Documentation for Confluence 4.2

Contents

Confluence Administrator's Guide

Confluence Administrator's Guide

Additional Resources

Visit the Configuration Guide for documentation on configuring databases and application servers.
The Confluence User's Guide has information on how to use Confluence as a collaborative tool.
Go to Documentation Home for links to more resources.

Download

You can download the Confluence Admin Guide in PDF, HTML or XML formats.

Site Administrator?

The **Confluence Administrator's Guide** provides information to site administrators on how to manage their Confluence instances.

If you still have a question that hasn't been answered, write and tell us about it.

Configuring Confluence

Site Configuration

Optional Settings

Enabling Threaded Comments
Attachment Storage Configuration
Configuring Attachment Size

Display Settings

Configuring Indexing Language
Configuring Character Encoding
Configuring Time and Date Formats
Configuring Number Formats
Configuring Shortcut Links

Data and Backups

Site Backup and Restore
Production Backup Strategy

Backups Configuration

Configuring Backups
Scheduled Jobs
Manually Backing Up The Site

Restoring Data

Restoring a Site
Restoring a Space
Restoring Data During Setup
Restoring Data from the Administration Console
Retrieve file attachments from a backup
Restoring a Test Instance from Production

Scheduled Jobs

Scheduled Jobs

Data Model

Confluence Data Model

System Administration

System Configuration

Viewing System Information
Viewing and Editing License Details
Cache Statistics
Viewing Site Statistics

System Administration

Content Index Administration
Upgrading Confluence
Migrating Confluence Between Servers
Migrate to Another Database
Important Directories and Files
Rebuilding the Ancestor Table
Finding Unused Spaces

Large Confluence Installations

Operating Large or Mission-Critical Confluence Installations
Configuring a Large Confluence Installation
Overview of Confluence Clusters
Cluster Administration page

Importing Data

Mail Configuration

Security

Overview and Advisories

Security Options

User Management

Confluence User Management

External User Management

Crowd User Management

JIRA User Management

Design and Layout

Configuring Site and Space Layouts

Configuring Themes

Integrating Confluence and JIRA

Plugin Management

Macros

Performance Tuning

Character Encoding

Support

Administration

Administrators Guide Home Confluence Documentation Home

Cache Statistics

Confluence provides statistics about its internal caches that allow you to track the size and hit ratio of each cache and tune it for better performance (if necessary). See Performance Tuningfor more information.

Configurable Caches

System administrators can change the sizes of Confluence's internal caches through the Administration Console and these changes will take effect without the need to first shut down and then restart Confluence. The maximum number of units for any of the defined cache regions can be adjusted individually.

Note that larger cache sizes will require more memory at runtime, so you should review the memory allocation of the Confluence Java process and the physical memory available on your server.

The information on this page does not apply to Confluence OnDemand.

Viewing Cache Statistics and Modifying Cache Sizes

To view the cache statistics:

1. Choose **Browse** > **Confluence Admin**.
2. Click '**Cache Statistics**' in the left-hand panel. There you will find a list of all objects cached within Confluence.
3. Click the '**Advanced**' tab for more detail. Below is an example for one of the most frequently used caches, the 'Content Object' cache.

Name	Percent Used	Effectiveness	Objects / Size	Hit / Miss / Expiry	Adjust Size	Flush
Content Object	80%	73%	4023 / 5000	374550 / 140460 / 55044	*Adjust Size*	*Flush*

About the generated numbers:

Percent Used:	=(Objects)/(Size)
Effectiveness:	=(Hits)/(Hits + Misses)
Objects / Size:	The number of entries in the cache / the number of total possible entries allowed (configurable).
Hit / Miss / Expiry:	The number of reads accessing cache where required content was found / the number of reads accessing cache where required content was not found / the number of objects evicted from the cache.
Adjust Size	Use this option to specify a different maximum cache size. Enter a new cache size and click the '**Adjust Size**' button to set it.
Flush:	Flushes the cache.

For instance, to calculate **Percent Used**:

```
Percent Used = Objects / Size

Percent Used = 4023/5000 = 80%
```

To calculate **Effectiveness**:

```
Effectiveness = (Hits)/(Hits + Misses)

Effectiveness = 374550 / (374550 + 140460)
= 73%
```

The clustered versions of Confluence use distributed cache called Tangosol Coherence.

Watching the Cache Contents

To see the specific items in the caches, view the cache statistics at `<baseUrl>/admin/cachecontents.jsp`.

Additional Notes about Configurable Caches

Changes to cache size configurations persist across confluence restarts as they are saved in the `<confluence-home>/config/ehcache.xml` file (or `<confluence-home>/config/confluence-coherence-cache-config-clustered.xml` for a clustered instance). In most cases, a Confluence administrator will never need to know about these files. However, if it is necessary to tune cache options other than the maximum cache size, this can be done by manually editing these files. See Cache Performance Tuning for details.

Important note about clustered Confluence installations

The cache configuration file is stored in a home directory of each cluster node. When a Confluence administrator changes a cache size, all running cluster nodes will automatically update their own configuration files in their respective home directories. However, if a cluster node is not running when an administrator adjusts a cache size, the `/config/confluence-coherence-cache-config-clustered.xml` file in its home directory will not be updated. Since cluster caches are configured by the first node to start, if a node with an outdated cache configuration is the first to start up, the whole cluster would end up using the configuration of that node. However, copying this file from one node to another would resolve this issue.

Performance Tuning

If you need to tune your application when under high usage, you may like to review this document for suggestions.

Related Topics

No content found for label(s) system-information.

Administrators Guide Home Confluence Documentation Home

Confluence Data Directory Configuration

Here is a link listing important Confluence files.

The home directory defines the location of the directory where Confluence will store its data, including attachments, indexes and backups. Administrators can set this location by defining a value for the file `<MY-INSTALL>/confluence/WEB-INF/classes/confluence-init.properties`. To find what your home directory is currently set to, open this file and check the `confluence.home` property. It is unset on new installations.

> ⚠ *The information on this page does not apply to Confluence OnDemand.*

Windows Configuration

On Windows, this path:

```
C:\confluence\data
```

will be written like so:

```
confluence.home=C:/confluence/data
```

Note that all backslashes (\) are written as forward slashes (/).

Linux/Solaris Configuration

On any Linux-based system, the property is defined using the normal directory syntax:

```
confluence.home=/var/confluence/
```

Symbolic links

If your `confluence.home` directory contains a symbolic link, you must define the absolute path.

