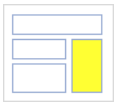
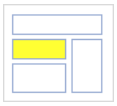
Tile	Description	Dependencies	 Narrow column	 Widecol-umn	 Jumbo column	Jive Dai-ly sup-port
Docu-ment Viewer	Shows a full preview of a document you choose to dis-play	Content added manually				
Helpful Links	Builds a list of key links for quick refer-ence. Links can be internal to your commu-nity or external URLs	Content added manually				
Key Dates	Shows select-ed dates for your team	Content added manually				

Graphic Elements tiles

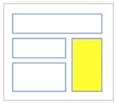
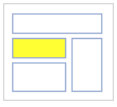
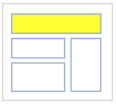
Tile	Description	Dependencies	 Narrow column	 Widecol-umn	 Jumbo column	Jive Dai-ly sup-port
Hero Im-age	Provides a key image with a link and call to action as a header for your News page	Content added manually				
Banner	Adds a series of linked im-ages with text to promote im-portant con-tent	Content added manually				
Carousel	Links a rotat-ing image carousel to crucialdestina-tions	Content added manually				
Create an HTML Tile	Adds HTML	Content added manually				*
Image Gallery	Creates a slideshow with images and captions	Content added manually				
Video (Exter-nal)	Shows a manu-ally selected video from an external, non-community source	Content added manually				

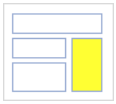
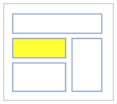
* The configuration of each Custom HTML tile defines if it is available on Jive Daily: Intranet on the go.

Custom List tiles

Tile	Description	Dependencies	 Narrow column	 Widecol-umn	 Jumbo column	Jive Dai-ly sup-port
Expand-able Sec-tions	Shows links to community content under collapsible headings	Content added manually				
Featured People	Builds a list of important peo-ple for your place	Content added manually				
Helpful Links	Builds a list of key links for quick refer-ence. Links can be internal to your commu-nity or external URLs	Content added manually				
Key Con-tent and Places	Displays a list of content and places that you can edit and manage yourself	Content added manually				

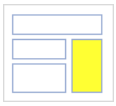
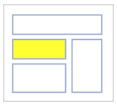
Dynamic List tiles

Tile	Description	Dependencies	 Narrow column	 Widecol-umn	 Jumbo column	Jive Dai-ly sup-port
Featured Quest	Shows the us-er's progress as they com-plete a quest	Relies on a quest being selected				
Latest Blog Posts	Shows the newest blog posts in your community	Content added manually. Blogs must be enabled				

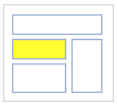
Tile	Description	Dependencies	 Narrow column	 Widecol-umn	 Jumbo column	Jive Dai-ly sup-port
Leader-board	Shows the top point earners in the commu-nity.	Internally-fac-ing communi-ties only				
News	Displays news headlines from the community that are pulled in from each of the News streams	Relies on con-tent from the News streams				
Similar Places	Shows places with the same tags	Relies on con-tent being tagged				
Super List	Shows an up-dated, filtered view of con-tent, people, or places	Relies on a query: click **Use this view in a tile** at the bottom of any People, Places, or Content browsing re-sult				
Tagged Content	Displays con-tent that matches specif-ic tags	Relies on con-tent being tagged				
Trending Content*	Displays con-tent that is getting an in-crease in views and likes	Relies on con-tent getting viewed or liked, or both				
Trending People	Displays peo-ple whose ac-tivity is getting an increase in views and likes	Relies on con-tent getting viewed or liked, or both				

* Content items can be excluded from the **Trending Content** tile.

Support tiles

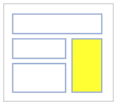
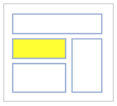
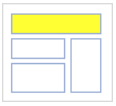
Tile	Description	Dependencies	 Narrow column	 Widecol-umn	 Jumbo column	Jive Dai-ly sup-port
Ask a Question	Finds a previ-ously asked or answered question, or gives the abili-ty to ask a new one	Relies on con-tent query. Configure to select content types and places to query				
Helpful Links	Builds a list of key links for quick refer-ence. Links can be internal to your commu-nity or external URLs.	Content added manually				
Super List	Shows an up-dated, filtered view of con-tent, people, or places.	Relies on a query: click **Use this view in a tile** at the bottom of any People, Places, or Content browsing re-sult				

External Add-Ons tiles

Tile	Description	Dependencies	 Narrow column	 Widecol-umn	 Jumbo column	Jive Dai-ly sup-port
Create an HTML Tile	Creates a cus-tom user expe-rience by in-serting HTML content into a tile for your place	Content added manually				*

* The configuration of each Custom HTML tile defines if it is available on Jive Daily: Intranet on the go.

Custom tiles

Tile	Description	Dependencies	 Narrow column	 Widecol-umn	 Jumbo column	Jive Dai-ly sup-port
Create a Content or Place Tile	Displays a list of content and places that you can edit and manage yourself. This tile and its content can be shared and used by other people in the community	Content added manually				
Create a People Tile	Build a list of important peo-ple for your place	Content added manually. This tile and its content can be shared and used by other people in the community				

Rebuilding News streams

If the synchronization of content or the users of a News stream is lost, you can rebuild the News stream. A stream rebuild verifies all place memberships against the rules of the stream, and corrects any issues, similar to the way a search index or browse system rebuild works.

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

The Activity Engine service handles a number of key features in the Jive application including streams for places and people. Because the Activity Engine is a remote system and users change place membership at will, there may be times when those kinds of changes are not propagated correctly and user and streams get out-of-sync. For example, a stream could get out of sync if you lose internet connectivity while you're creating or editing it.

During a rebuild, every member of the audience for a News stream you select is verified against the stream's rules and any out-of-sync issues are corrected.

To rebuild a News stream:

1. In the Admin Console, go to **System** > **Settings** > **News**
2. Under **(Publication) Rebuild**, select a stream to rebuild.
3. Click **Rebuild**.

Configuring News FAQ

Here are some frequently asked questions and answers about setting up the News page and news streams.

Who can create and modify the News page and news streams on the page?	People with Manage News Streams permissions have the rights to modify the News page and create, modify, or delete news streams for this page for the entire community, 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 other users Manage News Streams permissions, by going to **Admin Console: People** > **Permissions** > **System Administration** and creating a user override to assign the user Manage News Streams permissions.
Can I add a private unlisted place to the News stream?	Yes, if you are an owner or member of the private unlisted place. Be aware when you add a private unlisted place to a news stream to be displayed on the News page that other users with Manage News Streams or Manage

	Community permissions are able to see this stream. However, they are not able to modify or delete a News stream that has a private unlisted place of 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 on the News page configured in your community. This does not include each user's ability to create up to 10 custom streams of their own; so a user can see up to 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 up to 100 rules in a News stream. Within each rule, audiences and places are essentially unlimited.
Can I change the name of the News link on the navigation bar?	Yes. Just use the Single Custom Links feature in the theming interface. For more information, see Option reference of main navigation menu on page 36.
How do I turn off Top & Trending?	Contact your community administrator about turning off the **Top & Trending** News stream. Additionally, authors and community managers can exclude content items from the **Top & Trending** stream.

3

Managing a community

In this section you can find tasks related to day-to-day community management.

For details, see the following topics:

Managing user accounts and user groups

System administrators, user administrators, and group administrators can use the Admin Console to add, remove, and edit accounts for users and user groups.

Note that system and space administrators can set up permissions for users and user groups, but user and group administrators can not do this. For more information about setting up permissions, see Managing permissions on page 108.

Overview of 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 features.

User accounts and user groups

A *user account* represents a person who is using the application. Each user account has associated content, including the person's profile. For all users, you can use the Admin 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 users, for example when they're no longer involved, but you want to keep their content. For more information, see Managing user accounts on page 68.

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 administrators, who have the Admin Console access through which they can manage user group settings and membership. For more, see Managing user groups on page 65.

External user identity systems

The work you do with user accounts and user groups depend heavily on whether the application is connected to an external user identity management system. Generally, when you add user accounts and user groups by 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 is 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 are added to the application's database and not the external system. It is also possible that user accounts are managed by the external system, but the groups they're members of are created and managed locally in the application database. How user groups are managed is defined when the external system is connected to the application.

For more information on connecting an external LDAP or Active Directory system, see Setting up LDAP and Active Directory on page 84.

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 self-service user registration.

Managing user groups

A user group makes assigning and managing permissions easier by gathering users into one group. The existence of user groups isn't visible in the application's user interface unless you use role badges for the group.

An example of a user group is a group called *hr_users* that includes users who work in the human resources department as members.

User groups are made up of members and administrators. Unless they have access to the Admin Console, members typically aren't aware that they're in a user group. The member's account defines (at least partly) their access to the application features. Group administrators 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 administrator access, they are only able to access account management pages for the account they're administering.

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 are added to the application's database and not the external system. It is also possible that user accounts are managed by the external system, but the groups they're members of are created and managed locally in the application database. How user groups are managed is defined when the external system is connected to the application.

For more information on connecting an external LDAP or Active Directory system, see Setting up LDAP and Active Directory on page 84.

Creating user groups

You add user groups by creating and naming a group, then adding user accounts for each of the group's members. You should also add one or more user accounts as administrators for the group.

Fastpath:

- **Admin Console** > **Permissions** > **User Groups** , then click **Create New User Group**

You can assign role badges to groups. Role badges provide visual cues in the user interface that help people quickly identify community users and their responsibilities. For more information see Adding and removing users to user groups on page 67.

To create a user group:

1. Go to the configuration page:
   - **Admin Console** > **Permissions** > **User Groups** , then click **Create New User Group**
2. Under **General Settings**, in **User Group Name**, enter a user group name.

   The name should be meaningful and convey the group purpose, for example, HR_bloggers or Support_specialists.
3. In **Description (optional)**, enter the description of the user group.

   You should add the information about this group purpose and who is included in it.
4. If the group can be used as part of the News audience, select the **Visible to News Admins** check box.
5. If you want to use role badges, do the following:
   a) Under **Role Badge**, select **Enabled**.
   b) In **Badge Image**, browse and upload a 16 by 16 pixel image to be used as the role badge.
   c) Select the role for the users in this user group from the following roles:
   - Administrator
   - Champion

- Employee
- Expert
- Moderator
- Support

6. Click **Create Group**.
7. Use the **Add Members** links to add user accounts of the members of the new user group. For more information see Adding and removing users to user groups on page 67.
8. Use the **Add Admins** links to add user accounts for users who have permission to administer the account. If you use the badge roles, they are not applied to the administrators. For more information see Adding and removing users to user groups on page 67.
9. 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.

Adding and removing users to user groups

A user group includes members and administrators. As a user group administrator, you can add members and administrators to the group.

Fastpath:

- **Admin Console** > **Permissions** > **User Groups**

If you want administrators to have the same permissions (if any) granted to a user group, then you need also to add them to the Group Member list. When administrators 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. You can manage group administrators only from the Advanced Admin Console.

Note that unless they have access to the Admin Console, users won't know which user groups they're a part of.

Adding members and administrators to user groups

To add members and administrators to an existing user group:

1. Go to the configuration page:
   - **Admin Console** > **Permissions** > **User Groups**
2. To add members, in the **Admin Console**:
   a. Click > **Manage group members** next to the group from which you want to add or delete members.
   b. Under **Add Members to <user group>**, use the search box or people picker to select users whom you want to add as group members.
   c. Click **Add selected users**.

   The users you've selected are added to the group and you can see them in the **Group Members for <user group>** list.

Removing members and administrators from user groups

To remove members and administrators from an existing user group:

1. In the Admin Console, go to the configuration page:
   - **Admin Console** > **Permissions** > **User Groups**
2. To remove members, in the **Admin Console**:
   a. Click > **Manage group members** next to the group from which you want to add or delete members.
   b. Under **Group Members for <user group>**, select the **Remove** check box next to the members you want to remove.
   c. Click **Remove selected**.

   The users you've selected are removed from the group.

Managing user accounts

You can access just about everything related to a user from their user account in the Admin Console.

Note: If your community uses an external user identity system (such as LDAP or Active Directory) to manage user data, by default you cannot use the Admin Console to edit information managed there. Console fields corresponding to data in the external system are disabled, and you cannot delete users from the Admin Console. Note that 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, see Setting up LDAP and Active Directory on page 84.

Creating user accounts with the Admin Console

One of the ways to add new users to the community is to create their user account in the Admin Console.

Fastpath:

- **Admin Console** > **People** > **Add Users**

By default, if your community uses LDAP or Active Directory to manage users, new user accounts you create from the Admin Console go into the local application database (where content is stored). You can edit user account properties for LDAP-managed users if your LDAP provider allows it (by default, it is prohibited). For more information about using LDAP or Active Directory with Jive, see Setting up LDAP and Active Directory on page 84.

To create a new user account:

1. Go to the configuration page:
   - **Admin Console** > **People** > **Add Users**
2. In **First Name** and **Last Name**, enter the name of the person for whom you creating a user account.

   Note: A username may not contain any of the following characters: **, / ? & #**

   Note that some communities are preconfigured to use a user email address as their username.
3. In **Email**, enter the email address of the person.
4. In **User Type**, specify if this person is a regular user or an external contributor.
5. In **Password** and **Confirm Password**, enter the password to the account.

   The user will be able to change the password after logging in if the community settings allow that.
6. Select the **Send Welcome Email** check box to send the new user a welcome email.

7. If you want to create this user and finish up user additions, click **Create User**.

   The user account is created and the **User Summary** page opens for editing with the account properties. Generally, you should edit properties for the user account while you're creating it because a newly created account doesn't have permission to do anything in the community. For more information on the profile settings, see Overview of user account management on page 70.
8. If you want to create more user accounts after this one, click **Create and Create Another User**.

   The user account is created and the page's fields are cleared for you to create one more user account.

Overview of user account management

As an administrator, you can view and edit user's basic information, reset their passwords, view their community content, or delete their account altogether.

Fastpath:

- **Admin Console** > **People** > **Search Users**

To view a user account summary or edit it:

1. Go to the configuration page:
   - **Admin Console** > **People** > **Search Users**
2. In the list of users, click on the username of the user whose user account you want to edit.
3. View and edit the account settings.
4. Click **Update** to save the changes.

Here are the settings you can change.

Profile information

Among the user properties, you can 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. Note that you can configure the application to enable users to request their own password reset. If that feature is disabled, then you can reset the password from this account summary. For more information about self-registration, see Configuring self-service user registration.

Caution: If you change a user's password this way, the application does not send an email to the user whose password you changed.

Deactivation or deletion of user account

You can disable a user account, removing their access but keep their content in the system. Alternatively, you can delete the user with all their content. For more information, see Deleting and deactivating user accounts on page 74.

User activity in your community

You can view lists of the documents, discussion messages, and blog posts that a user has contributed or worked on. The User Properties lists 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.

Fields visibility settings

You can choose whether or not a user name and email address are visible to others in the community.

An administrator can configure the application so that a user can set the visibility of their own name and email address. In that case, then the user is able to change the setting independently of the setting you make in the Admin Console — that is, 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 are 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 user groups on page 65.

Avatars

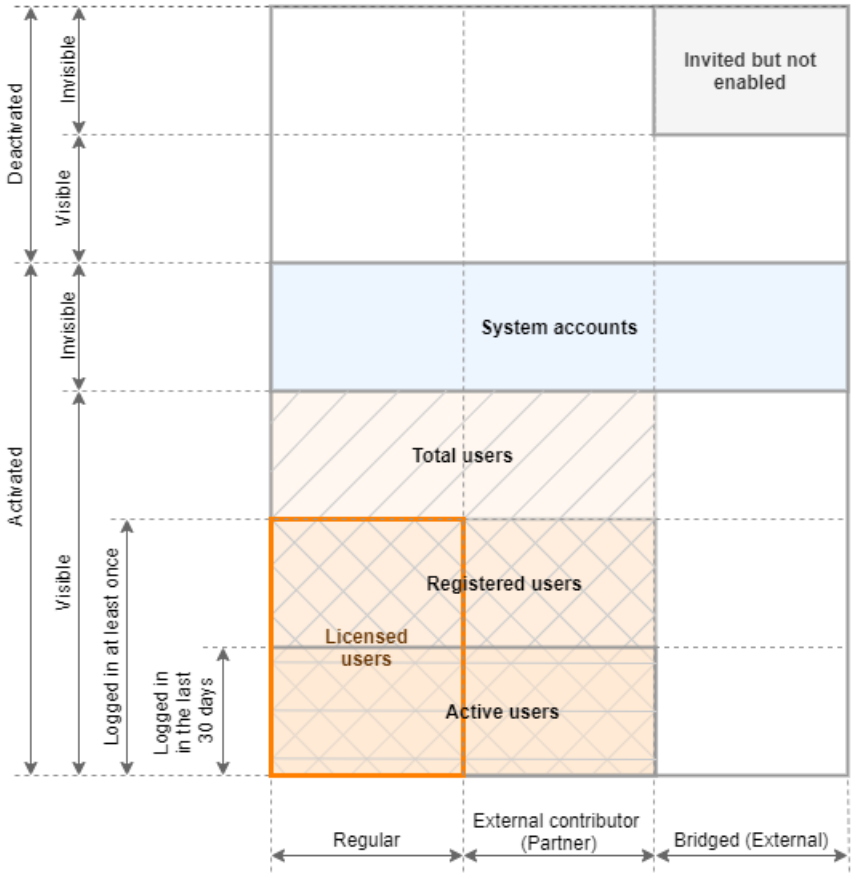
If a person has uploaded their own avatars, their User Summary page displays the images they've uploaded. You can delete avatar images from this page.