> ⛔ Please note that there can be no symbolic links within the `confluence.home` directory. If disk space is an issue, place the entire `confluence.home` directory on a disk partition where there is enough space.
>
> The absolute path of generated files (such as exports) is compared with the absolute path of the `confluence.home` directory when constructing URLs. When a sub-directory has a different path, the URL will be incorrect, and you may receive "Page not found" errors. These measures are in place to prevent "directory traversal" attacks.

Fixing the Confluence Configuration

The Confluence configuration file: `confluence-cfg.xml` inside the home directory may contain references to the original location of your Confluence home. You will need to edit this file to update these references to also point to the new location. The two properties in this file that need to change are:

- `daily.backup.dir` if you have not configured your backups to be placed elsewhere already
- `hibernate.connection.url` if you are using the embedded HSQL database.

Content Index Administration

The content indexes power Confluence's search functionality. They are also used for a number of related functions such as building email threads in the mail archive, the space activity feature and lists of recently-updated content. The Gliffy plugin also uses them for some of its functionality.

For reasons of efficiency, Confluence does not immediately add content to the index. New and modified Confluence content is first placed in a queue and the queue is processed once every minute (by default).

On this page:

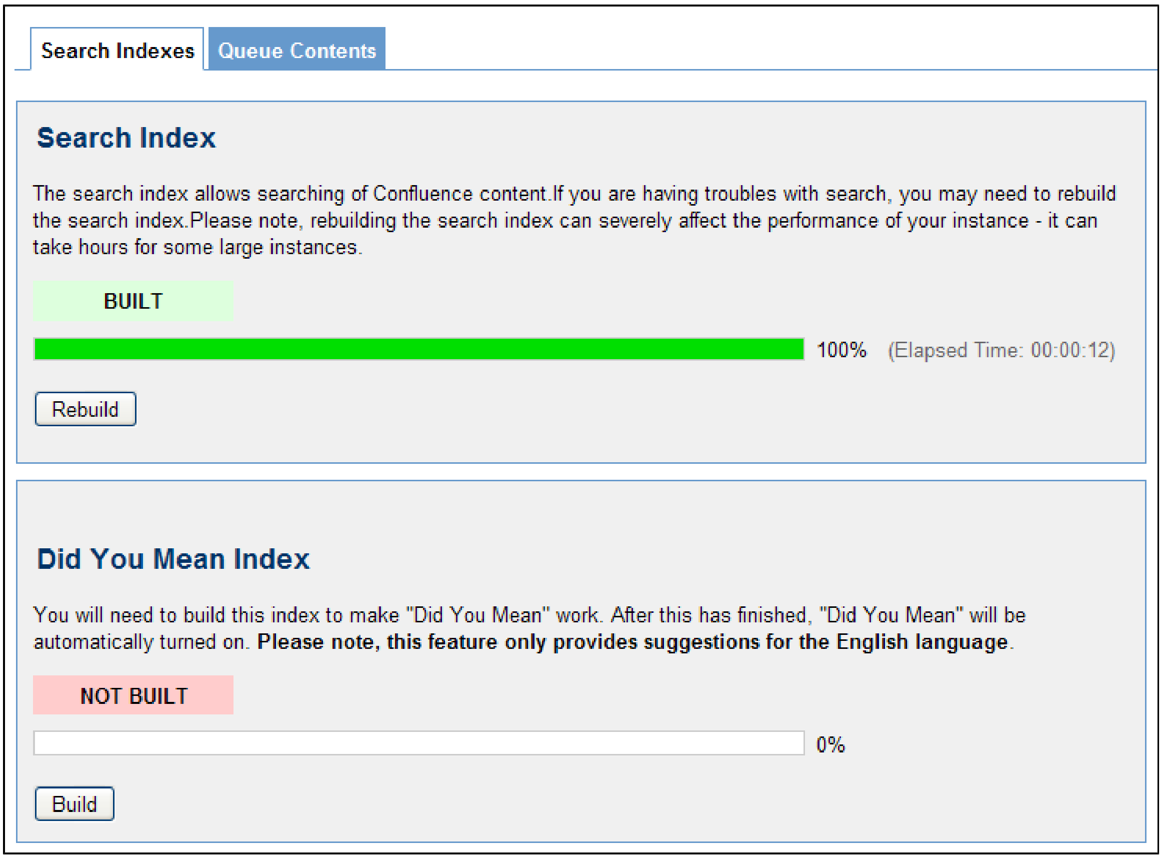
⚠ *The information on this page does not apply to Confluence OnDemand.*

Viewing the Content Index Summary

To see information about your Confluence instance's content indexing,

1. Choose **Browse** > **Confluence Admin**.
2. Click '**Content Indexing**' under the heading '**Administration**' in the left-hand panel.

Screenshot: Index summary



Search Index

The search index allows searching of Confluence content.If you are having troubles with search, you may need to rebuild the search index.Please note, rebuilding the search index can severely affect the performance of your instance - it can take hours for some large instances.

BUILT

100% (Elapsed Time: 00:00:12)

Did You Mean Index

You will need to build this index to make "Did You Mean" work. After this has finished, "Did You Mean" will be automatically turned on. **Please note, this feature only provides suggestions for the English language**.

NOT BUILT

0%

Rebuilding the Content Indexes

The content indexes are maintained automatically, but you may need to rebuild one or both of them manually under circumstances such as these:

- Your searching and mail threading are malfunctioning. (Rebuild the Search Index.)
- The Did You Mean feature is malfunctioning. (Rebuild the Did You Mean Index.)
- After an upgrade. If a content re-index is required after an upgrade, it will be noted in an upgrade subsection of the relevant Release Notes.