User account definitions

Jive identifies different types of user accounts to separate users into groups for accounting purposes.

You can find them across various Jive components and reports, such as the Admin Console, JCA, community analytics, and posted reports.

Figure 5: User account type definitions



We distinguish user accounts as follows:

Regular	These are user accounts registered within your community.
External contributors	Users who are not part of your community but are provided access to specifically defined groups. For more information, see Using external groups in the Cloud User Help. Note that previously external contributor accounts have been referenced as *partner*.
Bridged	User accounts from other Jive communities bridged to your community. Note that previously bridged accounts have been referenced as *external*.

Activated and deactivated	Activated accounts can be used to interact with the community – log in, view and collaborate on content, manage users, or do any other tasks. Note that if an LDAP server is used to manage user accounts for your Jive community, you may see a large number of activated accounts as a result of user sync which may not represent the number users actually using the community. Deactivated accounts are kept in the system but are inert and cannot be used to access the community. At the same time, the content that is associated with the account remains until the account is deleted. For more information, see Deleting and de-activating user accounts on page 74. Note that previously activated accounts were referenced as *enabled* and deactivated accounts as *disabled*.
Visible and invisible	Account visibility defines whether or not an account is visible from the front-end of Jive. This property is used with system administration and service accounts, such as the built-in *admin* user account. You can check the visibility of a user account through the Person Service API endpoint.
Logged in and logged in within the last 30 days	*Logged in* means that the account has been used to log in to the community at least once. Additionally, we separate accounts that have been used to log in within the last 30 days to determine active community users.

Keeping in mind these groups, we count users as follows:

Total users	*Activated Visible* users that are not *Bridged*.
Registered users	*Activated Visible* users that are not *Bridged*, and have logged in at some point in time.
Active users	*Activated Visible* users that are not *Bridged*, and have logged in at some point in the last 30 days.
System accounts	*Activated Invisible* accounts created for administrative purposes. System service accounts are typically generic accounts utilized for purposes other than for accessing the community. For example, the built-in *admin* user account.

Licenses are counted only for **registered visible active user accounts with at least one login**. You can find details in the License Usage report in the Admin Console. For more information, see Viewing user licenses on page 173.

User account statuses

Each user account is assigned a particular status that defines its registration status. Here you can find the list of possible statuses.

Invited	A community has sent an invitation to an unregistered person including the person's email in the message. This status is

	available if invitations are enabled in the community. For more information, see Configuring self-service user registration.
Awaiting moderation	The user account has at least the minimum necessary data and is awaiting moderation if account moderation is enabled in the community.
Approved	The user account in this status has successfully passed moderation if account moderation is enabled in the community.
Rejected	The user account in this status has failed moderation if account moderation is enabled in the community.
Awaiting validation	This status shows that the user's email is not confirmed if the email validation is enabled in the community. For more information, see Configuring self-service user registration.
Validated	This status shows that the user has their email validated if the email validation is enabled in the community.
Registered	After a user logs in to the community for the first time the account status
None	This status is used for the user accounts that do not belong to any other status, such as the system accounts.

Deleting and deactivating user accounts

You can deactivate or delete a user account when you want to remove the person's presence from the community.

Fastpath:

- **Admin Console** > **People** > **Search Users**

Deactivating a user account removes their access but keeps their content in the system. When you deactivate someone's account, Jive replaces their former avatar with a blank avatar; the word "Deactivated" appears on their profile. The person is no longer be able to log in or receive notifications, but their content remains viewable in the application.

Deleting a person's user account deactivates their access and 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.

Caution: Deleting someone's account is permanent. This action deletes 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). We recommend that you read the warnings on the Delete User page!

Note that tiles created by users in places belong to the places and not to the user. Consequently, when the account of the creator is deleted, all tiles and content added by using tiles are not deleted; they remain available in places.

Note: An administrator can ban someone from being able to access to the community.

To delete or deactivate a user account:

1. Go to the configuration page:

   Fastpath:

   - **Admin Console** > **People** > **Search Users**

2. Find the user account you want to delete in the list and click on the user name.

   This opens the user properties page.
3. To deactivate the user account, click **Deactivate User**.

   The user account is deactivated and the user is not able to access the community. The content that is associated with the account remains.
4. To delete the user account, click **Delete**.

   The user account and all associated data are deleted. This may take some time to finish, depending on how much content is associated with the account.

Configuring self-service user registration

You can configure the application so that new users can create their own accounts and invite others to join the community.

Fastpath:

- **Admin Console** > **People** > **User Registration**

If you allow user self-registration in the community, you can control who can register and who are prohibited from registering. For more information about the settings, see User registration settings reference.

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

To enable and configure user self-registration:

1. Got to the configuration page:
   - **Admin Console** > **People** > **User Registration**
2. Under **User-Created Accounts**, select the **Allow users to create their own account** to enable self-registration, and then specify the additional parameters.
3. Under **New Account Settings**, in the **Welcome Email**, select **Enabled** to send Welcome emails to newly registered users.

4. In the **Username Blacklist**, select **Enabled** to prohibit the use of specific words in user names, and then enter the words in the text box.

   For example, you can add the words "admin" and "administrator" to prevent deceit.

5. In the **Fields displayed at registration** section, specify the list of required and optional fields for users to fill in when they are registering.
6. Click **Save Settings**.

With these settings enabled and configured, the allowed users can create accounts for themselves.

User registration settings reference

Here you can find the settings available for user self-registration.

- **Admin Console** > **People** > **User Registration**

User-Created Accounts

Setting	Description
Allow users to create their own account	With this check box selected, user-created accounts are enabled, and registered users can invite others to join via email. For more information, see Inviting people to community on page 51. People can sign up for a new account from the community login page. The registration process then takes them through a brief set of screens through which they add information about themselves.
Require email address validation for users creating their own account	With this check box selected, self-registering users must validate their email.
Use Enhanced Registration Flow	With this check box selected, self-registering users can complete account creation before being approved by an administrator. This setting enables a simplified form with only required fields. If you have guest access enabled, users who complete the form can be directed to continue navigating the site while waiting for registration approval.
Enforce Community Domain list	With this check box selected, a person must have an email account belonging to the Community Domain List which is configured in its own section.
Allow new external contributors to create their own accountwheninvited by email to an externallyaccessible group	With this check box selected, external contributors can create their own accounts. Alternatively, community administrators create accounts for external users themselves. For more information, see Managing external groups on page 153.

Security

Setting	Description
Registration Moderation	With this enabled, new requests appear on the moderator page in the community (**Moderation** > **Pending Items** .) If you have a user administrator, that person must approve or decline requests; otherwise, the system administrator gets those requests.

New Account Settings

Use the following table to configure user account settings.

Setting	Description
Password Strength Check	This setting defines how strong user passwords must be. The password strength indicator then helps the person registering to create a password that's strong enough to qualify.
Human Input Validation	With this enabled, a person registering is 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	With this feature enabled, the application sends an email to the person registering at the address they provided. By default, the email includes a link that the person must follow to prove that the email address they gave is a valid one. This is another means to discourage false registration.
Welcome Email Settings	With this feature enabled, the application sends the new user an email when they've finished registering.
Fields displayed at registration	The fields that are displayed to prompt a user for information while they're registering. The list of fields here is based on the fields defined for user profiles. For more information on profile fields, see Configuring user profile templates on page 82.

Configuring password settings

You can give people the ability to change or securely reset their own passwords and define the strength of each password.

Fastpath:

- **Admin Console** > **People** > **User Registration**
- **Admin Console** > **People** > **Password Reset**

When password reset is enabled, users can change their passwords with the help of password strength tips and a strength meter. They can access the functionality or the option under the avatar in the user interface:

- By using the link on the Login page: The user provides the required information about themselves and receives an email with instructions on password change.
- By selecting **Change Password** under their avatar on the user interface.

To enable and configure password reset:

1. Go to the **User Registration** configuration page:
   - **Admin Console** > **People** > **User Registration**
2. Under **Security**, in the **Password Strength Check** section, specify how strong each user password must be.
3. In the **Human Input Validation** section, select **Enabled** to present a captcha.
4. Click **Save Settings**.
5. Go to the **Password Reset** configuration page:
   - **Admin Console** > **People** > **Password Reset**
6. Under **Password Resetting Status**, select **Enabled**.
7. Click **Save Settings**.

Additionally, you can to configure the template of the email confirming the password reset.

Configuring the Org Chart

The Org Chart shows the organizational relationships as a diagram making it easier for users to understand relationships between people. You can enable or disable the Org Chart in the Admin Console.

Setting up the Org Chart includes the feature setup and the user relationship configuration. By default, the Org Chart is enabled.

When you set up the feature, you define how the Org Chart should work in the community, in the Advanced Admin Console. And after you configure organizational relationships, users can see a graphical representation of their places in the organization structure, including their manager and coworkers. For more information, see Defining organizational relationships on page 79.

Defining organizational relationships

After you've set up the org chart, users will see a graphical representation of a user's place in the org chart, including their manager and coworkers, on a user's profile page.

Fastpath:

- **Admin Console** > **People** > **Org Chart**

To add organizational relationships

1. Go to the configuration page:
   - **Admin Console** > **People** > **Org Chart**
2. Under **Create a user relationship**, enter the team leader and the team member usernames.

   You can type the usernames or browse and search a list of users to add users.
3. Click **Add** to add the relationship.

The relationship is added immediately and appears under **View relationships**. You can select how many items should on the page in **Items per page** — 15, 30, or 50. Additionally, you can filter the list to display only the relationships that include a particular user by entering the username in the **Filter by Username** box and clicking **Filter**.

Besides that, the relationships of a particular user are displayed on the Org Chart on the user profile page.

To remove organizational relationships

1. Go to the configuration page:
   - **Admin Console** > **People** > **Org Chart**
2. Under **View relationships**, find the relationships of by the username of one the user.

   You can filter the list to display only the relationships that include a particular user by entering the username in the **Filter by Username** box and clicking **Filter**.
3. To break a relationship, click **Retire** next to the relationship.

The relationship is removed immediately from the **View relationships** list. Besides that, it is removed for both affected users on the Org Chart on the user profile page.

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 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 can see their name and email address.

Fastpath:

- **Admin Console** > **People** > **Global Profile Settings**

The settings on 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 more information on customizing the user profile fields, see Configuring user profile templates on page 82.

By configuring settings in the **Featured Profile Fields**, **Other Profile Fields**, and **Availability and Location** sections you can 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 more information on customizing the user profile fields using the Header Profile Fields and Other Profile Fields sections, see Configuring user profile templates on page 82.

Table 6: User Profile Fields settings

Setting	Description
Name Visibility	Select the check box 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 with the following exceptions: • Users see their full names on their profile page. • The administrators with Manage Groups or higher permissions see the full names on the user profile pages. For more information about permission levels, see Overview of System Administration permission levels on page 114.
Profile Image Visibility	Select the check box to let users set who can view their profile image. You can also set who sees the profile image by default.

Setting	Description
Creation Date Visibility	Select the check box 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 the check box to let users set who can view their last login date. You can also set who sees the last login date by default.

Table 7: Other Options settings

Setting	Description
Allow Profile Images	Select **Yes** to allow people to display an image (such as a photo of themselves) on their user profile. You can also set the maximum number of profile images users can upload.
Allow Banner Image	Select **Yes** to allow people to allow users to use a banner image on their profile.
Show Full Name by Default	Select **Yes** to have a person full name displayed on their profile, as opposed to merely their user name. In external-facing communities, people usually prefer not to have their full name displayed. In the **Name Visibility** field, you can allow users to customize the visibility of their name.
Show Full Name in User Mentions	Select **Yes** to have a person's full name displayed when they are at-mentioned. In external-facing communities, people usually prefer not to have their full name displayed. In the **Name Visibility** field, you can allow users to customize the visibility of their name.
SkillsandEndorsements	Select whether you want to enable both skills and endorsements, enable only skills, or disable both. Skills are how users tag their own profile and endorsements are the tags others give users.
EmailNotifications	Select whether you want to enable email notifications, disable them completely, or let users decide for themselves. By default, users can change their Notification Preferences by going to on their preferences page in the **Receive email or mobile notifications** field (**User Avatar** > **Preferences** > **General Preferences**). If you enable or disable email notifications, the users can see the **Receive email or mobile notifications** field but are not able to edit it.

Configuring user profile templates

A user's profile can include biographical and professional information, along with links to content they've contributed. You can use configure the fields that show up in profiles and set up visibility options.

- **Admin Console** > **People** > **Global Profile Settings**

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.

On the Profile Settings page, you can see the **Availability and Location** 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 can see the **Featured 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 information about them0, see Letting users control their own settings on page 80.

The application includes several commonly used fields by default, and you can add custom fields, as described in Creating new user profile fields on page 83. Order the fields in the same order you want users to see them. Note 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.

You can change the behavior of profile fields by clicking the attribute icons under **Manage Properties**. These icons define the field's behavior in the system, such as who can see it or whether it's editable. We recommend that you consider the field visibility. For example, in external-facing communities, people might not want their phone number widely visible.

Note: Only visible fields are available when searching or browsing.

The attributes should reflect how people use profiles. 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 are not 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 to be no earlier than last year.
-  Searchable: A searchable field is available to the search engine.

-  Editable: People can edit their editable profile fields.
-  Externally Managed: Enables users to set this field to their own visibility preferences.

Creating new user profile fields

You can create custom fields for user profiles. This can be useful if you want to show a unique aspect of your users, such as Astrological Sign or Pet's Name.

- **Admin Console** > **People** > **Global Profile Settings**

To create a custom profile field for user profiles:

1. Go to the configuration page:
   - **Admin Console** > **People** > **Global Profile Settings**
2. Click **Create New Field**.

   This opens the **New Profile Wizard** page.
3. Choose the field type. You can choose from one of the available types to help provide the best user experience for this field's information.
4. Click **Continue**.
5. Under **Name and Type**, in **Field Name**, 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.
6. Under **Translations**, enter the display name for the default language, and click **Add Translation** for each language you want to provide translations for.

   This is what the user sees in their profile field.
7. Under **Visibility**, select the **Users may edit the visibility for this profile field** check box to let users edit their own profile field's visibility or clear the check box to set visibility to the default value for all users.

   Note: Only visible fields are available when searching or browsing.
8. Under **Visibility**, select the default visibility for the field from the available list.
9. Under **Attributes**, specify the following attributes for the field:
   - Required: People are not 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 to be no earlier than last year.

- Searchable: A searchable field is available to the search engine.
- Editable: People can edit their editable profile fields.
- Externally Managed: Enables users to set this field to their own visibility preferences.

10. Click **Finish** to create the field.

The new field is added to the **Other Profile Fields** section on the **Global Profile Settings** and pages.

Setting up LDAP and Active Directory

By default, Jive doesn't use a directory server and stores all user data in a database from where it uses it for authentication. 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. During setup, you can choose users and groups stored in the directory server for providing them access to Jive.

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

Note: If you are using Active Directory, make sure it allows LDAP querying.

LDAP Security

The Jive application database never caches or stores user credentials. However, if the LDAP system property `ldap.ldapDebugEnabled` is set to `true`, the directory server traffic can be logged, and user passwords can be exposed in plain text to the `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

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

Overview of directory server 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 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 complex products.

Gather information about your server configuration

To complete the integration setup, you need the following information.

- The address of your directory server and how it will communicate with Jive. If you are 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 Base DN 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 that are required to limit the number of users returned when you sync Jive to your LDAP tree. Without the filters, synchronizing to your directory server returns 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 field identifiers for any groups you want to map to permissions groups in Jive. You don't need to map any groups if you are going 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.

Connect your LDAP server with Jive instance

1. Start the directory server integration setup by going to the configuration page in the Admin Console:
   - **Admin Console** > **People** > **Directory Server**

   Note: The individual fields on this page have helpful tooltips that you can access by hovering on the question mark next to the field.

2. Enter your connection settings and test the connection by clicking **Test Settings** at the bottom of the tab. If you cannot connect, you may need to check your credentials. The account you are binding with must have read access to users and groups for the entire subtree rooted at the base DN.
3. Click **Save** to save your connection settings and display the rest of the configuration settings in tabs.