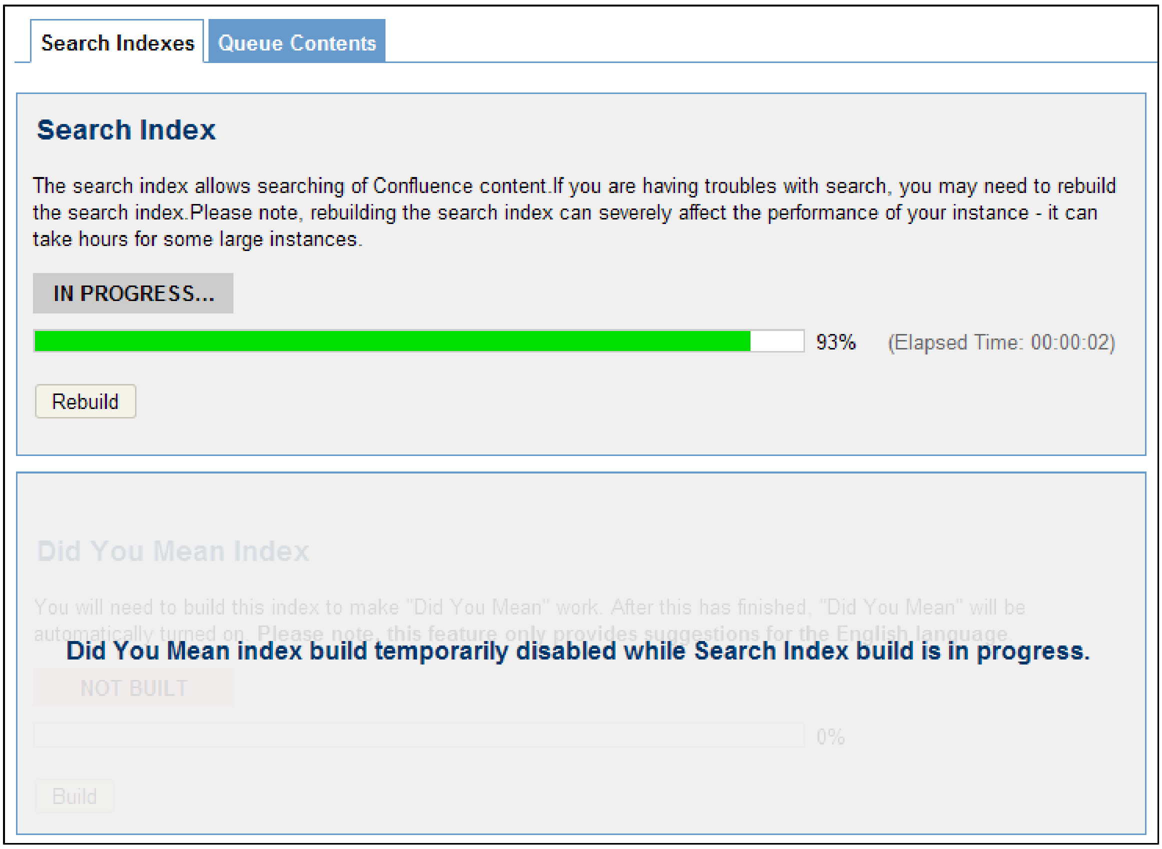
> In new Confluence installations, the 'Did You Mean' feature is not initially activated. To activate it, you first need to build its index by clicking its '**Build**' button on this page.

To rebuild either of the content indexes,

1. Choose **Browse** > **Confluence Admin**.
2. Click '**Content Indexing**' under the heading '**Administration**' in the left-hand panel.
3. Click the '**Rebuild**' button in either the 'Search Index' or 'Did You Mean Index' sections on this page, depending on the particular index you want to rebuild.

> - If one of these indexes has not yet been built, its button will indicate 'Build' instead of 'Rebuild).
> - As shown in the image below, only one index can be (re)built at a time.

Screenshot: Content Indexing



Search Index

The search index allows searching of Confluence content.If you are having troubles with search, you may need to rebuild the search index.Please note, rebuilding the search index can severely affect the performance of your instance - it can take hours for some large instances.

Did You Mean Index

You will need to build this index to make "Did You Mean" work. After this has finished, "Did You Mean" will be automatically turned on. Please note, this feature only provides suggestions for the English language

Did You Mean index build temporarily disabled while Search Index build is in progress.

Slow Reindexing

Does the reindexing take a long time to complete? The length of time depends on the following factors:

- Number of pages in your Confluence instance.
- Number, type and size of attachments.
- Amount of memory allocated to Confluence.

It may help to increase the heap memory allocation of Confluence by following the instructions in the JIRA documentation.

If you are running an older version of Confluence and find that the index rebuild is not progressing, you may need to shut down Confluence, and restart it with the following *Java system property* set: `bucket.indexing.threads.fixed=1`. This will cause the re-indexing to happen in a single thread and be much more stable (but slower).

Viewing the Index Browser

Confluence uses a search engine called Lucene. If you need to see more details of the indexed pages in your Confluence site, you can download and run Luke. Luke is a development and diagnostic tool that accesses existing Lucene indexes and allows you to display and modify their content in several ways.

Start Luke and use it to open the `index` directory, located in your Confluence Home directory. For example: `c:\confluence\data\confluence-home\index`.

More Hints and Tips

- If you are still experiencing problems after performing the above rebuild, the next step might be to remove the index and rebuild it from scratch.
  ⚠ The space activity feature uses the index to store data. If you remove the index file, the existing activity data will disappear.
- A tip for the development community: If you have the Confluence source, you can look for references to the SmartListManager to find the screens and lists that rely on the content index.

RELATED TOPICS

No content found for label(s) index.

Administrators Guide Home Confluence Documentation Home

Finding Unused Spaces

Sometimes, you want to know what is *not* being used. It's great to know what's getting most attention, but what about stagnant pages, or even entire spaces that are no longer active?

While viewing space activity can provide hints, it doesn't always provide enough detail. The simple way is to go directly to the database. We recommend DbVisualizer, and have basic instructions for connecting it to HSQLDB.

The following query identifies the last date on which content was modified in each space within a single Confluence instance:

```
SELECT spaces.spacename, MAX(content.lastmoddate)
FROM content, spaces
WHERE content.spaceid = spaces.spaceid
GROUP BY spaces.spacename;
```

It returns a list of spacenames, and the last date and time at which any content was added or changed.

⚠ *The information on this page does not apply to Confluence OnDemand.*

Alternatively, this one simply identifies spaces whose content hasn't changed since a specified date:

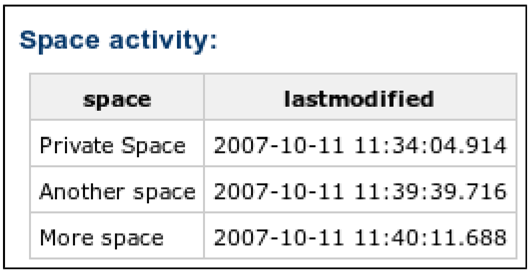
```
SELECT spaces.spacename
FROM content, spaces
WHERE content.spaceid = spaces.spaceid
GROUP BY spaces.spacename
HAVING MAX(content.lastmoddate) <
'2006-10-10';
```

The result is a simple list of space names.

It's also possible to present the information in a wiki page, using the SQL plugin, which can be installed using the Plugin Exchange. You'll also need to define a database resource in `conf/server.xml` and `confluence/WEB-INF/web.xml`, as described here. Having done so, you can use wiki markup code like the following, replacing `confluenceDS` with the name of your own local datasource:

```
h3. Space activity
{sql:dataSource=confluenceDS|output=wiki}
SELECT spaces.spacename AS Space,
MAX(content.lastmoddate) AS LastModified
FROM content, spaces
WHERE content.spaceid = spaces.spaceid
GROUP BY Space;
{sql}
```

The result will be something like this:



Space activity:

space	lastmodified
Private Space	2007-10-11 11:34:04.914
Another space	2007-10-11 11:39:39.716
More space	2007-10-11 11:40:11.688

You can try the Chart plugin in combination with the SQL plugin to give more visually attractive results.

Important Directories and Files

The Installation Directory

The 'Confluence Installation directory' is the directory into which the Confluence application files and libraries have been unpacked (unzipped) when Confluence was installed. Confluence does not modify or store any data in this directory. This directory is also sometimes called the 'Confluence Install directory'.

Important Files and Directories

- `confluence/WEB-INF/classes/confluence-init.properties` : This file tells Confluence where to find the Confluence Home Directory. This file is modified by the administrator when installing Confluence.
- `confluence/WEB-INF/classes/osuser.xml` : This file is modified when connecting Confluence to an external user management system such as an LDAP server or JIRA instance in Confluence 2.0 and earlier. For more information, refer to Understanding User Management in Confluence.
- `confluence/WEB-INF/classes/atlassian-user.xml` : This file is modified when connecting Confluence to an external user management system such as an LDAP server or Crowd. For more information, refer to Understanding User Management in Confluence.
- `confluence/WEB-INF/lib/` : This directory is used when deploying plugins, especially those plugins that cannot automatically be loaded through the Administration Console.
- `confluence/WEB-INF/classes/log4j.properties` : Confluence's logging configuration file. See Working with Confluence Logs.
- `confluence/WEB-INF/classes/ehcache.xml` : This is where you can configure the size of Confluence's internal caches
- `confluence/WEB-INF/classes/styles/site-css.vm` : Confluence's main stylesheet, modify at your own risk
- `conf/server.xml` : SSL configuration.

Memory Settings

The file used to edit JAVA_OPTS memory settings will depend on the method used to install Confluence, as well as the operating system used for your installation.

- Windows Users
  - **Confluence** — `bin/setenv.bat`
  - **Confluence Installer** — `wrapperwin32.conf`
- Mac/Linux Users
  - **Confluence** — `bin/setenv.sh`
  - **Confluence Installer** — `wrapperosx.conf`

> ⚠ *The information on this page does not apply to Confluence OnDemand.*

The Temp Directory

The temp directory is configured in the Java runtime and some Confluence components write temporary files or lockfiles into this directory.

Typically, this directory is `/tmp` on Linux systems, or `C:\Temp` on Windows.

To change the location of this directory, you should start the Java Virtual Machine in which confluence is running with the argument:

`-Djava.io.tmpdir=/path/to/your/own/temp/directory`.

The Confluence Home Directory

The Confluence Home directory is the folder where Confluence stores its configuration information, search indexes and page attachments. If you are using the embedded HSQLDB database supplied for evaluation purposes, the database files are also stored in this directory.
✅ Tip: Another term for 'Home directory' would be 'data directory'.

Administrators can expect the Confluence Home Directory to grow quite large in a busy site.

The location of this directory is configured by the system administrator during installation (see `confluence-init.properties` above).

Important Files and Directories

- `confluence.cfg.xml` : Confluence's core configuration file; includes the configuration for connecting to its database.
- `default-formatting.properties` : Some auxiliary configuration data concerning default number and date formats.
- `attachments/` : All file attachments in the Confluence site are stored under this directory. This is the only place Confluence keeps attachment files.
- `backups/` : If Confluence is configured to produce daily backups, these are kept in this directory. Administrators should occasionally delete old or unwanted backups from this directory to prevent it from growing too large.
- `config/` : Miscellaneous global and per-space configuration files are kept in this directory.
- `database/` : If Confluence is being run from the embedded HSQL database, the database files will be kept in this directory.
- `index/` : The full-text search index is kept in this directory. Removing or modifying files in this directory may cause search to no longer function. Rebuilding the search index from Confluence's global administration screen will completely regenerate the contents of this directory.
- `plugins/` : Dynamically uploaded plugins are stored in this directory. Administrators can install new plugins by copying them into this directory and triggering a scan from the plugin management page.
- `temp/` : Confluence stores temporary files in this directory, especially during backups and exports. A daily job within Confluence deletes files that are no longer needed.
- `thumbnails/` : Stores temporary files for image thumbnails. The contents of this directory can be safely deleted, as Confluence will regenerate thumbnails as required.
- `velocity/` : Storage for customised page layouts, globally and per-space.

Database

All other data — page contents, links, archived mail and so on — is kept in the database. If you have configured Confluence to use the embedded HSQL database, the database will store its files under `database/` in the Confluence Home Directory. Otherwise, the database management system you are connecting to is responsible for where and how your remaining data is stored.

> **Tip**
>
> All of Confluence's persistent data is stored either in the Confluence Home Directory, or the database. If you have backup copies of both of these, taken at the same time, you will be able to restore Confluence from them (see Restoring Data from other Backups).

RELATED TOPICS

Confluence Home Directory
Confluence Installation Directory
The Embedded HSQLDB Database
Database Configuration

Administrators Guide Home Confluence Documentation Home

Confluence Home Directory

Often in the documentation, you'll see a reference to the 'Confluence Home directory'.

What is the Confluence Home Directory?

The Confluence Home directory is the folder where Confluence stores its configuration information, search indexes and page attachments. If you are using the embedded HSQLDB database supplied for evaluation

purposes, the database files are also stored in this directory.
✅ Tip: Another term for 'Home directory' would be 'data directory'.

> ⚠ *The information on this page does not apply to Confluence OnDemand.*

Finding the Confluence Home Directory

The location of the Confluence Home directory is defined when you install Confluence. This location is stored in a configuration file called `confluence-init.properties`, which is located inside the `confluence/WEB-INF/classes` directory in your Confluence Installation directory.

When Confluence first starts up, it reads the `confluence-init.properties` file to determine where to look for the Home directory.

Once Confluence is running you can find the Confluence Home directory via the Administration console, under Administration > System Information > Confluence Information - Confluence Home.

Content of the Confluence Home Directory

The Confluence home directory contains some of the configuration data used by Confluence. Other data is stored in the database. This section outlines the purpose of the files and directories in the Confluence home directory.