Map LDAP fields to Jive profile fields

1. In the **User Mapping** tab, 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 are updated from the directory server whenever a synchronization takes place. For more information, see Mapping users from a directory server on page 87.
2. Click **Test Settings** to validate your mappings against the directory server. If the attribute you specified cannot be found, you see an error message identifying the problem.
3. Click **Save** to save the mapping settings.

Synchronize permission groups

In the **Group Mapping** tab, 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.

Important:

Recommendations for synchronizing permission groups:

- When syncing LDAP groups to Jive, you should sync only the groups used by Jive. If you leave the **Group Filter** with the default setting, Jive will sync *all* groups a user is assigned to in LDAP.
- Maintaining less than 500 Jive user groups simplifies administration and minimizes any performance impact from having too many groups.
- After mapping groups from a directory server, you need a migration strategy to switch back to Jive for maintaining groups.

For more information, see Mapping groups from a directory server on page 88.

Set up account synchronization

Use the **User Synchronization** tab to determine when and how user information must be synchronized between LDAP and Jive. For more information, see Synchronizing LDAP users on page 90.

A LDAP group is synced into Jive only when a user from that LDAP group logs into your community. So you may not see all your LDAP groups synced into the community once you create the groups, but they will be synced over some time. To minimize the impact, the sync runs in small batches after the user logs into Jive.

For more information, see Synchronizing LDAP users on page 90.

Mapping users from a directory server

If you are provisioning users from a directory server, you can use the User Mapping tab to map selected user fields to be synched with your Jive user information.

Before you begin, make sure you have an active connection to an LDAP directory server in the **Server Configuration** tab to see the other configuration tabs. For more information, see Overview of directory server integration steps on page 85.

Fastpath:

- **Admin Console** > **People** > **Directory Server** , than the **User Mapping** tab

---

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

To set up user mapping:

1. Go to the directory server configuration page:
   - **Admin Console** > **People** > **Directory Server**
2. Make sure you defined a valid connection to an LDAP directory server in the **Server Configuration** tab.

   If you don't have a working connection established, you won't be able to see the rest of the configuration tabs.
3. In the **User Mapping** tab, map the user account fields to connect user accounts based on the LDAP fields to be used to create and enable a Jive account based on the directory listing.
4. 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 social group, specify a name-value pair by using the **User Type Field** and **External Contributor User Type Value** settings.
5. 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 by using a field that is predefined for this purpose, or you can use any other available name-value pair to disable users based on an attribute. You must also select **Disable federated user accounts not found in the directory** in the **User Synchronization** tab.

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**.

6. Specify any profile fields you want to synchronize by providing the field information from your directory.
7. If you want to narrow down the number of users to be synched, use the **User Filter** and **User RDN** fields to apply the user filters. For more information about preparing user filters, see Overview of directory server integration steps on page 85.

Mapping groups from a directory server

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

Before you begin, make sure you have an active connection to an LDAP directory server in the **Server Configuration** tab to see the other configuration tabs. For more information, see Overview of directory server integration steps on page 85.

Fastpath:

- **Admin Console** > **People** > **Directory Server** , than the **Group Mapping** tab

Important:

Recommendations for synchronizing permission groups:

- When syncing LDAP groups to Jive, you should sync only the groups used by Jive. If you leave the **Group Filter** with the default setting, Jive will sync *all* groups a user is assigned to in LDAP.
- Maintaining less than 500 Jive user groups simplifies administration and minimizes any performance impact from having too many groups.
- After mapping groups from a directory server, you need a migration strategy to switch back to Jive for maintaining groups.

To connect your LDAP groups to Jive:

1. Go to the directory server configuration page:
   - **Admin Console** > **People** > **Directory Server**
2. Make sure you defined a valid connection to an LDAP directory server in the **Server Configuration** tab.

If you don't have a working connection established, you won't be able to see the rest of the configuration tabs.

3. If necessary, define and save user mappings. For more information, see Mapping users from a directory server on page 87.
4. In the **Group Mapping** tab, select **Use LDAP to manage Groups** and provide the group mapping information for your directory server.
5. Click **Test Settings** to validate group mappings against the directory server.
6. Click **Save** to save group mapping.

Note: A LDAP group is synced into Jive only when a user from that LDAP group logs into your community. For more information, see Synchronizing LDAP users on page 90.

Using LDIF to inventory your directory

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

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

Any LDAP directory browser provides the ability to export to and import from an LDIF file.

LDIF output example

If you are using Active Directory, you can use the ldifde command line tool. For more information about ldifde, see http://support.microsoft.com/kb/237677 on the Microsoft portal.

Here is an example of the `ldifde` command which yields an LDIF output:

```
ldifde -f output.txt -d ou=Jive_Users,dc=support,dc=jive,dc=com
```

The resulting LDIF output:

```
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 synch users or synch them during a nightly batch job, but make sure for good performance you use the correct rules.

Before you begin, make sure you have an active connection to an LDAP directory server in the **Server Configuration** tab to see the other configuration tabs. For more information, see Overview of directory server integration steps on page 85.

Fastpath:

- **Admin Console** > **People** > **Directory Server** , than the **User Synchronization** tab

---

Typically the application is configured to synchronize a user profile to LDAP each time the user logs in to the community. Additionally, you can also run the synchronization nightly to catch up with any changes during the day. However, you may want to sync users 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. Go to the directory server configuration page:
   - **Admin Console** > **People** > **Directory Server**
2. Make sure you defined a valid connection to an LDAP directory server in the **Server Configuration** tab.

If you don't have a working connection established, you won't be able to see the rest of the configuration tabs.

3. In the **User Synchronization** tab, specify the synchronization setting.
   a) If you want to synch fields every night automatically, select **Scheduled sync task enabled**.
   b) If you want to synchronize each user fields whenever they log in, select **Synchronize user profiles on login**.
   c) 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.
4. Click **Save Changes** to save the configuration.
5. If you want to synch accounts immediately, click **Run Synchronization Task Now**.

A LDAP group is synced into Jive only when a user from that LDAP group logs into your community. So you may not see all your LDAP groups synced into the community once you create the groups, but they will be synced over some time. To minimize the impact, the sync runs in small batches after the user logs into Jive.

Setting up Single Sign-On

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

Fastpath:

- **Admin Console** > **People** > **Single Sign-On**

You can use Jive's local database storage to authenticate users out of the box; this is a default setting. 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. We recommend you to implement SSO as part of a larger audience profile synchronization effort that includes LDAP and SAML.

Understanding SSO with SAML

When you implement single sign-on (SSO) with SAML 2.0, information for each user is passed from the identity provider 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 the 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, you should know the requirements and best practices.

A successful SAML implementation requires the following prerequisites.

- SAML is a protocol for exchanging authentication credentials between two parties, a service provider (SP) and an identity provider (IdP).
- An identity provider that complies with the SAML 2.0 standard. You should make sure you have required knowledge of how to configure your identity provider before proceeding.

For more information, see SAML identity providers on page 94.

- 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 that the details of how SAML works. Alternatively, you should enlist the assistance of a SAML professional. For more information about SAML, see Oasis SAML Technical Overview (.pdf) at http://www.oasis-open.org/committees/download.php/27819/sstc-saml-tech-overview-2.0-cd-02.pdf.

Note: You need Full Access administrator rights to configure SAML SSO. Support or another Full Access administrator in your organization can grant you this access.

SSL implementation

It is theoretically possible to implement SSO without SSL, but this raises some difficult security challenges. You should implement SSL and set your `jiveURL` to `https`, not `http`.

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. For more information, see Setting up LDAP and Active Directory on page 84.

Migrating existing 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 the username identity to sync them.
- Add the external IDs in Jive and federate the users by using 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.

If you have non-federated 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.
  - 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, contact 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 must be included in the Jive Community, and with what rights. For example, you need to decide whether all your organization users should be able to create accounts in the Jive community and whether you assign them to user groups for authorization. If you're primarily responsible for the technical implementation of this feature, you should discuss these decisions with your Community Administrator.

SAML identity providers

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

Commonly used IdPs

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

Microsoft ADFS	This is the most common SSO provider used by our customers. For more information, see http://msdn.microsoft.com/en-us/library/bb897402.aspx at the Microsoft portal.
Shibboleth	This is the open-source standard for IdPs. For more information, see http://shibboleth.internet2.edu/.

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

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.

Note: We 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 by using the Base metadata URL in the **Advanced** tab of your SAML SSO settings, is the same as the `jiveURL`.

Configuring SSO with SAML

Here you can find SAML configuration for your community. You can set up single sign-on with a SAML identity provider, or enable, disable, or tweak a configured SAML SSO configuration.

Fastpath:

- **Admin Console** > **People** > **Single Sign-On** , then the **SAML** tab

For more information, see Understanding SSO with SAML on page 92.

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. For more information, see Getting ready to implement SAML SSO on page 92.

Setting up the IdP connection

To begin setting up the connection between Jive and your identity provider:

1. Go to the configuration page:
   - **Admin Console** > **People** > **Single Sign-On** , then the **SAML** tab
2. On the **IDP Metadata** tab, paste in the XML containing the connection metadata.
3. Click **Save All SAML Settings** to load the XML.
4. On the **User Attribute Mapping** tab, map the user attributes in the Jive profile to your IdP's attributes.

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. For more information, see User attribute mapping on page 96.

5. If you want to assign users to groups by passing a special group attribute from your IdP to Jive, select **Group Mapping Enabled**.
6. Click **Save Settings**.
7. Click **Download Jive SP Metadata** at the top right of the **SAML** tab to download the Service Provider metadata you 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 then select the **Federated** check box.

Any fields you don't map are user-configurable in the Jive profile settings. Any field that you specify, but do not mark as federated, is populated with the specified value but still configurable.

By default, Jive uses the `NameID` property as the unique key 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 user groups for authorization automatically by passing a special group attribute from the IdP to Jive.

- To enable user group mapping and provide the attribute, select **Group Mapping Enabled** on the **Advanced** tab.

The group mapping attribute is used to get user group names from each assertion. If the corresponding user groups with these names do not exist, they are created when you synchronize, and users are 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 by using user groups created in Jive.

SAML SSO group mapping

You can manage your user groups by using either your IdP or local permissions groups. You can also use a mix of both kinds of groups. Only federated permissions groups are managed by using SAML.

Fastpath:

- **Admin Console** > **People** > **Single Sign-On** , then the **SAML** > **Advanced** tab

To manage groups with SAML, you initially enable group mapping and provide the group mapping attribute. You can assign users to security groups automatically by passing the group mapping attribute from the IdP to Jive. This attribute is used to retrieve security group names from each assertion. If a group specified within the group mapping attribute doesn't already exist in Jive, it will be created when you synchronize, and the user will be added to the group. If a group specified within the group mapping attribute does already exist in Jive but is not federated, it will automatically be federated.

To manage groups using SAML:

1. Go to the configuration page:
   - **Admin Console** > **People** > **Single Sign-On** , then the **SAML** > **Advanced** tab
2. Select the **Group Mapping Enabled** check box and provide the group mapping attribute in **Group Name Attribute**.
3. In the SAML response, pass the name of each group in the response for each user. Each group name should be listed as a separate attribute value as shown in the following example:

```
 <Attribute name="groups">
      <AttributeValue>groupOne</AttributeValue>
      <AttributeValue>groupTwo</AttributeValue>
      <AttributeValue>groupThree</AttributeValue>
</Attribute>
```

   The groups you specified in the `groups` attribute will automatically be federated when user members are synchronized at login.

SAML SSO attribute mapping tips

Here you can find general tips on attribute mapping for SAML SSO.

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`

Mixed-mode authentication

You can configure Jive so that it allows you to use SAML SSO for some users, and forms authentication for others. The Login Entry Page settings determine the initial login page wording if you have enabled externally accessible groups, or if your community uses SAML SSO, and you have also enabled form-based authentication for non-SSO users.

Fastpath:

- **Advanced Admin Console** > **People** > **Settings** > **Login Settings**
- **Admin Console** > **People** > **Single Sign-On** , then **Login Entry Page** tab

---

Mixed-mode authentication assumes that some of your users are provisioned from a SAML IdP, and others will be self-registered or created by another method. These two kinds of users will access the application via different login pages.

You can use the Login Entry Page settings to customize how different 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 determine which language they see.

To set up mixed-mode authentication:

1. Set up SAML SSO as described in Configuring SSO with SAML on page 95.
2. In the Advanced Admin Console, go to **People** > **Settings** > **Login Settings** .
3. Select **Enabled** for **Enable Form-based Login**.
4. Click **Save Settings**.

This enables a dual login page since SSO users will log in differently than non-SSO users.

5. Go to the **Login Entry Configuration** page:
   - **Admin Console** > **People** > **Single Sign-On** , then **Login Entry Page** tab
6. Provide text for each type of login.

   By default, the application shows the options as employee and non-employee, but you can customize the text to guide your users to the correct login. For more information about login entry page configuration, see Login pages on page 99.

Login pages

The Login Entry Page settings determine the initial login page wording if you have enabled externally accessible groups, or if your community uses SAML SSO, and you have also enabled form-based authentication for non-SSO users.

Fastpath:

- **Admin Console** > **People** > **Single Sign-On** , then **Login Entry Page** tab

If you enabled non-SSO users to use your site by using the form-based login, or you enabled externally-accessible groups, you can use the Login Entry Page settings to customize how different 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 determines which language they see.

To configure the login entry page:

1. Make sure SAML SSO is configured in your community.
2. Enable external groups, as described in Enabling external groups on page 153, or enable the form-based login, as described in Mixed-mode authentication on page 98.

   Now the **Login Entry Page** tab becomes available on the **Single Sign On** page.
3. Go to the **Single Sign On** page:
   - **Admin Console** > **People** > **Single Sign-On** , then **Login Entry Page** tab
4. In **Language**, 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 see the first time they navigate to the site directly, as opposed to clicking through from an invitation.
5. If required, 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. Note when you design your text that your regular community users are typically logged in automatically by using SSO, while external users need to provide user name and password to access the site.

6. Click **Save**.

   If you want to revert to the original text at any time, you can click **Reset to Defaults**.

General SAML integration settings

Here you can find the general settings reference of the SAML SSO configuration.

Fastpath:

- **Admin Console** > **People** > **Single Sign-On** , then the **SAML** tab

On the **SAML** > **General** tab of the **Single Sign-On** page you can find the most commonly used SSO configuration properties.

Enabled	Enable this setting to enable SAML SSO for your community.
Debug Mode	Enable this setting 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 by using SSO, they will not have an associated `external ID`. When **Username identity** is enabled, Jive maps 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 enabling **Merge Local Users**, make sure your existing users are marked as federated users. Otherwise, non-federated 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 add users to the Jive community before enabling SSO.
Enable disabled user	Enable this setting to reenable disabled user Jive accounts when they log in.

account on login	
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 the signature to be valid. At the same time, 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	Define 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 used commonly. 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 some browser versions and some firewalls have restrictions on the length of the HTTP path. **Note:** If you're configuring ADFS, note 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 Single Logout (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.
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.

Fastpath:

- **Admin Console** > **People** > **Single Sign-On** , then the **SAML** tab

On the **SAML** > **Advanced** tab of the **Single Sign-On** page you can find the less commonly used SSO configuration properties.

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.
Force Authentication	This setting forces any user with an existing IdP session to log in again.
Passive Authentication	When guest access is enabled, this issues a SAML AuthnRequest upon first access with `isPassive=true`, which should cause the IdP to 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 is signed. If you use ADFS, you must clear this check box.
IDP Want Response Signed	Adds 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 that is used in the digital signatures within the SAML messages. Most IdPs use the default value of the namespace, as specified at http://www.w3.org/2001/04/xmldsig-more#rsa-sha256. You may need to change this value if your IdP uses a different algorithm.
Group Mapping Enabled	Enable this property if you plan to use one of the SAML Response Assertion Attributes to synchronize the user into Permission Groups. For more information, see SAML SSO group mapping on page 97.
Require Valid Metadata	Use this setting to determine whether the IdP metadata which 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.
Include Scoping	Some IdPs may require a scoping definition. This option is disabled by default. If you use ADFS, it must remain disabled.
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 two proxy redirects, adjust this value accordingly.
Validate InResponseTo	Defines if `InResponseTo` is validated from incoming SAML responses. By default, the setting is enabled.

Troubleshooting SAML SSO

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

Fastpath:

- **Admin Console** > **People** > **Single Sign-On** , then the **SAML** tab

You can enable the debug mode by selecting the **Debug** check box on the **Single Sign-On** > **SAML** tab. You should disable this setting in production.

An attribute is missing or was mistyped

In the following sample error message, the name of the attribute configured for the user 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.SSOAuthenticationException:
 User did not have the required attributes send from the
```

```
identity provider. Missing attribute: email. Given attributes:
 [MAIL, title, companyname, FIRSTNAME, LASTNAME]
```

"Missing attribute" field in an error message is blank

If Jive is trying to sync a single name as `Firstname` and `Last-name`, you will see a message like this:

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

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 succeeds on some nodes and fail on others. To verify that the same key is being used on each node, go directly to the `/saml/metadata` path for each node.