`confluence.cfg.xml`

This file contains all of the information necessary for Confluence to start up, such as:

- Product license
- Context path
- Database details, such as location and connection pool settings
- Paths to important directories

`attachments`

This directory contains every version of each attachment stored in Confluence. This directory is not used when Confluence is configured to store attachments in the database. Attachments are always stored in the database in clustered instances of Confluence.

Paths within this directory have the following structure:

```
/attachments/PAGE_ID/ATTACHMENT_ID/VERSION
```

You can specify an alternative directory for attachment storage by setting the `attachments.dir` property in `confluence.cfg.xml`.

`backups`

Confluence will place its daily backup archives in this directory, as well as any manually generated backups. Backup files in this directory take the following form:

```
daily-backup-YYYY_MM_DD.zip
```

You can specify an alternative directory for backups by setting the `daily.backup.dir` property in `confluence.cfg.xml`.

`bundled-plugins`

Confluence ships with a set of *bundled* plugins. These are plugins written by the Atlassian and the Confluence community that we think provide useful and broadly applicable functionality in Confluence. The {{bundled-plugins)) directory is where Confluence will unpack its bundled plugins when it starts up. This directory is refreshed on every restart, so removing a plugin from this directory will not uninstall the plugin. It will simply be replaced the next time Confluence starts up.

`database`

This is where Confluence stores its database when configured to run with the HSQL embedded database. In such cases this directory contains all Confluence runtime data. Installations configured to run using an external database such as MySQL will not use this directory.

`index`

This is where Confluence stores its indexes for rapid retrieval of often used data. The Confluence index is used heavily by the application for content searching and recently updated lists and as such is critical for a running Confluence instance. It is important to note however that should the data in this directory be lost or corrupted, it can be restored by running a full reindex from within Confluence. This can take a long time depending on how much data is stored Confluence's database.

An alternative directory may be specified for the index by setting the `lucene.index.dir` property in `confluence.cfg.xml`. As this is the most heavily accessed directory in the Confluence home directory you might want to consider hosting it on the fastest disk available. It would also be useful if the disk holding the Confluence index was not heavily used by any other application to reduce access contention.

`plugin-cache`

All Confluence plugins are stored in the Confluence database. To allow for quicker access to classes contained within the plugin JARs, Confluence will cache these plugins in the `plugin-cache` directory. This directory is updated as plugins are installed and uninstalled from the system and is completely repopulated from the database every time Confluence is restarted. Removing plugins from this directory does not uninstall them.

`resources`

The `resources` directory stores any space logos used in your Confluence instance. For each space with a space logo, there is a directory within `resources` named after the space's key. That directory contains the space's logo.

`temp`

The `temp` directory is used for various runtime functions such as exporting, importing, file upload and indexing. As the name suggests, and file in this directory is of temporary importance and is only used during runtime. This directory can be safely emptied when Confluence is offline.

An alternative directory may be specified for temporary data by setting the `webwork.multipart.saveDir` property in `confluence.cfg.xml`.

`thumbnails`

When Confluence generates a thumbnail of an image (for example when the `gallery` macro is used), the resulting thumbnail is stored in this directory for quicker retrieval on subsequent accesses. This directory is essentially a thumbnail cache, and deleting files from this directory simply means the thumbnail will have to be regenerated on the next access.

RELATED TOPICS

Confluence Installation Directory
Important Directories and Files
The Embedded HSQLDB Database

Confluence Installation Directory

The 'Confluence Installation directory' is the directory into which the Confluence application files and libraries have been unpacked (unzipped) when Confluence was installed. Confluence does not modify or store any data in this directory. This directory is also sometimes called the 'Confluence Install directory'.

> ⚠ *The information on this page does not apply to Confluence OnDemand.*

RELATED TOPICS

Confluence Home Directory
Important Directories and Files

Installing a Language Pack

Confluence ships with a number of bundled language packs. These languages appear as options on the 'Language Configuration' screen in the Administration Console when choosing a default language and as 'Language' options for users in their user settings. You can make additional languages available for selection by installing language packs. Please note, you must be a Confluence administrator to install a language pack.

Language packs are plugins. The process of installing a language pack is the same as installing a new plugin.

> ⚠ *The information on this page does not apply to Confluence OnDemand.*

Installing a Language Pack using the Plugin Manager

To install a language pack using the plugin manager:

1. Click '**Plugins**' in the Confluence Administration Console.
2. Click '**Install**'.
3. Locate the language pack and install it via the plugin manager interface.

Installing a Language Pack Manually

To install a language pack manually, you will need to upload the language pack plugin as described below. The language pack plugin will be enabled by default once you have installed it.

Plugins are distributed as a jar file. To install a plugin:

1. In the 'Administration' section of Confluence, click **Plugins**.
2. Use **Browse** to find the plugin jar you wish to install from your hard drive or network location, and select it.
3. Click **Upload**.
4. The plugin will be uploaded to Confluence and will be automatically installed.
5. Check the 'Plugin Administration' screen to ensure that the plugin is available.
6. Enable the plugin if necessary. (Some plugins will be enabled by default when they are installed. Others will have to be manually enabled from the 'Plugin Administration' screen.)

Finding more Language Packs

- You can download official language packs from the Atlassian Plugin Exchange. You can also download language packs developed by the Confluence user community from the Language Pack Translations page.

Showing User Interface Key Names for Translation

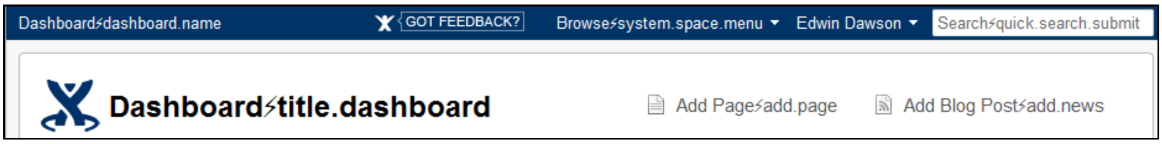
For those customers working on creating translations of the Confluence user interface, from 4.1 onwards there is a feature that will help. After opening the Confluence dashboard, you can simply add this text to the end of your Confluence URL, like so:

```
?i18ntranslate=on
```

Then press Enter.

This will then cause each element of the user interface to display its special **key name** while Confluence is still in an interactive mode. This makes it easier to find the essential context for each key, which can then be searched on http://translations.atlassian.com where you can enter an appropriate translation for your custom language pack.