This problem occurs when the Storage Provider File system caching is enabled. To disable it, go to **System** > **Settings** > **Storage Provider** , click **Edit**, and then select **No** under **Cache Enabled**.

"Responder" message

A status message in the following format indicates a problem with your IdP configuration.

```
<samlp:Status>
<samlp:StatusCode
Value="urn:oasis:names:tc:SAML:2.0:status:Responder"/>
<samlp:StatusMessage>something_is_wrong</samlp:StatusMessage>

</samlp:Status>
```

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 following 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. For more information, see Response Skew on page 102 in Configuring SSO with SAML on page 95.

usernamedoesn't exist in attribute

If the attribute with the username does not exist, you can see the following message:

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

The attribute may be located in the `Subject NameID` instead, in which case you should make sure the `Override Subject NameID` for `Username` checkbox is cleared on 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. For more information, see Advanced SAML integration settings on page 102.

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 external login

When you implement single sign-on (SSO) by using an external login, users can choose to log in by using Facebook Connect, or Google OpenID Connect.

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 a 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 include Facebook Connect or Google OpenID Connect authentication. Both Google OpenID Connect and Facebook Connect use the Attribute Exchange standard for exchanging information, which enables Jive to pull in profile information about new users. After logging in, 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.

Migrating existing 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 the username identity to sync them.
- Add the external IDs in Jive and federate the users by using 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.

If you have non-federated 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.

Configuring SSO with external login

Here you find instruction on enabling SSO with Facebook Connect and Google OpenID Connect.

Fastpath:

- **Admin Console** > **People** > **Single Sign-On** , then **General** and **External Login** tabs

---

You can enable either external login or externally accessible groups.

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. For more information, see Understanding SSO with external login on page 105.

To implement SSO for Jive with external logins, you set the **Single Sign-On** > **External Login** page to **Enabled**. 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** on the **Single Sign-On** > **External Login** page. 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. Then you should provide your app credentials (the Application ID and secret) in the Jive application to complete SSO authentication with Facebook.

To enable Facebook authentication:

1. Set up an app on the Facebook developer site. When you're creating your Facebook app, you need to provide your Jive URL for both the **App Domains** field and the **Website with Facebook Login** field.
2. Make a note of both the application id and the application secret: you need them to configure SSO.
3. Go to the SSO configuration page:
   - **Admin Console** > **People** > **Single Sign-On**
4. On the **General** tab, select the **Enable Username Confirmation for New Users** check box.
5. On the **External Login** tab, under **Facebook**, provide the client ID and secret.

Google OpenID Connect configuration

Google OpenID Connect requires an ID and secret from a Google Developers Console project. You can the instructions on obtaining the ID and secret on the Google IdentityPlatformathttps://developers.google.com/identity/protocols/OpenIDConnect.

Google OpenID Connect replaces OpenID 2.0, which is no longer supported by Google. You should only need to specify a realm in case of a migration.

To enable SSO with Google on the Jive side:

1. Go to the SSO configuration page:
   - **Admin Console** > **People** > **Single Sign-On**
2. On the **General** tab, select the **Enable Username Confirmation for New Users** check box.
3. On the **External Login** tab, under **Google OpenID Connect**, provide the client ID and secret.

SSO global settings reference

The general SOO settings described here apply to all configured SSO implementations.

- **Admin Console** > **People** > **Single Sign-On** , then **General** tab

Enable Username Confirmation for New Users, Enable Email Confirmation for New Users	Use these settings to define the behavior for new users when they first log in. When enabled, users are 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 and 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 by using External ID.

Allow Federated Users to Change Name	Use this setting if you want federated users to be able to change their names in the profile settings and have the change propagated to the IdP.
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 or all uppercase.

Managing permissions

You can control user access to administrative settings, spaces, blogs, social groups, and content. To configure access, you grant or revoke permissions to individual users or groups of users that you define. You can use the standard permission levels included with the application or create your own.

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. You can't break out the bundled permissions in the administrative area (as you can with space permissions). For more information, see Managing System Administration permissions on page 114.
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. For more information, see Managing space permissions on page 120.
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 on page 132.

Social Groups These permissions allow users to view and create social groups. Projects contained by a group inherit the permissions of their container group. For more information, see Managing social group permissions on page 134.

Content 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. For more information, see Managing Home page and other content permissions on page 138.

Default permissions for content items

Here you can find a reference of the default permissions for content items.

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 five avatars*
Profile Images	• View • Create • Create up to 10 images*
User Profile Fields	• Edit and view all fields except the Mobile phone number field • Mobile phone number field: Edit and view, but only Connections can view this by default

* This is the default setting. It can be changed in your community.

Overview of permission assignments

When assigning permissions, you follow these basic steps.

While you can assign permissions to individuals, you 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, and people in the Products department. You create user groups based on how you want to structure access to your community and its features.

1. Create user groups, as described in Creating user groups. Add user groups to different areas: system administration, spaces, social groups, blogs, and content. For more information, see Managing user groups on page 65.
2. Assign permissions to user groups in one of the following ways:
   a) Assign permission levels to groups. Note that administrative permissions and spaces have several bundled permissions levels. You can also create custom space permission levels. For more information, see Overview of System Administration permission levels on page 114 and Overview of space permission levels on page 121.
   b) Assign one or more access permissions, as described in Setting up permissions for user groups on page 113. For blogs, social groups, and the rest, you assign access by choosing from a list of fine-grained options.
3. Assign permissions to individual users by creating user override for special cases, as described in Creating user overrides on page 113. 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.

Overview of user groups

A Jive community includes three predefined user groups and you can create more user -groups for assigning permissions.

You can define a set group of users to quickly assign them a variety of permissions. Forming user groups that reflect the kinds of access to be granted lets you use a convenient, built-in way to manage people's access to application features.

For more information about user groups, see Managing user groups on page 65.

These groups can be defined in your community itself, in an external user identity system (such as an LDAP system), or in the application database. Additionally, several system-defined user groups are available by default.

System-defined user groups: Everyone and All Registered Users

The application includes three user groups that are defined by the system: Everyone, All Registered Users, and All External Contributor 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 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 only 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.
- **All External Contributor Users** includes external users who are not members of the community but have some access to community resources. For more information about external users, see Managing external groups on page 153.

Your user groups

You can set up your own user groups. We recommend that these groups should 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 — for example, with groups representing departments in your organization, people with specific privileges (such as blogging), virtual teams within the organization.

Creating user groups

You add user groups by creating and naming a group, then adding user accounts for each of the group's members. You should also add one or more user accounts as administrators for the group.

Fastpath:

- **Admin Console** > **Permissions** > **User Groups** , then click **Create New User Group**

You can assign role badges to groups. Role badges provide visual cues in the user interface that help people quickly identify community users and their responsibilities. For more information see Adding and removing users to user groups on page 67.

To create a user group:

1. Go to the configuration page:
   - **Admin Console** > **Permissions** > **User Groups** , then click **Create New User Group**
2. Under **General Settings**, in **User Group Name**, enter a user group name.

   The name should be meaningful and convey the group purpose, for example, HR_bloggers or Support_specialists.
3. In **Description (optional)**, enter the description of the user group.

   You should add the information about this group purpose and who is included in it.
4. If the group can be used as part of the News audience, select the **Visible to News Admins** check box.
5. If you want to use role badges, do the following:
   a) Under **Role Badge**, select **Enabled**.
   b) In **Badge Image**, browse and upload a 16 by 16 pixel image to be used as the role badge.
   c) Select the role for the users in this user group from the following roles:
   - Administrator
   - Champion
   - Employee
   - Expert
   - Moderator
   - Support
6. Click **Create Group**.
7. Use the **Add Members** links to add user accounts of the members of the new user group. For more information see Adding and removing users to user groups on page 67.
8. Use the **Add Admins** links to add user accounts for users who have permission to administer the account. If you use the badge roles, they are not applied to the administrators. For more information see Adding and removing users to user groups on page 67.
9. 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.

Setting up permissions for user groups

You set up permissions in the Admin Console to grant various levels of access to individuals or groups of users you define.

This is a general overview of the steps you should take to assign permissions to a user group. You can find the detailed procedures in other documentation sections.

To set up permissions:

1. On the permissions page, under **Groups with access**, review permissions to user groups.
2. To assign permissions to a user group not yet added:
   a. Click **Add group**.
   b. Enter the name of the user group to add.
   c. Click **Select Permissions**.
   d. In the dialog box, select the permissions you want to apply for the user group.
3. To edit permissions for a user group already added:
   a. Locate the group in the list.
   b. Next to its name, click **edit permissions**.
   c. In the dialog box, select the permissions you want to apply for the user group.
4. Click **Set Permissions**.

Creating user overrides

For particular users, you can create 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.

This is a general overview of the steps you should take to configure user overrides. You can find the detailed procedures in other documentation sections.

About user overrides

To grant a particular set of permissions to an individual, you create a user override. An override can be used if:

- A user 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 user 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 — if the person is an exception to the rule. For example, you might want to separately define the user permissions to enhance or limit their access in the place.

Creating user overrides

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 **Set override** to view the permissions you can assign.
4. In the permissions dialog box, select and clear check boxes to assign the user only the required permissions.

   Note that you clear a check box to remove a permission — there's no need to revoke the permission explicitly.
5. Click **Set Permissions** to save the override you've created.

The user has the permissions you configured.

Managing System Administration permissions

A user with system administration permissions can make configuration changes to the system, as well as manage spaces and user accounts.

System administration permissions give designated users the ability to keep the application running. Assign these permissions to delegate behind-the-scenes work.

Fastpath:

- **Admin Console** > **Permissions** > **System Administrators**

Overview of System Administration permission levels

You can 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 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.
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.
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.
Moderate Content	This permission level allows the users 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 passes through their queue before it appears in the community.
Manage Users	This permission level allows the users to manage the users of the application. For more information, see Managing user accounts and user groups on page 64.
Manage Groups	This permission level allows the users to create and manage user groups, such as for assigning permissions. For more information, see Managing user accounts and user groups on page 64.
Manage News Streams	This permission level allows the users to manage the News page, including creating and managing news streams for users and creating and configuring tiles on the News page. For more information about news streams, see Customizing News page on page 52.
Manage Support Center	This permission level allows the users to configure the Support Center layout by adding sections and places, designing the background, or changing the header text. This permission is only useful if you have the Support Center enabled, which can be done by creating a case with Support. For more information, see Managing Support Center on page 41.

How administrative permission levels affect access

Administrative permission levels control access to the Admin Console. Here you can find the sections of the Admin 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.
- Users with only Manage News Streams permissions cannot see the Admin Console.

Table 8: Overview

Console page	Manage community	Manage system	Moderate content	Manage users	Manage groups
Overview			Ø		

Table 9: System

Console page	Manage community	Manage system	Moderate content	Manage users	Manage groups
System > **Management**					
All pages			Ø	Ø	Ø
System > **Settings**					
All pages			Ø	Ø	Ø
System > **Moderation**					
Moderation Configuration			Ø		Ø
Config Spam Prevention			Ø	Ø	Ø
Spam Link Domain WL			Ø	Ø	Ø

Table 10: Spaces

Console page	Manage community	Manage system	Moderate content	Manage users	Manage groups
Spaces > **Management**					
All pages		Ø	Ø	Ø	Ø
Spaces > **Settings**					
All pages		Ø	Ø	Ø	Ø

Table 11: Blogs

Console page	Manage community	Manage system	Moderate content	Manage users	Manage groups
Blogs > **Management**					
All pages			Ø	Ø	Ø
Blogs > **Settings**					
All pages			Ø	Ø	Ø

Table 12: People

Console page	Manage community	Manage system	Moderate content	Manage users	Manage groups
People > **Management**					
User Search			Ø		
Create User			Ø		Ø
Group Summary			Ø	Ø	
Create Group			Ø	Ø	
User Relationships			Ø		Ø
Org Chart			Ø		Ø
People > **Settings**					
Avatar Settings			Ø	Ø	Ø
Ban Settings			Ø		Ø
Directory Server Settings			Ø	Ø	Ø
Forgot Username			Ø	Ø	Ø
Guest Settings			Ø	Ø	Ø
Hover Card Settings			Ø		Ø
Login Security			Ø	Ø	Ø
Org Chart Settings			Ø	Ø	Ø
Password Reset			Ø	Ø	Ø
Profile Image Moderation			Ø	Ø	Ø
Profile Settings			Ø		Ø

Console page	Manage community	Manage system	Moderate content	Manage users	Manage groups
Registration Settings			Ø	Ø	Ø
Single Sign On			Ø	Ø	Ø
Status Level Settings			Ø	Ø	Ø
Terms and Conditions			Ø	Ø	Ø
User Status Update Settings			Ø	Ø	Ø

Table 13: Permissions

Console page	Manage community	Manage system	Moderate content	Manage users	Manage groups
All pages			Ø	Ø	Ø

Table 14: Mobile

Console page	Manage community	Manage system	Moderate content	Manage users	Manage groups
All pages			Ø	Ø	Ø

Table 15: Add-ons

Console page	Manage community	Manage system	Moderate content	Manage users	Manage groups
All pages			Ø	Ø	Ø

Table 16: Video

Console page	Manage community	Manage system	Moderate content	Manage users	Manage groups
Preferences			Ø	Ø	Ø

Table 17: Events

Console page	Manage community	Manage system	Moderate content	Manage users	Manage groups
General			Ø	Ø	Ø

Table 18: Ideas

Console page	Manage community	Manage system	Moderate content	Manage users	Manage groups
All pages			Ø	Ø	Ø

Setting up administrative permissions for user groups

You can assign groups of users the system administrator permissions.

Fastpath:

- **Admin Console** > **Permissions** > **System Administrators**

To set up administrative permissions for user groups in the Admin Console:

1. Go to the configuration page:
   - **Admin Console** > **Permissions** > **System Administrators**
2. To assign permissions to a user group not yet listed:
   a) Click **Add group**.
   b) Enter the name of the user group to add.
   c) Click the **Select Permissions** button.
   d) In the **System Administration Permissions for <user_group>** dialog box, select check boxes for the permission levels you want to apply for the user group and clear check boxes for the permissions to be removed.
   e) Click **Set Permissions**.

   The selected permissions are granted to the user group.
3. To edit permissions for a user group already listed:
   a) Locate the group in the list.
   b) Next to its permission level, click **edit permissions**.
   c) In the **System Administration Permissions for <user_group>** dialog box, select check boxes for the permission levels you want to apply for the user group and clear check boxes for the permissions to be removed.
   d) Click **Set Permissions**.

   The selected permissions are granted to the user group.

Managing space permissions

Spaces are places where users can post content such as documents, discussions, and blog posts. You can assign users or user groups a variety of space permissions to control their level of access to the space.

Space permissions have various levels and customization options. For more information, see Overview of space permission levels on page 121.

At a high level, setting up space permissions typically includes these steps:

1. Create user groups that capture how you want to grant access to the community's features. For more information, see Overview of user groups on page 110.
2. Set the default space permissions. These should represent the access you 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: Projects and sub-spaces inherit the permissions of their parent space. Social groups, however, are independent of spaces. For more information, see Managing social group permissions on page 134.

Overview of space permission levels

Jive includes several standard space permission levels, such as a Moderator or Administrator, that you can assign to individual users or groups of users that you define. Additionally you can create your own custom space permission levels.

When you assign permissions for access to a space, you can assign a level, and then further customize as needed with overrides for particular users.

Standard space permission levels	These permission levels are designed for common roles, such as a space Administrator, a Moderator. These permission levels control how users access space features at a high level. For more information, see Standard space permission levels on page 127.
Custom space permission levels and user overrides	Create a custom space permission level to allow fine-grained access to the 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). For more information, see Custom permission levels and user overrides for spaces on page 128.

Note: Projects and sub-spaces inherit the permissions of the space that contain them. Social groups, on the other hand, are independent of spaces. For more, see Managing social group permissions on page 134.