The key names are displayed with a "lightning bolt" graphic between elements of the names. For example, the buttons will show up with elements shown like so:



For example, for the **Browse** button, the associated key **system.space.menu** can be found on http://translations.atlassian.com, allowing you to write a better translation for the term **Browse**, being able to see the full context of where the UI element belongs and what it means to the user.

To turn off the translation view, add this code to the end of the Confluence URL:

```
?i18ntranslate=off
```

RELATED TOPICS

Choosing a Default Language
Configuring Indexing Language
Installing a Plugin

Site Backup and Restore

> ⚠ Atlassian suggests establishing a backup strategy using a native database tool for a production instance of Confluence.

By default, Confluence backs up all data and attachments once a day to a backup file. These files are called XML site backups, and are stored in the `backups` directory of Confluence home. You can also create XML site backups manually. This mechanism is intended for small to medium-sized deployments of Confluence. It is not intended for use with large deployments with lots of pages and attachments (see below).

- Restore your site from an XML site backup

- Manually create an XML site backup
- Configuring Backups
- User Submitted Backup & Restore Scripts

XML site backups are fine for most small to medium-sized instances of Confluence, containing a few thousand pages and attachments. However, large instances of Confluence may find that backups become slow to create and use large amounts of disk space.

> ⚠ *The information on this page does not apply to Confluence OnDemand.*

Backups For Large Instances

XML site backups are unsuitable for instances of Confluence that contain thousands of pages, as XML backups take progressively longer to complete as the amount of text increases. Another issue with XML site backups is that Confluence instances with gigabytes of attachments will consume disk space rapidly. This is because each site backup contains all content needed for a site restore. For example, if a 1 GB instance of Confluence is backed up daily, it will create 30 GB of backups per month if left unattended. When administering a large instance, you can reduce disk space by setting XML site backups to exclude attachments, then manually scheduling a backup of your attachments from the Confluence home directory or database. The backup manager can save space by saving changed files instead of all content.

Creation Delay	Disk Usage	Recommended Backup Method
Acceptable	Acceptable	XML site backup with attachments
Acceptable	Unacceptable	XML site backup minus attachments, plus manual backup of attachments
Unacceptable	Unacceptable	Manual backup of database and attachments

Creation Delay is the time it takes to create an XML site backup *minus attachments*.
Disk Usage can be estimated by multiplying the frequency of your XML site backups by their current size.

Manual Backups

Confluence's Attachment Storage Configuration can be set to store attachments in the Confluence home directory, or in the database.

Database Backup
Use your Database Administration Tool to create a backup of your Confluence database. If your database is storing your attachments, importing this later will restore all content. For instances with big attachments, please note that currently Confluence migrate attachments in a single transaction: CONF-9888.

Attachment Backup
If stored on the filesystem, attachments are placed under the `attachments` directory of your Confluence home directory. Copy this directory to create a backup of all attachments.

To restore from these backups, please refer to Restoring Data from other Backups.

Related Topics

Production Backup Strategy

Backup FAQ

Production Backup Strategy

Confluence's Built-in Backup

Confluence automatic daily XML backup is ideal if you:

- are evaluating Confluence
- do not have database administration familiarity, and your Confluence installation is small

Once your Confluence installation reaches more than a few thousand pages, the XML backup facility can be inefficient compared to your database's own backup tools.

> ⚠ *The information on this page does not apply to Confluence OnDemand.*

Establishing a Production System Backup Solution

The built in backup functionality in Confluence requires a lot of memory to run and is less reliable when restoring. Atlassian recommends establishing an alternative database backup strategy:

- Create a backup or dump of your database using tools provided by your database
- Create a file system backup of your Confluence home directory

Once this is in place, disable the daily backups through the scheduled jobs feature via **'Administration Console > Administration > Scheduled Jobs'**.

We want to stress that creating these two backups is *better* than having a Confluence XML backup. It's more robust and far more reliable for large production instances. You will be able to restore your whole site, including all data, attachments and configuration information intact with these two backups. We have written up a document on how to do this here.

Step by step instructions

Take a look a the Migrating Confluence Between Servers document for instructions on restoring a backup using this technique.

Other processes

XML backups are described and used for other processes in Confluence, like upgrading and moving servers. Using the backup strategy described here will work for those processes. Our upgrade guide does not require the use of an xml backup (an old upgrade procedure, and the JIRA upgrade guide use XML backups for upgrading), and our migrate server procedure - used to set up a test server - can leverage an sql dump as well.

The only process that requires the XML backup is the database migration procedure. Large data sets will require third party database migration tools.

RELATED TOPICS

Site Backup and Restore
Backup FAQ

Configuring Backups

Confluence backs up your data regularly into a zipped XML file. By default, this backup is performed at 2.00 a.m. each day and the backup files are stored in the `backups` folder under the Confluence Home directory. The default naming convention for the backup files is '`backup-yyyy_MM_dd`'. Confluence can write backups to both local and mapped network drives.

From the **Backup Administration** section of Confluence's administration console, you can:

- Include or exclude attachments in backups.
- Configure a different path to store backup files. (By default, this option is not available. See below for information about enabling the configuration option.)
- Change the naming format used for the files.

✓ You can also change the schedule of this backup using Confluence's scheduled jobs feature.

ℹ You need to have System Administrator permissions in order to configure these options.

On this page:

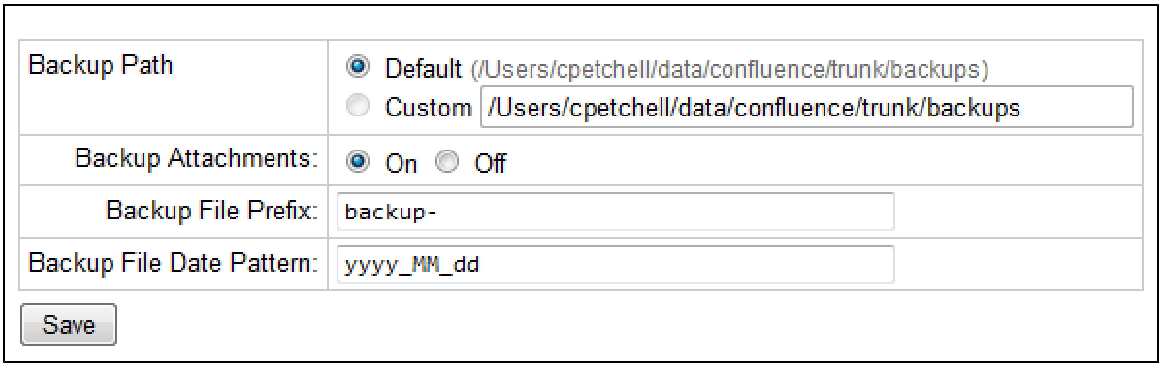
⚠ *The information on this page does not apply to Confluence OnDemand.*