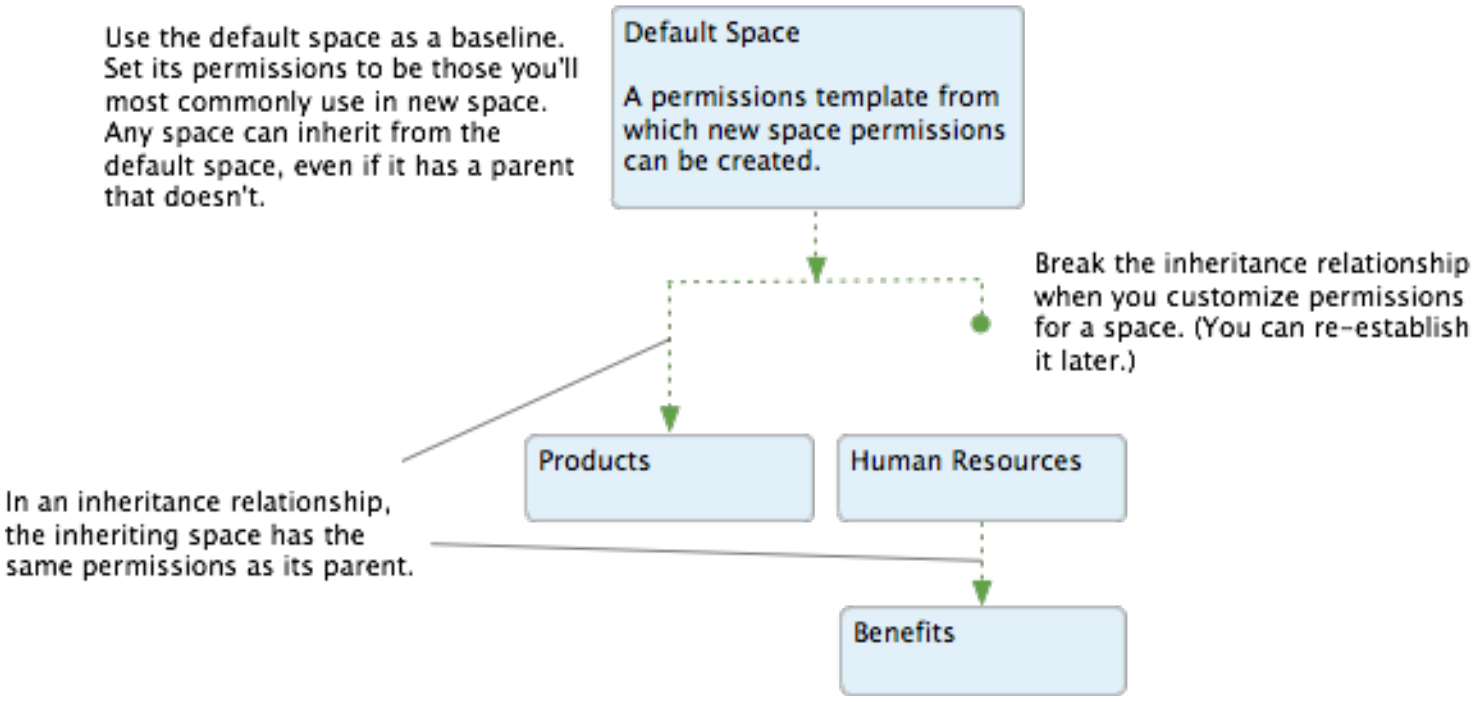
How spaces inherit permissions

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 use those permissions as a starting point.

When a space a created, it inherits permissions from the parent space. The inheritance relationship means that changes to the parent space permissions automatically change permissions in inheriting spaces and sub-spaces. A root space typically called *community* 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 root space is useful as a permission template.

Note: The Admin Console provides cues about inheritance for a particular space — for example, by noting how many spaces inherit permissions from it.

Important inheritance characteristics



- You can customize the root space permissions to represent a permission set that is commonly used when creating new spaces. A new space can use these, if only as a starting point.
- A space inherits its parent space permissions, a relationship that must be broken before the sub-space permissions can be customized. For spaces at the top level, the root 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 in spaces that inherit from the sub-space.

- A new space can begin with its parent space permissions as a starting point only. When it does, those permissions aren't inherited, thus providing a basis for customization.
- A new space can begin with the default space 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.

Customizing root space permissions

The community includes a root space, called *community* by default. From there you can add more spaces to create a hierarchy.

Fastpath:

- **Admin Console** > **Permissions** > **Spaces**

The root 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 root space's, if only as a starting point to customize. You can customize the root space, setting commonly-used permissions that make sense for new spaces to have.

The root space permissions are applied to all top-level spaces which inherit the settings and are used as the default setting when creating a new space. For more information on setting up permissions, see Overview of permission assignments on page 110.

To customize root space permissions:

1. Go to the configuration page:

   - **Admin Console** > **Permissions** > **Spaces** , then click  > **Configure permissions** next to the name of the root space.

     The root space is the top one in the list; it's called `community` by default.

   This opens the **Default Space Permissions** page where you can set up the default permissions for the community.

2. Set up permissions for user groups.

   a. On the permissions page, under **Groups with access**, review permissions to user groups.

   b. To assign permissions to a user group not yet added:

      a. Click **Add group**.

      b. Enter the name of the user group to you want to add.

      c. Under **Select Permissions**, select the default permission level for the group.

You can choose one of the default permission levels or click **View/edit custom level** and define custom permissions for the group.

d. Click **Add Group**.

The group is added to the list and the group members are assigned the configured permissions.

3. Set up permissions for individual users.

Attention: We recommend creating and employing user groups with necessary permissions instead of assigning permissions for individual users.

a. Under **User Overrides**, click **Create a user override**.

b. 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.

c. Click **Set exception**.

This opens the **Set exception** dialog box.

d. Under **Access and administration**, select the general permission level, and then select permissions for user.

e. Click **Save** to save the changes.

The permissions are applied to the selected user immediately.

Setting up user group permissions for spaces

For any space, you can assign various permission levels to individual users or groups of users.

Fastpath:

- **Admin Console** > **Permissions** > **Spaces**

You can assign custom permissions levels for any space or sub-space in the community. For more information about space permission levels and overrides, see Standard space permission levels on page 127 and Custom permission levels and user overrides for spaces on page 128. For user groups permissions, the user group must exist before you can assign it permissions.

To set up permissions for user groups to a space:

1. Go to the configuration page:

   - **Admin Console** > **Permissions** > **Spaces** , then click  > **Configure permissions** next to the name of the space.

   This opens the space's page.

2. Click **Customize this space's permissions** to start customizing space permissions.

   This option is available until the space inherits permissions from the parent place. If the space permissions are customized you will see a **This space is using a custom permission scheme** message.

3. 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) Under **Select Permissions**, select the default permission level for the group.

      You can choose one of the default permission levels or click **View/edit custom level** and define custom permissions for the user group.

   d) Click **Add Group**.

   The selected permissions are granted to the user group.
4. 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) Under **Select Permissions**, select the default permission level for the group.

      You can choose one of the default permission levels or click **View/edit custom level** and define custom permissions for the user group.

   d) Click **Save**.

   The selected permissions are granted to the user group.

Re-establishing permission inheritance between spaces

You can re-establish inheritance of permissions between parent spaces and their child spaces if the inheritance has been broken previously by customizing the child space permissions.

Fastpath:

- **Admin Console** > **Permissions** > **Spaces**

Note that by re-establishing inheritance you remove any customizations you've made to permissions in the sub-space and in spaces that inherit from the sub-space.

To re-establish permission inheritance between a parent space and its child space:

1. Go to the configuration page:

   - **Admin Console** > **Permissions** > **Spaces** , then click  > **Configure permissions** next to the name of the space.

   This opens the space's page.

2. Click **Re-establish permission inheritance to <space name>** and click **Apply** to confirm.

The inheritance from the parent place is re-established, all permission customizations of the child space are removed, and the permissions from the parent place are applied to the space.

Creating user overrides for spaces

You can create an override for an individual user of a space.

Fastpath:

- **Admin Console** > **Permissions** > **Spaces**

To grant a particular set of permissions to an individual, you create a user override. An override can be used if:

To create a user override for a space:

1. Go to the configuration page:

   - **Admin Console** > **Permissions** > **Spaces**

2. Click **Customize this space's permissions** to start customizing space permissions.

   This option is available until the space inherits permissions from the parent place. If the space permissions are customized you will see a **This space is using a custom permission scheme** message.

3. Under **User Overrides**, click **Create a user override**.
4. 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.
5. Click **Set override** to view the permissions you can assign.
6. In the permissions dialog box, select and clear check boxes to assign the user only the required permissions.

   Note that you clear a check box to remove a permission — there's no need to revoke the permission explicitly.

7. Click **Set Permissions** to save the override you've created.

The user has the permissions you configured.

Standard space permission levels

Jive includes several predefined space permission levels that you can assign to user groups or individual users.

You can see the list of space levels on the Space Permissions page in the Admin Console, on the **Standard Levels** tab.

Fastpath: Admin Console > **Permissions** > **Spaces**

Additionally, you can also add your own levels, as described in Custom permission levels and user overrides for spaces on page 128.

Standard levels overview

The following table lists the standard space permission levels, along with a summary of the access granted by each. The details on specific permissions are described in Access granted for each level on page 127.

Space permission level	Access granted
Administer	Design the space layout, read and write 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 user content
Create	Read and write all content types
Contribute	Comment on commentable content types and reply to questions and discussion threads
View	View content
Discuss	Read and write in discussions and questions, contribute on all other content types. This permission applies only for a space's own content.
No Access	Only applicable when creating a user override. Use this to prevent access to the space and no entitlements are set

Note: Shared content always inherit its own place's permission. For example, shared content from a private place may not be visible for other users with different permissions.

Access granted for each level

The following table lists each default space permission level, along with the specific permissions granted by each.

Space Permission Level	View	Create	Reply	Comment	Attach file	Insert image	Rate	Vote	Create Project	Create Announcement	Edit Comment	Delete Comment	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, and creating spaces beneath it.

Fastpath: Admin Console > **Permissions** > **Spaces**

When you create this kind of customization, your options are divided into three categories:

No access Available for a user override only, this option lets you 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. This is useful if you want to create a permission level that grants access to create discussion threads but only view documents.

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 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 is not able to see content from it.

Access Space

This category is used to grant custom content-specific access in the space. When you select this category while customizing, you have access to a list of the content types, each with a list of the access levels available for it. Choose an access level for each content type.

The following table lists the access levels that each content type permission level includes, along with the specific permissions each allows.

Table 19: Access Granted for Each Content Type Permission Level

Content Type Permission	View	Create	Reply	Comment	Rate	Vote
Create						
Create (for discussions and questions)						
Contribute		Ø				
View		Ø	Ø	Ø	Ø	Ø
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 which you want to be customizable.

The following table lists what's available in the **Advanced** level for each content type.

Table 20: Access settings available for each content type

Content Type	View	Create	Rate	Comment/Reply	Additional
External Object					
Discussion and question					
Poll					Vote
Blog Post					

Content Type	View	Create	Rate	Comment/Reply	Additional
Document					
Video					
Content share			Ø	Ø	
Idea					
Event					Insert Image

The following options are also available for customization.

Table 21: Additional access settings

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 briefly describes the available access levels with more details provided below.

Table 22: Manage space settings

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 queue but hasn't been approved yet. They can designate other space administrators.

Moderate Granting moderator permission gives someone two areas of access:

- A content moderator can approve or reject content before it's published. When moderation is on for the place in which the place was created (such as the space, social group, or globally), the content moderator for that place is 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 to be moderated. Note that this ability is not inherited in

sub-spaces; the moderator can approve or reject content only in the place where they've been assigned permission.

- A content moderator has access to certain links for handling content after it is 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.

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 remain in the queue until someone approves or rejects them there. Existing requests are not be routed to the next queue up. If there's only one moderator and that user 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 revoked for someone, then that user will still have access to the requests currently in the queue but won't be able to approve or reject them.

Note that in order to have moderators approve and reject content in a moderation queue, moderation needs to be enabled for specific content types.

Creating custom space permission levels

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** > **Permission Levels** .

For more information about custom space permission levels, see Custom permission levels and user overrides for spaces on page 128.

To create a custom space permission level:

1. In the Admin Console, go to .
2. On the **Custom Levels** tab, click **Create new permission level**.
3. In the **Create a Custom Permission Level** dialog box, enter a name and description for the permission level.

   These help other administrators know the purpose of the new level.

4. Under **Access and administration,** select a category for the level, then choose from among the options in the category.
5. 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 section describes the permission settings for blogs and how to configure them.

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).

Overview of global blog permission levels

Blog permission levels enable people to view, create, and comment on global blogs.

Global blogs are the ones 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). 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.

Permission	Access Granted
View blog	View and read all public blog posts
Create blog	Create and manage a personal blog, and author blog posts in it
Comment	Leave comments on public blog posts

Note: You configure settings and membership for global blogs by using the Blogs tab of the Advanced Admin Console.

Overview of non-global blog permission levels

Non-global blog permission levels enable people to view, create, and comment on blogs which are associated with specific places.

Managing permissions for non-global blogs varies depending on what kind of place the blog lives in. The following table gives a brief description of each:

Blog location	Permissions management
Space	You manage permissions for blogs in a space when you manage permissions for the space. For more information, see Managing space permissions on page 120.
Social group	Access for blogs in social groups is 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 allowed things tasks, such as viewing and posting. For more information, see Managing social group permissions on page 134.
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 information, see Managing space permissions on page 120.

Setting up global blog permissions for user groups

Global blogs are those that are not associated with a specific place. Here you can find how to set up global blog permissions for user groups.

Fastpath:

- **Admin Console** > **Permissions** > **Blogs**

For user groups permissions, the user group must exist before you can assign it permissions.

To set up permissions for user groups to a global blog:

1. Go to the configuration page:
   - **Admin Console** > **Permissions** > **Blogs**
2. On the permissions page, under **Groups with access**, review permissions to user groups.
3. To assign permissions to a user group not yet added:
   a. Click **Add group**.
   b. Enter the name of the user group to add.
   c. Click **Select Permissions**.
   d. In the dialog box, select the permissions you want to apply for the user group.

4. To edit permissions for a user group already added:
   a. Locate the group in the list.
   b. Next to its name, click **edit permissions**.
   c. In the dialog box, select the permissions you want to apply for the user group.
5. Click **Set Permissions**.

Setting up user overrides for global blogs

Global blogs are those that are not associated with a specific place. Here you can find how to set up overrides to global blogs for individual users.

Fastpath:

- **Admin Console** > **Permissions** > **Blogs**

To grant a particular set of permissions to an individual, you create a user override. An override can be used if:

To set up overrides for global blogs to individual users:

1. Go to the configuration page:
   - **Admin Console** > **Permissions** > **Blogs**
2. Under **User Overrides**, click **Create a user override**.
3. 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.
4. Click **Set override** to view the permissions you can assign.
5. In the permissions dialog box, select and clear check boxes to assign the user only the required permissions.

   Note that you clear a check box to remove a permission — there's no need to revoke the permission explicitly.
6. Click **Set Permissions** to save the override you've created.

The user has the permissions you configured.

Managing social group permissions

In social groups, users can create content such as documents, discussions, and blog posts, but whether users 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 that are 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 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.

Overview of 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.

Fastpath:

- **Admin Console** > **Permissions** > **Social Groups**

Permissions for each content type in a social group, however, are not configurable. They're essentially unlimited (such as read, create, comment, or attach file). Projects created inside a social group inherit these permissions.

Note: You should select **View social group** when granting access to create groups. Without that permission, users are not able to see aspects of the user interface 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. It must be selected in order for users to choose **Group** from the **New** menu in the user interface.
Create group (public)	Create a new a public or members only social group.
Create group (private)	Create a new private or secret (also known as private unlisted) social group.

Permission	Access granted
Manage social group	Manage any social groups.
Create externally accessible group	Create private and secret (also known as private unlisted) social groups that are accessible to invited external contributors.

Setting up social group permissions for user groups

Here you can find how to set up social group permissions for user groups.

Fastpath:

- **Admin Console** > **Permissions** > **Social Groups**

You can set social group permissions in the Admin Console on the Social Group Permissions page. For user groups permissions, the user group must exist before you can assign it permissions.

To set up permissions for user groups to a social group:

1. Go to the social groups configuration page:
   - **Admin Console** > **Permissions** > **Social Groups**
2. On the permissions page, under **Groups with access**, review permissions to user groups.
3. To assign permissions to a user group not yet added:
   a. Click **Add group**.
   b. Enter the name of the user group to add.
   c. Click **Select Permissions**.
   d. In the dialog box, select the permissions you want to apply for the user group.
4. To edit permissions for a user group already added:
   a. Locate the group in the list.
   b. Next to its name, click **edit permissions**.
   c. In the dialog box, select the permissions you want to apply for the user group.
5. Click **Set Permissions**.

Configuring user overrides to social groups

Here you can find how to configure overrides to social groups for individual users.

Fastpath:

- **Admin Console** > **Permissions** > **Social Groups**

To grant a particular set of permissions to an individual, you create a user override. An override can be used if:

To set up overrides for social groups to individual users:

1. Go to the social groups configuration page:
   - **Admin Console** > **Permissions** > **Social Groups**
2. Under **User Overrides**, click **Create a user override**.
3. 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.
4. Click **Set override** to view the permissions you can assign.
5. In the permissions dialog box, select and clear check boxes to assign the user only the required permissions.

   Note that you clear a check box to remove a permission — there's no need to revoke the permission explicitly.
6. Click **Set Permissions** to save the override you've created.

The user has the permissions you configured.

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 let them see any other content items that live in the group.

Fastpath:

- On the Group Activity page: **gear icon** > **Settings** > **Non-Member Content Editing**

To enable non-member content editing for private groups in your community:

1. Go to the configuration page:
   - On the Group Activity page: **gear icon** > **Settings** > **Non-Member Content Editing**
2. Select **Enable non-member content editing**.
3. Click **Save**.

With the setting enabled, owners of private groups see the option to enable non-member content editing when they are editing the private group. People with Create Group (Private) permissions see the option when creating (or editing) a private group. Note that Private: Unlisted, also known as 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 and other content permissions

The Other content permissions enable you to manage global permissions for features such as polls and announcements on the community Home page, as well as manage permissions that fine-tune the video and update features. These global permissions are not limited by any container.

Overview of Home page and Other Content permissions

Other Content 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 is displayed on the community Home 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.

Important: We do not recommend that you use widgets and widgetized Overview pages (including the Home page) in your community.

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. When setting permissions for the Home page, remember 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. For more information, see Overview of Home page and Other Content permissions on page 138.

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 Other Content Permissions page of the Admin Console.

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 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
Create and Repost status updates	Create their own status updates and repost someone else's update
Like status updates	Like status updates of other users, which affects their status points
Comment on updates	Comment on other user status updates
View status updates	Allows users to view updates that others post
Insert status update images	Add images to their update as an attachment
Insert comment images	Add images to comments on updates

Permission	Access Granted
DM/Sharing user override	Override the DM/Sharing connection requirement
Create Attachments	Create attachments on content
Insert images	Insert images into content
Customize Site	Customize site appearance (theming)
Manage Slideshow Carousel	Manage the slide show displayed in a carousel widget used on the community's Home page and Overview pages
Save JavaScript	Create static HTML content that references or embeds JavaScript

Setting Home page and Other Content permissions for user groups

Here you can find how to set up Home page and other global content permissions for user groups.

Fastpath: Advanced Admin Console > **Permissions** > **Other Content Permissions**

To set up permissions for user groups to Home page and other content types:

1. In the Advanced Admin Console, go to **Permissions** > **Other Content Permissions** .
2. On the permissions page, under **Groups with access**, review permissions to user groups.
3. To assign permissions to a user group not yet added:
   a. Click **Add group**.
   b. Enter the name of the user group to add.
   c. Click **Select Permissions**.
   d. In the dialog box, select the permissions you want to apply for the user group.
4. To edit permissions for a user group already added:
   a. Locate the group in the list.
   b. Next to its name, click **edit permissions**.
   c. In the dialog box, select the permissions you want to apply for the user group.
5. Click **Set Permissions**.

Creating user overrides to Home page and Other Content

Here you can find how to configure overrides to the Home page and other content types for individual users.

Fastpath:

- **Admin Console** > **Permissions** > **Content**

To grant a particular set of permissions to an individual, you create a user override. An override can be used if:

To set up overrides for the Home page and other content types to individual users:

1. Go to the configuration page:
   - **Admin Console** > **Permissions** > **Content**
2. Under **User Overrides**, click **Create a user override**.
3. 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.
4. Click **Set override** to view the permissions you can assign.
5. In the permissions dialog box, select and clear check boxes to assign the user only the required permissions.

   Note that you clear a check box to remove a permission — there's no need to revoke the permission explicitly.
6. Click **Set Permissions** to save the override you've created.

The user has the permissions you configured.

Customization permissions for Overview pages

The Overview pages of places are customizable. Here you can find who can change what on place Overview pages.

Page	Description	Who can customize
Space Overview	Is displayed on the Overview tab of space	A space administrator
Project Overview	Is displayed on the Overview tab of a project	The project's creator. Space and group owners can edit projects that belong in the space or group

Page	Description	Who can customize
GroupOverview	Is displayed on the Overview tab of a group	All group owners
Community Overview (Home)	Is displayed the landing page of your community (if configured)	Community manager

Managing places and pages

Spaces, social groups, and the blogs and projects associated with them give your site structure. You can use space hierarchies and specially designed place pages in your community to highlight the focus and function of different areas.

Note that you can create spaces and manage certain aspects of them in the Admin Console, but social groups are created and managed from the user interface.

To make a place easier to search, you can use the search term in the title, description, and tag fields as many times as possible, with as few other words as possible.

Jive places: spaces, groups, and projects

A place in Jive is essentially a container that houses all the collaborative content for a certain subject or team. There are three types of places: **Spaces**, **Groups**, and **Projects**. The differences between them can sometimes be confusing, so here're the basics of each one.

Spaces

Spaces are built in a hierarchy, with the ability to have a network of multi-level sub-spaces underneath them. They also use permissions, set by community administrators, to define who can see and do different things in the space. Permissions get inherited by any sub-spaces unless they are customized for that space, so if a user can do something in one space, this user can do it in the sub-spaces as well (unless the permissions have been customized). Any type of content can be created in a space, unless it has been turned off for a particular space by community administrators. Due to their hierarchical nature, spaces are typically used to represent organizations and departments within a company, and other concepts that require a network of places linked together.

For more information about creating spaces, see Designing space hierarchies on page 145 and Creating new spaces from the Admin Console on page 150.

Social groups

Groups, or *social groups*, are isolated containers within a community; they have no ties to other places and cannot have sub-groups. Permissions are managed on a per-group basis by the original group creator or the admins selected for the group, or both. Groups can also house any type of content unless one or more is turned off by community administrators. Because they are a freely created containers, groups get used most often for topic-specific collaboration, rather than something general to a team. They also get used for collaboration between specific teams or different departments that often work together closely and rely on each other.

For more information, see Using content and Types of groups in the User Guide.

Projects

Projects can only reside within a space or a group; they cannot stand alone. However, they can still house any type of content unless one or more is turned off by community administrators. Permissions get inherited from the place in which the project was created. Projects also get created with a Start Date and an End Date and come with additional titles on their pages that display the progress being made in the project (if the project administrator keeps them up to date). Projects are generally used for short-term projects, which users need to collaborate on and house the content for in a single area.

For more information, see Using projects and tasks in the User Guide.

What to use

Use a space if you:

- Need to share information about your department, program or initiatives with the rest of the organization/larger audience
- Need to add permissions controlling who can create which kinds of content in your place
- Need to create a hierarchical set of places
- Need permissions for your place to be managed centrally

Create a group if you:

- Want to collaborate privately with your team or project team
- Want to invite individuals to collaborate, and don't need centrally managed permissions
- Want to invite people from outside the organization to access your place

Comparison of place properties

	Spaces	Groups	Projects
Hierarchical?	Yes	No	No
Can be private?	Yes, via permissions	Yes, via group settings.	Depends on parent place

	Spaces	Groups	Projects
Access permissions	Defined in the Admin Console. Inherited by sub-spaces	Defined in group settings. No inheritance	Inherited from containing place. Not customizable
Create permissions	Defined in the Admin Console. Inherited by sub-spaces	Any user	Inherited from containing place. Not customizable
Content allowed	Any; may be customized or restricted, or both by community administrators	Any; may be customized or restricted, or both, by community administrators	Any; may be customized or restricted, or both, by community administrators
Best uses	Large-scale collaborative needs with sub-space ability, such as those of an entire department or office, or an expansive topic	Smaller-scale collaborative needs either by a specific audience or a more specialized topic	Short term area to collaborate on a finite topic

Creating community structure

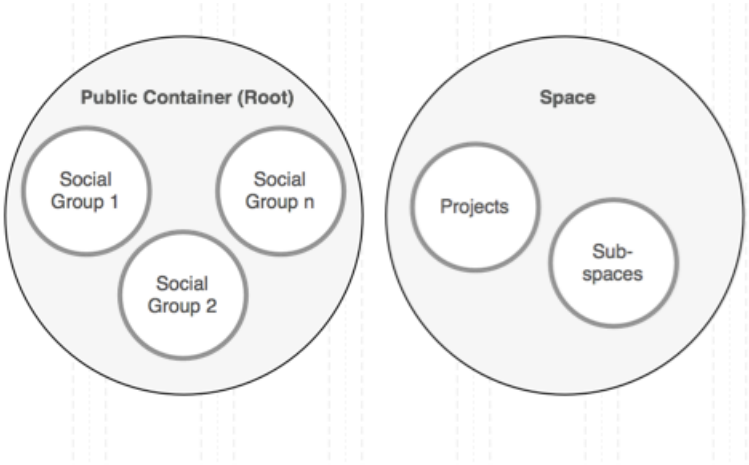
Creating a structure for content is one of the most important things you do to get your community started. Because people post content in various places, the places you create should help your users intuitively understand where to post (and find) content.

For example, you might organize the spaces to reflect the organization of the company itself including spaces like HR, Accounting, and Research.

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 do not have a hierarchical structure. Consequently, 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:



It is especially important when you are 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. The settings inherited at the time of creation are used as a starting point but can be modified later.

For more information about creating spaces, see Designing space hierarchies on page 145 and Creating new spaces from the Admin Console on page 150.

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. For more information about different types of places, see Jive places: spaces, groups, and projects.

Designing space hierarchies

One of the first things you do when setting up your community is to 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 should have special permissions — such as blog authors, moderators, and so on. As you create spaces and sub-spaces by using the Admin Console, you'll be prompted for this information.
- Each space and sub-space can have different sets of permissions so that you can control access and capabilities within a space.
- When defining spaces and sub-spaces, make 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 and sub-space hierarchy and get user feedback on it.
- Create a general, high-level hierarchy to get started. After people are involved, they refine the categorization by using tags. Generally, a significant numbers of spaces and sub-spaces tend to create a lot of unused content and reduce the impact of tagging.
- Define spaces with the role of tags in mind. Spaces organize content, but over time tags grow to constitute virtual groups used to organize content. 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." 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 significant 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.

Arranging space hierarchy

You can view the list of spaces and organize the space hierarchy in the Admin Console.

Fastpath:

- **Admin Console** > **Permissions** > **Spaces**

You can view the list of all spaces and subspaces of your community in the Admin Console. You can add new spaces, change the order of spaces under one parent space, move spaces to other parent spaces, edit general space settings, and delete spaces.

Note: You can't move or delete the root space.

To arrange spaces in the hierarchy:

1. Go to the configuration page:
   - **Admin Console** > **Permissions** > **Spaces**
2. To create a new space, select the parent space for the new space and then:
   - Click  > **Add a Subspace** .

   For more information, see Creating new spaces from the Admin Console on page 150.
3. To edit space properties, select the space and then:
   - Click  > **Edit general information** .

   For more information, see Setting up general space settings on page 152 and Re-naming the root space.
4. To change the order of subspaces of a space, drag-and-drop the subspaces.
5. To move a space to another parent space, select the space and then:
   - Click  > **Move Space** .

   After that, select a new parent space in the dialog box, and click **Move Space**.
6. To delete a space and all content inside it, select the space and then:
   - Click  > **Delete Space** .

   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. If you delete a space that includes subspaces, all subspaces are deleted as well. Also note that deleting a space make take some time.

Renaming the root space

You can change the name and description of the root space from the Admin Console. By default, the root space is named `community`.

Fastpath:

- **Admin Console** > **Permissions** > **Spaces**

To change the name of the root space in the Admin Console

1. Go to **Admin Console** > **Permissions** > **Spaces** .
2. Click > **Edit general information** next to the name of the root space.
   The root space is the top one in the list; it's called `community` by default.
3. In **Name**, enter the community name.
4. Optionally, in **Description**, enter the community description.
5. Optionally, in **Locale**, specify the default community locale.
   The default locale is `Inherit [English]`.
6. Click **Save Changes**.

The root space becomes available under new name throughout the application, for example, when you need to select a place.

Space creation options

You have several options when setting up a space.

Space landing page

By default, the Activity page is used as the main space page. It uses tiles to present information. In some cases, you can also enable the Overview page that uses widgets instead of tiles.

Advanced space creation options

In the following table, the asterisks (*) note when this advanced option for place navigation might be unavailable.

Important: We do not recommend that you use widgets and widgetized Overview pages (including the Home page) in your community.

I want to. . .	You should. . .	Can I change this later?
Design a landing page that's optimized for a specific work purpose.	Create a group, then for the Activity page choose and configure a Place Template customized for the kind of work you want to do. For moreinformation,seeDesigning activity and custom pages for places. Place Templates only apply to Activity pages.	Yes.
Design a landing page with widgets*	Select the **Overview page** check box under the **Advanced Options** during setup, and fill out a widget layout under **gear icon** > **Overview Page** from the group page. For more information, see Designing Overview pages for places.	Yes.
Make more custom pages in the place for displaying information, not just a landing page.	Create the group, and then add the pages to your place afterward. See Adding custom pages to places.	Yes.
Integrate external streams from Facebook, Chatter, or any other apps your community admin has enabled.*	Create the group, then click **Add a stream integration** when configuring the Activity page. For more information, see Adding tiles with external stream integrations to Activity page.	Yes, but keep in mind that some external stream typescannotbedisconnected 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 Activity page.	Yes.
Store the place binary documents outside Jive, for example, in Box or SharePoint.	During place setup, after you preview the topic, edit the Activity page. External file storage is available if at least one storage provider has been set up by community administrators. For more information, see Using external file 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 place categories to your place in the place settings.	Yes. Just remove or replace the tags or place categories.

Creating new spaces from the Admin Console

Creating several spaces quickly is easy from the Admin Console, although you can create spaces from the user interface as well. After the space is created, you can apply place templates from the user interface.

Fastpath:

- **Admin Console** > **Permissions** > **Spaces**

Note that if you creating a new space in the Admin Console, the content type settings are copied from the parent space. You can you can redefine them later.

You can apply place templates to the Activity page for each space later, or create Overview pages for them if you choose.

To create a space from the Admin Console

1. Go to **Admin Console** > **Permissions** > **Spaces** .
2. To create a new space, next to the name of the space that will contain it click  > **Add a subspace** .

   This opens the **Space Creation: <parent space>** page where you can specify the space details. The parent space is listed for reference.
3. In **Space Name**, enter the space name to appear in the user interface.
4. In **Description of space**, enter a description to appear in the user interface, such as a brief description of what the space is for.
5. In **Space Display Name**, specify the text to be used in space URLs if you want to change the default one.
6. If you want the to have the same access scheme as the parent space, then select **Inherited** under **Permissions** and then click **Create**.

   This creates a new space with the permissions inherited from the parent space.
7. If you want to customize the access scheme, than select **Custom** under **Permissions**.
8. Choose one of the following options as the staring point for further permissions configuration:
   - **Use inherited permissions as a starting point**: The new space will have the same permissions as the parent space.
   - **Use default space permissions as a starting point**: The new space will have the same permissions as the default (root) space. Note that the space is only assigned the same permissions as the root space but won't inherit them.
   - **No permissions, start with a blank slate**: The permissions won't be set for any user group or account.

The permissions are not selected for the default user groups **Everyone** and **All registered users** as well.

9. Click **Create - Then Define Permissions**.

   The space is created with the specified settings and the space page where you can define the space permissions is opened for editing. For more information about setting up space permissions, see Managing space permissions on page 120. For details on settings up for user groups and individuate user accounts, see Setting up user group permissions for spaces on page 124 and Creating user overrides for spaces on page 126.

Creating new space from user interface

Creating spaces from user interface let you fully set up the space, apply place templates, and configure the space Activity page.

When you create a space from the user interface, the Activity page is used as the landing page by default. You can apply a space template to the page or configure it yourself. If you choose, you can also add an Overview page to the space.

Important: We do not recommend that you use widgets and widgetized Overview pages (including the Home page) in your community.

Note: Creating several spaces quickly is easier from the Admin Console, as described Creating new spaces from the Admin Console on page 150.

To create a space:

1. In the user interface, click  > **Space** , and then select the place where you want to create the space.
   - If you want to space, select the root space. By default, the root space is called *community*.
   - If you want to create a sub-space, select the parent space.
2. In the **Create Space** dialog box, in **Name**, enter the space name to appear in the user interface.
3. In **Description**, 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. In **Tags**, enter tags to be used when searching for the space.
5. In **Categories**, select the space categories to be used when searching for the space.

   Note: This is available if place categories have been configured in the community.
6. If available, click **Advanced Options** to expose more options.

Your place uses an Activity page as its main page by default, 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.

7. When you're finished, click **Create Space** .

With the space created, you can customize it to your requirements. Note that the Team Collaboration template is used to populate the space banner and the tiles and streams on the Activity page. You can change the template to update the theme of your space.

Configuring spaces

Some of the space parameters you can configure only by using the Admin Console.

Setting up general space settings

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

Fastpath:

- **Admin Console** > **Permissions** > **Spaces** , then > **Edit general information**

The *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 URL is a quick way to get to the space. Note that you can't change the display name for the root space.