Configuring Confluence Backups

To configure Confluence backups:

1. Choose **Browse** > **Confluence Admin**.
2. Click '**Backup Administration**' in the '**Configuration**' section.
3. Click the '**Edit**' button on the '**Backup Administration**' screen.
4. Now you can do the following:
    - To specify an alternate path to store backup files — Select '**Custom**' and then enter the path. The directory must be on either a local drive or a mounted network drive.
      ℹNotes:
        - By default, this option is not available. See below for information about enabling the configuration option.
        - Please ensure the mapped drive is on a physical server, not a Virtual Machine image.
    - To exclude attachments from backups — Select '**Off**' beside '**Backup Attachments**'. By default, this feature is 'On'.
    - To use a different naming prefix format — Enter the new format in the '**Backup File Prefix**' input field.
    - To use a different date format — Enter the date format in the '**Backup File Date Pattern**' input field using the syntax described in this document from Sun.
5. '**Save**' your changes.

✓ You can disable Confluence backups through the scheduled jobs feature.



Backup Path	● Default (/Users/cpetchell/data/confluence/trunk/backups) ○ Custom /Users/cpetchell/data/confluence/trunk/backups
Backup Attachments:	● On ○ Off
Backup File Prefix:	backup-
Backup File Date Pattern:	yyyy_MM_dd

Screenshot above: Editing the Backup Configuration

Enabling Backup Path Configuration

By default, it is not possible to specify a backup path via the Confluence Administration Console. This feature is disabled by default for security reasons. Administrators can restore this functionality by updating the relevant configuration property as described below. However, we recommend that you turn the feature **off** in production environments.

To enable the configuration option:

1. Edit the `confluence.cfg.xml` file found in the Confluence Home Directory.
2. Set the value of property `admin.ui.allow.daily.backup.custom.location` to '`true`' (without the quotation marks).
3. Restart Confluence.

If the value of the above configuration property is 'true', it will be possible to specify a backup path via the Confluence Administration Console. If the value of this property is 'false' or the property is not present in the configuration file, the backup path is not configurable.

Notes

Time is derived from the Confluence server

The time zone is taken from the server on which Confluence is running.

To check the time according to the server, do the following:

1. Choose **Browse** > **Confluence Admin**.
2. Click '**System Information**' in the left-hand panel and look at the '**System Time**'.

Backup strategy for large Confluence sites

Consider using the production backup strategy if your Confluence site is large or you are encountering problems with your automated backup.

RELATED TOPICS

No content found for label(s) daily-backup.

Administrators Guide Home Confluence Documentation Home

User Submitted Backup & Restore Scripts

These scripts are user-submitted and should be used with caution as they are not covered by Atlassian technical support. If you have questions on how to use or modify these scripts, please post them to Atlassian Answers. Feel free to submit new scripts or post updates by logging in and adding them to the page as a comment.

> ⚠ *The information on this page does not apply to Confluence OnDemand.*

Delete Old Backups - Wscript Script On Windows

This script examines backup filename and deletes them if necessary, it may need to be edited.

```
'If you want 3 day old files to be deleted
then insert 3 next to Date - "your number
```

```
here"
'This script will search out and delete
files with this string in them
".2005-12-04-" This of course depends on
the number you enter.
'You can always do a wscript.echo
strYesterday or strFileName to see what
the script thinks you are searching for.

dtmYesterday = Date - 3

strYear = Year(dtmYesterday)

strMonth = Month(dtmYesterday)
If Len(strMonth) = 1 Then
    strMonth = "0" & strMonth
End If

strDay = Day(dtmYesterday)
If Len(strDay) = 1 Then
    strDay = "0" & strDay
End If

strYesterday = strYear & "-" & strMonth &
"-" & strDay

strFileName = "C:\test*." & strYesterday
&"-*"
```

```
Set objFSO =
CreateObject("Scripting.FileSystemObject")
objFSO.DeleteFile(strFileName)
```

Delete Old Backups - Basic Bash Script For Linux

Old XML backups can be deleted automatically by inserting a nightly or weekly automation script or cron similar to the following:

```
ls -t <path to your backup dir>/* | tail
-n +6 | xargs -i rm {}
```

Or, using the older form of the `tail` command if your system does not support the standard form:

```
ls -t <path to your backup dir>/* | tail
+6 | xargs -i rm {}
```

Delete Old Backups - Advanced Bash Script For Linux

Old XML backups can be deleted automatically by inserting a nightly or weekly automation script or cron similar to the following. Set the BACKUP_DIR and DAYS_TO_RETAIN variables to appropriate values for your site. Between runs, more files than DAYS_TO_RETAIN builds up.

```
#!/bin/sh

# Script to remove the older Confluence
backup files.
# Currently we retain at least the last
two weeks worth
# of backup files in order to restore if
needed.

BACKUP_DIR="/data/web/confluence/backups"
DAYS_TO_RETAIN=14

find $BACKUP_DIR -maxdepth 1 -type f
-ctime +$DAYS_TO_RETAIN -delete
```

Manual Database & Home Backup - Bash Script For Linux

This backs up a mySQL database and the Confluence home directory.

```
#!/bin/bash
CNFL=/var/confluence
CNFL_BACKUP=/backup/cnflBackup/`date
+%Y%m%d-%H%M%S`

rm -rf $CNFL/temp/*
mkdir $CNFL_BACKUP
mysqldump -uroot -p<password>
confluence|gzip >
$CNFL_BACKUP/confluence.mysql.data.gz
tar -cjvf $CNFL_BACKUP/data.bzip $CNFL >
$CNFL_BACKUP/homedir.status
```

Backup by Date - Postgres

```
export d=`date +%u`
mkdir -p /home/backup/postgres/$d

sudo -u postgres pg_dumpall | bzip2 >
/home/backup/postgres/$d/sql.bz2
```

Related Topics

- Site Backup and Restore
- Backup FAQ

Manually Backing Up The Site

Confluence is configured to back up its data. A System Administrator can also manually perform this back up from the **Administration Console**.

You need to have System Administrator permissions in order to perform this function.

> ✓ Consider an Production backup strategy if your Confluence site is large or you are encountering problems with your automated backup.