You can change the space's locale setting to set user UI characteristics, such as language and date format. Note that this locale setting applies to one of several locale behaviors. For more information on how the locale is chosen for displaying to the user, see Setting up locale and time zone on page 50.

You can also specify the content types the space and its sub-spaces supports.

Managing Content Permissions

You can manage global permissions for content features, such as polls and announcements, for the whole community and, if required, set up separate content permissions for individual spaces.

The community's landing page includes global permissions for actions like managing announcements, which is typically seen by everyone at one time or another. The landing page in your community, can be a great place to put things that should be visible to everyone. In other words, when setting global permissions, 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.

Configuring community content types

You can define which content types users are able to create, such as blog posts, discussions, and documents. Here you can determine the settings for the whole community.

Fastpath: > **Content** > **Content Types**

You choose some or all of the available types for your community.

Note: If you would want to change the settings later, deselecting a content type does not remove existing content from your community, it only prevents people from creating new content of that type.

Managing external groups

Jive provides external access for *private* and *private unlisted* groups. With externally accessible groups, you can add external contributors by using group invitations or LDAP and you can restrict who can create external groups.

Note: While external contributors can use groups much the same way standard community users can with certain restrictions, they can never become group owners. For more information, see What can external contributors see? in the Cloud User Help.

For more information about working with a community as external contributor, see Contributing to community as external user in the Cloud User Help.

Enabling external groups

Group owners can make private and secret (also known as private unlisted) groups accessible to outside contributors if this feature is enabled in your community.

Fastpath:

- **Admin Console** > **Permissions** > **Social Groups**

In an externally accessible group, group members (both external contributors and standard community users) can invite external contributors to these groups.

When disabled after being enabled for a period, all content created by external contributors continues to exist, and external contributors continue to be visible in the community, but they are no longer able to log in.

By default, externally accessible groups are enabled.

Note: For more information about using SSO with external groups enabled, see Mixed-mode authentication on page 98.

To give users permission to create an externally accessible group:

1. Go to the configuration page:
   - **Admin Console** > **Permissions** > **Social Groups**
2. Assign specific users or user groups the permission to **Create externally accessible groups**. For more information, see Permissions for external groups on page 154.

The users with the permissions assigned can see the option to Enable external access under the Advanced options when creating or editing a group in the user interface. For step-by-step instructions on creating a group with external access, see Creating externally accessible groups in the Cloud User Help.

Permissions for external groups

Jive provides the *Create externally accessible group* permission that allows users to create social groups with external access. The *Manage social group* permission also gives users this ability, but it also includes being able to manage any social group.

Fastpath:

- **Admin Console** > **Permissions** > **Social Groups**

You can assign the *Create externally accessible group* permission to either individual users (user override) or groups of users (user groups). The user group must exist before you can assign it permissions.

For more information about managing permissions, see Managing social group permissions on page 134. For more information about managing user groups, see Managing user groups on page 65.

Setting user group permission for externally accessible social groups

Generally, to set up a user group permission for creating and managing external social groups:

1. Go to the user group configuration page and create a new user group for the users who must be able to create externally accessible social groups:
   - **Admin Console** > **Permissions** > **User Groups** , then click **Create New User Group**

   For more information, see Creating user groups.
2. Go to the social group permission configuration page and assign the **Create externally accessible group** permissions to the user group created in Step 1 on page 155:
   - **Admin Console** > **Permissions** > **Social Groups**

   For more information, see Setting up social group permissions for user groups on page 136.

With the user group in place, you can manage users with the permission by adding them to the user group or removing them from the group. For more information, see Adding and removing users to user groups on page 67.

Creating user overrides for social groups

Although creating user groups is preferable, you can assign the *Create externally accessible group* permissions to individual users.

To set up for creating and managing external social groups for particular users:

1. Go to the social group permission configuration page:
   - **Admin Console** > **Permissions** > **Social Groups**
2. Assign the **Create externally accessible group** user override to the users.

   For more information, see Configuring user overrides to social groups on page 137.

Adding external contributors

Jive enables you to add external contributors either by inviting them to a group in your community or by adding them directly into the LDAP directory.

External contributors can either be invited by group members or you can use the Admin Console to add them into the LDAP directory. For more information on inviting users, see Inviting external contributors in the User Guide. For more information on adding users to the LDAP directory, see Mapping users from a directory server on page 87.

Configuring content-related settings

The settings you can find in this section are related to how the application handles content, such as setting size limits and threading for discussions, enabling search, and spell checking.

Configuring community content types

You can define which content types users are able to create, such as blog posts, discussions, and documents. Here you can determine the settings for the whole community.

Fastpath: > **Content** > **Content Types**

You choose some or all of the available types for your community.

Note: If you would want to change the settings later, deselecting a content type does not remove existing content from your community, it only prevents people from creating new content of that type.

Configuring spell check

Jive checks spelling when users create and edit content. As a community manager, you can customize the spell check feature by using the Admin Console.

Fastpath:

- **Admin Console** > **Content** > **Spell Check**

The spell checker uses the main dictionary you specify for all content in the community. Consider using a technical dictionary if your community creates content with terms from a specific industry.

Additionally, you can add words to your custom dictionary, so that words commonly used in your community (such as jargon or product names) won't be marked as misspelled.

To configure spell check:

1. Go to the configuration page:
   - **Admin Console** > **Content** > **Spell Check**
2. In **Main Dictionary**, specify the main dictionary for your community.

3. Under **Include Technical Dictionary?**, decide if you want to add a technical dictionary.
4. If required, under **Custom Dictionary**, specify a comma-delimited list of words which you want to add to dictionary, and then click **Add**.

   Custom words are listed under **Current Custom Dictionary**. You can remove the any word if, for example, it has been mistakenly added.

Managing images and collections

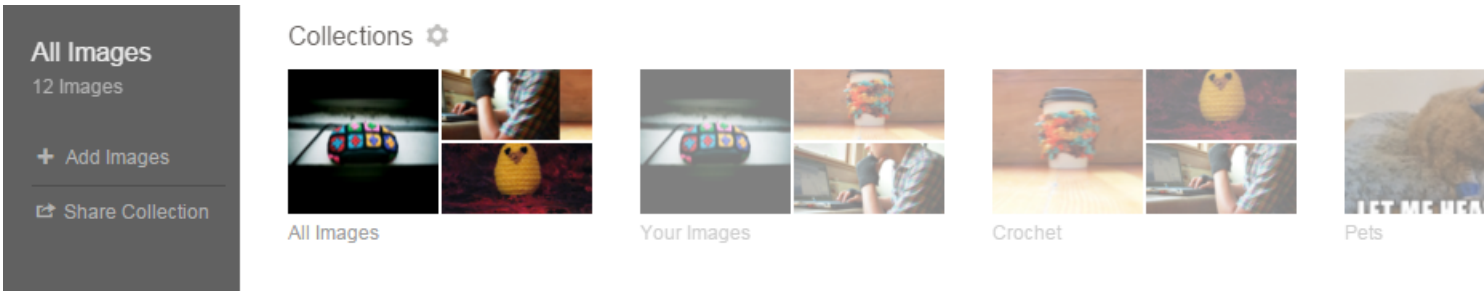
Jive users can include images in content of different types, or import images to places as separate pieces of content and gather them into collections. You can configure the options for importing and using images in places.

Enabling collections

Depending on place permissions, community members can view images, organize them into collections to share, and save and display collections to view and share later.

Fastpath:

- **Admin Console** > **Overview** > **New Features Available**



To enable collections in your community:

1. Go to the configuration page:
   - **Admin Console** > **Overview** > **New Features Available**
2. Under **Image Browse and Collections**, select **Enabled**.
3. Click **Save**.

With the feature enabled, Jive places include an **Images** page where users can view images and organize them into collections to share with other community members. Place owners are also able to save and display collections for place members to view and share later. For more information about collections, see Images and Collections in Jive Places in the Cloud User Help.

Note: The maximum size of an image that can be added to a collection is the same as the **Maximum image size** setting for your entire Jive community. If you want to change this setting for your Jive community (and for collections), you can go to **Advanced Admin Console** > **System** > **Settings** > **Images** .

Removing content items from Top and Trending

If you do not want your blog post (or other content items) feature in the trending lists of your community, you can remove this post from the global lists.

Jive uses the Recommender service analyzes content and people over a period of time and uses that data to display the top and trending lists. 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.

The Recommender works globally for the whole community but some point you may want to remove your content items from the trending lists. If you use this option, your content items will not be displayed in:

- In the **Top & Trending** list in the News streams.
- On the **Recommended** tabs when you browse content (`/content?filterID=recommended`).
- In the **Trending Content** tiles.
- In the **Trending Now** section of newsletter emails.

You can hide items of the following content types:

- Status updates
- Discussions
- Questions
- Blog posts
- Documents
- Uploaded files
- Polls
- Events
- Ideas

Content authors and users with the Manage Users, Manage Community, Manage System, or Full Access permissions can remove a content item from Top and Trending lists.

To remove a content item from Top and Trending lists

1. Go to the content item.
2. Click **Actions** > **Remove from Top & Trending** .

To add a content item to Top and Trending lists

1. Go to the content item.
2. Click **Actions** > **Allow in Top & Trending** .

Managing search

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

Cloud Search service

The Jive Cloud Search service enhances Jive search with infinite scale, continuous improvements, and an advanced social context. Here you can find how Jive Cloud search works.

About Cloud Search service

Jive Cloud Search service is available when you are using the Jive Cloud. It is enabled by default.

The Cloud Search service follows best practices for data separation. All data is written, stored, and accessed with a tenant-ID unique to the owner of the data, and no access to data for a given tenant-ID is permitted unless a client also presents a secret key for verification in accordance with OAuth. All communication is over HTTPS.

Attention: The Cloud Search service is based on the Amazon Elasticsearch service. If your organization requires you to whitelist IP addresses, see Required Jive domains and firewall rules for the addresses you need to whitelist.

Cloud Search benefits

Cloud Search provides the following benefits:

Infinite scale	By leveraging a cloud-based Big Data infrastructure, the search service can scale to any level while providing full redundancy.
Continuous improvement	Because search is deployed as a separate service, it can be improved at any time without disrupting other Jive functionality. Just as with familiar web search tools, the relevance of Jive search results gets better over time.
Redesigned architecture	The Cloud Search Service is based on Amazon Elasticsearch Service. The main benefits are improved stability and performance, greater relevance due to enriching Jive objects with metadata, and reduce the downtime for reindexing of content, people and places. For more information about the employed services, see Amazon Elasticsearch Service on the AWS portal.

Attention: The Cloud Search Service reindexes only the first 40,000 characters of each content item.

Better experience for users	Enhanced filtering options, user's search history, suggestions that are based on the context of your community, and other search aspects make using search more intuitive and comfortable for users. For example, spelling corrections when you search for people are provided from the community users corpus. And suggestions for content search are provided from the text corpus of your community, including the object metadata.

Basic search algorithm

Searching is done on the available fields, where a *field* is a single piece of information within the content, place, or user profile you're searching. For example, in a document, you have the title/subject, the content, and the tags. For a user, you have first name, last name, expertise, tags, and many more.

By default, Cloud Search uses `OR` search on content and places (that means that at least one term must be present) and `AND` search on users (that means that all terms must be present). Users may specify search operators directly if necessary; for more information, see Search rules in the Cloud User Help. The algorithm searches all included text, including attachments and comments – not just the initial blog post, document, or discussion.

Users can apply special modifiers, such as quotes or keywords, to make search phrases more specific. For more information, see Search overview in the Cloud User Help.

The results depend on what users are searching for: content, people, or places. For more information on how different search types work, see Content search on page 162 and People and place search on page 168.

Spotlight search and Advanced search

The Spotlight search appears at the top of each page. It's intended as the "quick access" search feature, with suggestions, frequently used items, and search history. So, when typing the first few letters in the search box you can see suggestions based on the quick search performed in the background – including content completion and spelling correction options. In order to initiate the search, you will need to click on one of the suggestions or press `Enter`.

In order to initiate the search, you will need to click on one of the suggestions or press `Enter`. At this point, the Spotlight search adds a wildcard (`*`) to the end of your search term. This means that if you're searching for `Library of Congress` and press `Enter` after typing `Librar`, it searches for `library`, `libraries`, and other words with the same stem, not just `librar`. Note that the Spotlight search searches for tags as well as content, people, and places.

If that is not enough, you can switch to the Advanced search. It offers more options to refine your search and does not apply the wildcard, as it expects you to provide all of your detailed criteria for the most specific results. For example, here you can limit a document search by author.

For more information, see Search and browse features and Using Spotlight search in the Cloud User Help.

@Mentions

When you start to @mention someone or something, Jive searched similarly to the Spotlight search. The search algorithm takes what you've typed in so far and adds a wildcard (*) to it. This means that no stemming is done with this search.

The main difference from the Spotlight search is that @mentioning only searches the title of content or place and username, name, and email of a user.

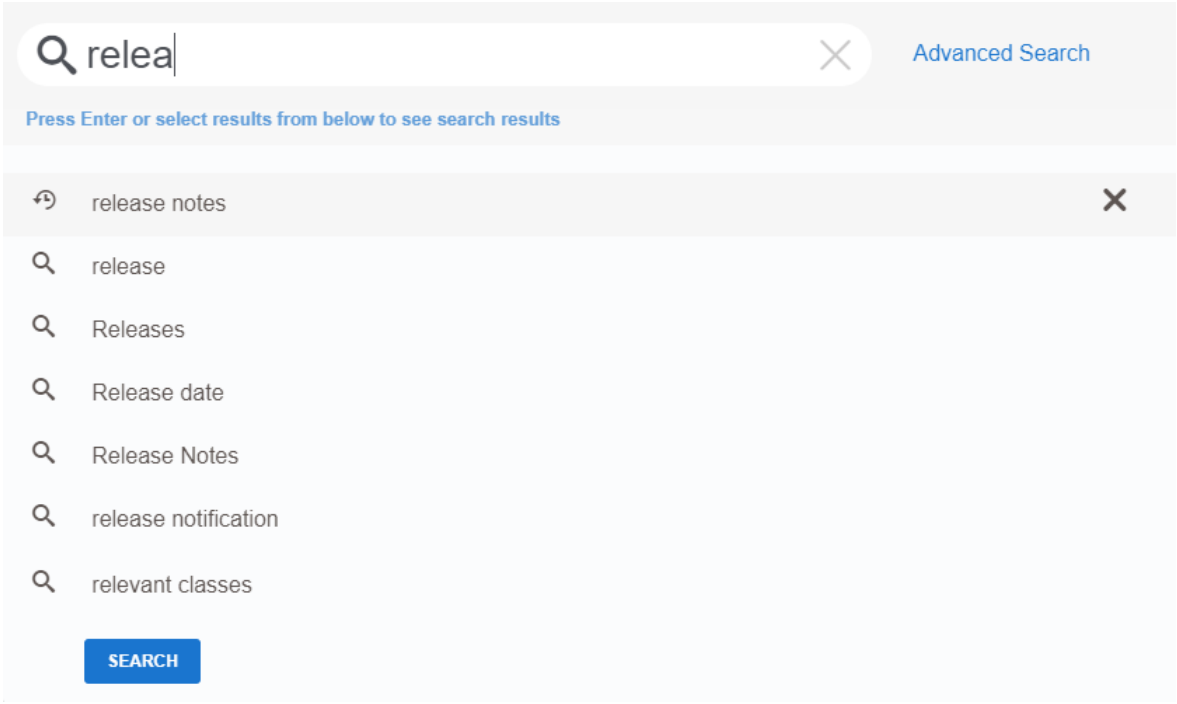
For @mentions, search synonyms work only on exact words (not suffixed with a wildcard `*`). For example, let's see how it works for a mention query that looks like this: `Alice_Ford OR (Alice AND Ford*)`. In this case, synonyms will be used for `Alice` only unless `Ford*` has been added to the synonyms list.

For more information about using @ mentions, see Search overview in the Cloud User Help.

Suggestions

The Cloud Search Service provides suggestions based on the index content. So, when you type first few letters in the search box you can see suggestions based on the quick search result done in the background for you.

Figure 6: Possible search suggestions when you type `relea`



These suggestions are based on a special multi-valued field data that is provided during document indexing; is field is not used in the regular search. For people search, it contains person first name and full name, for other content it contains the title (subject).

The search service checks for prefix matches that user types in the search box at the same time allowing fuzzy matching to be able to provide suggestions to correct some spelling mistakes. In practice, the first letter must always match. And the longer search phrase is the less exact matches are allowed.

Suggestions respect user access rights, as well as access to content and filtering by type. So if a user wants to search just for some blog post and they selected the **Blog posts** type filter, in suggestions, they will see only blog posts which they can access.

Note that suggestions are not affected by synonyms, both for content and people search.

Search configuration

For more information about configuring search, see Configuring content search on page 169, Configuring user search on page 172, and Configuring OpenSearch.

Content search

Here you can find how the Jive Cloud Search service searches for content.

When searching for content, Jive searches in content items available for users as follows:

- `subject`: Title field of Jive objects, such as place or doc title.
- `body`: Content of objects, such as blog post text.
- `tag`: Tags added to objects.

By default, Cloud Search uses `OR` search on content, meaning that items with at least one search term will be present in the results. Users may specify search operators directly if necessary; for more information, see Search rules in the Cloud User Help.

The results are then ordered by the relevancy score the items gain when users search for a specific search phrase. Stop words are excluded before search queries are processed.

Search relevancy

The relevancy rank is calculated as follows:

```
Rank = (SimilarityScore + ProximityScore) * OutcomeType * ObjectType * Recency
```

These parameters are explained in detail in Search relevancy in content and place search on page 163.

Searchable content types

The system searches for the search phrase in all of these content types:

- Direct message
- Poll
- Blog post
- Idea
- Announcement
- Document
- Question
- Discussion
- File
- Photo
- Status update
- Task
- Event
- Video
- External activity
- Comments on content

Users can limit the results to a specific content type by using filters.

Synonyms

You can define common synonyms for terms that are relevant for your particular system. For example, `docs` and `documentation` may be equal when searching. The searched word must match exactly the one from the synonyms list. So, if a user will add a wildcard (`*`) at the end of the word, the search will not include synonyms for this word (unless you add word ending with a wildcard to the synonyms list).

Note that the synonyms do not affect the suggestions but only search results.

For more information, see Configuring search synonyms for content items on page 169.

Search relevancy in content and place search

> *Getting the relevant results is critical for the success of the community. Here you can what parameters impact the relevancy score for content items and places and the rank a result will get when you search for a specific search phrase.*

Jive searches object fields. Stop words are excluded. The parameters, described in this article, impact the rank of a content item and can provide a boost to get it to the top of the search results.

The relevancy rank is calculated as follows:

```
Rank = (SimilarityScore + ProximityScore) * OutcomeType * ObjectType * Recency
```

The resulting rank determines what will be displayed in the user's search results and in what order, with the objective to surface the most relevant content first.

Fields that are searched

Cloud Search uses information from the following fields:

- `subject`: Title field of Jive objects, such as place or doc title.
- `body`: Content of objects, such as blog post text.
- `tag`: Tags added to objects.

Attention: Stop words are removed before searching content from the object fields, as well as from the `Analyzed` and `Edgengram` fields.

Stop words

The Cloud Search service uses a predefined set of stop words for the specified languages. *Stop words* are common words often occurring in any text. For example, the stop words for the English language include `of`, `the`, `this`, `a`, and `and`.

When a search request is processed, these words are skipped from the searched object fields and the Analyzed and Edgengram sub-fields.

Similarity score

When searching for a phrase the system looks at each word in the phrase and checks the match type and place of match for this work. Each match type and place has its own boost score. The boost score is normalized with the number of times the searched term appears in the given content (the more it appears the better), as well as with the number of times this term appears in the search index (the more common the term is, the less impact it has on the rank). The default settings are listed in Table 23 on page 164.

Match types reflect how well your search query matches the results:

- **Raw**: Exact matches of the search term.
- **Analyzed**: Matches that are created by language analyzer. In this case, *stemming* is used, that is, looking for the root of the word. Stop words are ignored. For example, `focusing` will also find `focus`, `focused`, and other related words with the same stem.
- **Edgengram**: Partial match, used for wildcard search matches and matches in search-as-you-type queries. Stop words are ignored.

Table 23: Similarity boosts

Match place	Match type		
	Raw	Analyzed	Edgengram
`subject`	1.0	1.0	1.0
`body`	0.1	0.1	0.1
`tag`	0.5		0.5

Attention: Stop words are removed before searching content from the object fields, as well as from the `Analyzed` and `Edgengram` fields.

Proximity score

The proximity score checks how close is the term the user searches for to what appears in the content – to boost more relevant results. When a user searches for a phrase built from several words, this phrase may appear exactly the same way in the content or it may appear in the content in a slightly different way. For example, content with the term `product one-pager brochure` is an approximate match when searching for `product brochure`.

Types of proximity boosts:

- **Exact match**: When all the search terms appear in the content next to each other
- **Proximity match**: When all the search terms appear less than three words apart from each other

The default settings are listed in Table 24 on page 165.

Table 24: Proximity and exact match boosts

Place	Proximity boost	Exact match boost
Subject	0.5	1.6
Body	0.5	1.0
Tags**	0.1	1.0

** Having proximity score on tags is unlikely to happen.

Note: Exact and proximity matches are boosted using only `raw` sub-field for tags and only `analyzed` sub-field for other search fields.

A higher the boost value, more matches in the given field, and the match method get ranked higher. Stop words are ignored.

Besides the matches, we also look for frequency. The score has a lot to do with how many occurrences of the word user is searching for exists in the field. For example, if a 20,000-word essay makes a single reference to the movie `Finding Nemo` somewhere in the document and another document in the system has only 50 words and includes `Finding Nemo`, the latter is counted more relevant to a query for `nemo`.

Outcome type

Content in Jive can be marked with structured outcomes. These outcomes impact the score of that content in the search results, results are boosted based on outcome type.

The boosts given to content according to outcome type are listed in Table 25 on page 166.

Table 25: Outcome boosts

Outcome	Boost	Outcome	Boost
Finalized	1.4	Official	2.0
Outdated	0.1	Default	1.0

This score is being multiplied by the boosts above. A higher boost results in that content being ranked higher in the search results, so the 0.1 score for outdated documents significantly reduces their rank.

Object type

Similarly to outcome boost, there is a boost for ranks based on the type of content used. Documents and blogs are ranked higher in the search results as these are usually used for more comprehensive content that may be more relevant for the searching user. The settings are listed in Table 26 on page 166.

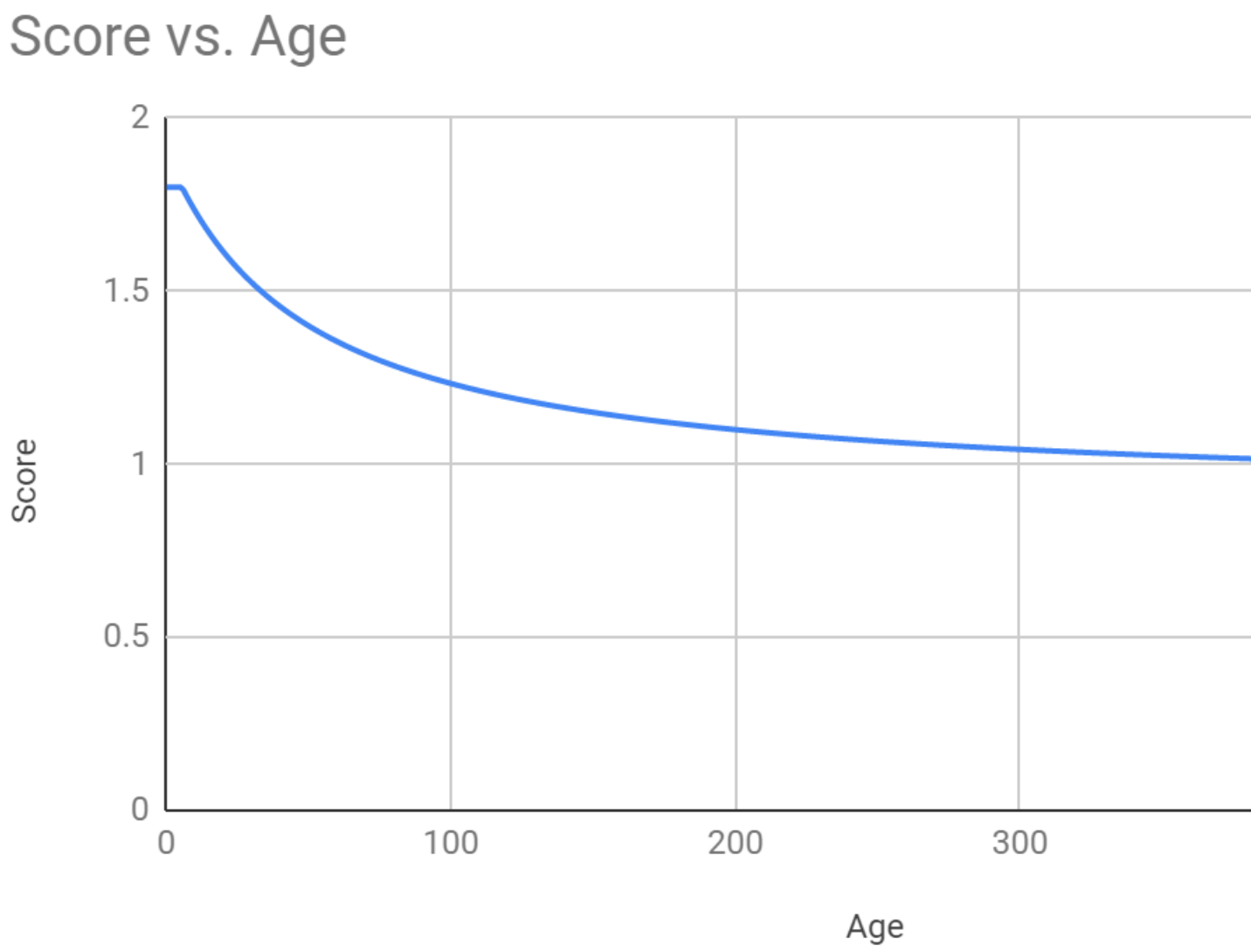
Table 26: Object boosts

Object	Boost	Object	Boost
Document	1.4	Poll	1.0
Blog	1.4	Idea	1.0
Blog post	1.4	Video	1.0
Discussion	1.0	Status Update	1.0
Question	1.0		

Recency

Recency (or *time decay*) lowers the score for older content. The impact of content can be seen this way:

Figure 7: Default recency boost



The recency score calculation is based on the following parameters:

Drop speed

Determines how fast the algorithm reduces the content score by age. The default setting in 50.

Max value

Determines the latest period the content from which has the same score without decay. The default setting is 4 weeks.

Minimum score

Determines the score difference of a very old document and a just created one as 2 times as maximum. It is set so that even the oldest relevant content can be found but allows preference for fresh content. The default setting is 0.9.

People and place search

In addition to searching for content, you can also search for users and places (such as spaces and groups). There are some important differences in these types of search.

@Mentions

When you start to @mention someone or something, Jive searched similarly to the Spotlight search. The search algorithm takes what you've typed in so far and adds a wildcard (*) to it. This means that no stemming is done with this search.

The main difference from the Spotlight search is that @mentioning only searches the title of content or place and username, name, and email of a user.

For @mentions, search synonyms work only on exact words (not suffixed with a wildcard `*`). For example, let's see how it works for a mention query that looks like this: `Alice_Ford OR (Alice AND Ford*)`. In this case, synonyms will be used for `Alice` only unless `Ford*` has been added to the synonyms list.

For more information about using @ mentions, see Search overview in the Cloud User Help.

User search

You can search for users both from the user interface and from the Admin Console.

When searching for users, the system uses the phrases and searches for them in each of the profile fields that user performing the search has access to (according to the user settings). However, you can't search for a user according to a specific profile field.

The user search uses the `AND` operator by default – that means that the results with all searched terms present will be listed first. Additionally, the boolean operators that users can specify directly work differently on some fields; for more information, see Search rules in the Cloud User Help.

You can define common synonyms for user names that are relevant to your particular system. For example, `Robert` may be equal to `Rob` and `Bob`. For more information, see Configuring search synonyms for user names on page 172.

Places search

When searching for places, the system searches the title, the description, and the tags.

By default, Cloud Search uses `OR` search on places, meaning that items with at least one search term will be present in the results. Users may specify search operators directly if necessary; for more information, see Search rules in the Cloud User Help.

The search algorithm is similar to content search: a field that contains 5 words, one of which is a match, receives a higher score than a field that contains 25 words, one of which is a match. To make a place easier to search, you can use the search term in the title, description, and tag fields as many times as possible, with as few other words as possible.

The following types of places can be searched for:

- Space
- Group
- Project
- Personal blog

Configuring content search

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

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

Configuring search synonyms for content items

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

Fastpath:

- **Admin Console** > **Content** > **Content Synonyms**

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`.

Note that by default, new synonyms work only on new content. Thus, the changes become available in ~30 seconds, after the search index is updated.

To set up search synonyms:

1. Go to the configuration page:
   - **Admin Console** > **Content** > **Content Synonyms**
2. Under **Synonyms**, type in a comma-separated list of synonyms for terms.
3. Click **Add Synonyms**.

   The added list appear as a line under **Current synonyms**.
4. Rebuild the content search index.

After synonyms are added, the indexing is updated automatically and in ~30 seconds the newly added synonyms will be available in search.

Promoting content search results

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

Fastpath:

- **Admin Console** > **Content** > **Promoted Results**

Promoting a result ensures that when you type certain keywords, a content item you select always appears 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 determine 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 and 2 in the results by assigning the rules priorities 0 and 1.

Note the following when promoting results:

- Promoted search only works on documents that are visible to the entire community. You should avoid promoting any document or content access to which is restricted.
- You can promote a maximum of two links per keyword in one language by default. If you want to shange the limit, you can contact Support.
- 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 is returned for spotlight search queries on "quart" as well as "quarter." But if you specify "quarterly sales," your selected content is not 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.
- 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. Go to the configuration page:
   - **Admin Console** > **Content** > **Promoted Results**
2. Under **Promoted Results Rules**, in **Language**, select the locale for which you want to add promoted links.
3. Under **Add or Edit a rule**, add a links for promotion as follows:
   a) In **Priority**, select the priority of the link.

      This is a number of the link in the list when the links are displayed to users. The starting number is `0`.

      Priority applies only within a group multiple rules with the same keyword or keywords. The rules are automatically set in the order in which you create them. Moving a rule to a higher priority moves other rules down in priority, affecting the numbering of all rules below it: the rules above and below it are renumbered to create a sequential list.

   b) In **Keywords**, add one or more keywords separated by commas.
   c) In **Content Link**, enter the full URL of a content item.

      For example, this can be `https://yourcommunity.com/docs/DOC-46692`.

   d) Click **Add**.
4. If you want more results to be returned for the same keyword, add more rules with the same keyword and different content items.

Because the rules 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 29. keyword2, keyword3 document n

The first ruleset says that when keyword 1 appears in a query, the first three results must 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 are documents x, r, and n.

Configuring user search

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

Configuring search synonyms for user names

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

Fastpath:

- **Admin Console** > **Content** > **User Synonyms**

You can set up synonyms for the names of users to improves results for user searches. For example, you might want to set up `James, Jim, Jimmy` or `Susan, Suzy, Susie`.

Note that by default, new synonyms work only on new content. Thus, the changes become available in ~30 seconds, after the search index is updated.

To set up search synonyms:

1. Go to the configuration page:
   - **Admin Console** > **Content** > **User Synonyms**
2. Under **Synonyms**, type in a comma-separated list of synonyms for user names.
3. Click **Add Synonyms**.

After synonyms are added, the indexing is updated automatically and in ~30 seconds the newly added synonyms will be available in search.

Getting information about performance

Jive provides tools by using which you can keep track of the application's performance and usage.

Auditing administrative tasks

Jive logs actions you and others take and you can see them in 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** > **Reports** > **Audit Log**

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 was executed. For each log entry, you can also see the detailed description and identity (IP address) of the web app node that captured the action.

You can filter this page by user and date.

Viewing user licenses

You can check the overall number of user licenses on the reports page and use the CSV download to check which users are counted towards licenses.

Fastpath:

- **Admin Console** > **Reports** > **License Usage**

How licenses are counted

License metering is the point of reference for measuring and billing for registered users in the Jive platform. Registered users are measured by the count of users who have logged in at least once.

- Licenses are counted only for **registered visible active user accounts with at least one login**.
- Deactivated users are not included in the licensing count.
- External contributors are not included in the licensing count.
- System service accounts are not included in the licensing count.

Licenses are measured on the last day of the month.

For more information on the account types, see User account definitions.

Downloading reports

To download a License Usage report:

1. Go to the report page:
   - **Admin Console** > **Reports** > **License Usage**
2. Select which fields you want to include in the report:
   - To download only the fields pertinent to license counting, leave the **Include additional profile fields** check box cleared.
   - To download the report with the full list of default profile fields, select the **Include additional profile fields** check box.
3. Click **Download CSV report**.

The report is downloaded to your computer in the CSV format.

Report contents

Reports are downloaded in CSV format.

This report includes the profile fields which are defined for your community. Depending on the selection, you can download:

- Only the fields pertinent to license counting with the **Include additional profile fields** check box cleared.
- The full list of the profile fields including the custom fields with the **Include additional profile fields** check box selected.

All date and time references are provided in the server time zone. For more information about account types and statuses, see User account definitions and User account statuses.