> ⚠ *The information on this page does not apply to Confluence OnDemand.*

Creating the Site Backup

To manually back up your site,

1. Choose **Browse** > **Confluence Admin**.
2. Click '**Backup & Restore**' in the 'Administration' section of the left-hand panel.
3. Select '**Archive to backups folder**' to store a copy of the backup in the same folder as Confluence's backups. (If you do not archive the backup it will be made available for you to download, and then deleted from the server after 24 hours).
4. Select '**Backup attachments**' to include attachments in your backup.
5. Click '**Backup**'.
   Please note that this process will take a few minutes.

> ✓ If you are running Confluence behind Apache and are facing timeout errors, please consider creating the export directly from Tomcat, instead of going through Apache. This will speed up the process and prevent timeouts.

Retrieving the Backup File

Confluence stores the backup as a zipped XML file in the '`backups`' directory under the Confluence Home directory on your Confluence server. To find your Confluence Home directory, see the documentation. You will need access to the Confluence server in order to retrieve this file.

Enabling the Download of the Backup File via the Administration Console

By default, it is not possible to retrieve the backup file via the Confluence Administration Console. This feature is disabled for security reasons.

Administrators can enable this functionality by updating the relevant configuration property as described below. When enabled, you will be prompted to download the backup file when the backup process finished. However, we recommend that you turn the feature **off** in production environments.

To enable download of the backup file from the Administration Console,

1. Edit the `confluence.cfg.xml` file found in the Confluence Home Directory.
2. Set the value of property `admin.ui.allow.manual.backup.download` to '`true`' (without the quotation marks).
3. Restart Confluence.

If the value of the above configuration property is 'true', it will be possible to download the backup file after manually backing up the site via the Confluence Administration Console. If the value of this property is 'false' or the property is not present in the configuration file, you will need to retrieve the backup file from the file system on the Confluence server. By default, the value is 'false'.

RELATED TOPICS

No content found for label(s) daily-backup.

Administrators Guide Home Confluence Documentation Home

Migrating Confluence Between Servers

This page describes how to move Confluence between physical servers. It is distinct from other functions. It does not cover database migration, application server migration, or upgrading. Atlassian suggests doing each of these steps separately. See also:

- Upgrading Confluence
- Migrate to Another Database
- Switching to Apache Tomcat

On this page:

⚠ *The information on this page does not apply to Confluence OnDemand.*

How to Create a Test or Development Instance

Administrators may need to move a Confluence instance from one server to another for upgrades or downtime. This page tells you how to copy a Confluence instance from one server to another. For example, you may want to transfer your current production snapshot to a test server as permitted in the licence agreement.

ℹ Development licenses are available for any Commercial or Academic license. Create one or contact Atlassian for help.

> ⚠ **Avoid upgrades while transferring**
>
> If you are planning to switch databases, application servers or Confluence versions, firstly perform the application transfer in isolation, and test that it was successful before making other changes.

Transferring Confluence To Another Server Using The Same Operating System

If the operating systems on both servers are the same, then the home and install folders can be copied straight into an identical external database and user management setup.

1. On the original server, create zips of the Confluence install and home directories. Copy the zips to the new server.
2. On the new server, unzip the install and home directories. Windows users should avoid unzipping with the Windows built-in extractor, instead use Winzip or the free 7Zip.

   > ⚠ If you are changing the location of the home directory, open the Confluence install\confluence\WEB-INF\classes directory and edit confluence-init.properties by changing the line starting with 'confluence.home='.

3. Modify the location of your war file if need be. If using Tomcat, this is likely in /Conf/Catalina/localhost. You'll want to make sure the docbase attribute is pointing to the right location.
4. This next step is dependent on your database:

   a. Database configuration:
      i. For users of the *internal database*, the database content is stored inside the home directory. You should switch to an external database after the transfer is successful.
      ii. For *external databases stored on another server*: change the user account or datasource permissions so that the new server has the same network access permissions as the original. Then confirm from the new server that the hostname can be resolved and is listening for database connections on the expected port.
      iii. For *external databases hosted locally (ie. localhost)*: on the original server, create a manual database backup using a native db dump backup tool. Copy the database backup to the new server.
   b. On the new server, install or upgrade the database version to match the original server.
   c. Import the database backup.
   d. Add a database user account with the same username and password as the original.
   e. Provide the user with the full access to the imported database.
   f. Use a database administration tool to confirm that the user can login from the localhost.
   g. To modify any database connection information, go to the Confluence home directory and edit confluence.cfg.xml. The connection URL is set under hibernate.connection.url. **Ensure it does not point to your production database server.**
   h. If you are using internal user management, skip this step. For users who have JIRA or LDAP integration, provide the new server with network or local access to the same hosts as the original. If this is a true test instance, set up a test of your JIRA instance or LDAP server so as not to disrupt production systems and change the server.xml or atlassian-user.xml files to point to the appropriate test servers. Note that it might be acceptable to use a production connection here, as users won't be logging on to the test system in high volume.
   i. If appropriate, make sure no emails are sent out from the test system.
   j. Start Confluence.
   k. Go to Administration > License Details and add your development license key. You can generate one at http://my.atlassian.com. There are more details in Getting a License for a Staging Environment.
   l. If you configured Confluence as a Windows service, repeat those instructions.
   m. Add your development license key.

5. Some customers have experienced problems with Confluence's search functions after performing a migration, or that the content of their `{recently-updated}` macro is not being updated correctly. Errors in the `atlassian-confluence.log` file corroborate such problems. Hence, to avoid these issues, it is strongly recommended that you perform a rebuild of your content indices after performing a migration.

Transferring Confluence To Another Server Using a Different Operating System

Migrating from Windows to Linux

You will need to replace the backslash of the following in confluence.cfg.xml with forward slash:

```
<property
name="attachments.dir">${confluenceHome}/attachments</propert
y>
    <property
name="lucene.index.dir">${confluenceHome}/index</property>
    <property
name="webwork.multipart.saveDir">${confluenceHome}/temp</prop
erty>
```

Using database tools (preferred option)

If you are using the Production backup strategy, follow these steps:

1. Download the proper distribution (**the same one you have from your original instance**) from the Download Archive.
2. Copy your Confluence *home* (not install) directory from your original server (even if it was a different OS).
3. If you are changing the location of the home directory, open the Confluence install\confluence\WEB-INF\classes directory and edit confluence-init.properties by changing the line starting with 'confluence.home='.
4. For external databases stored locally, on the original server, create a manual database backup using a native db dump backup tool.
5. Copy the database backup to the new server.
6. On the new server, install or upgrade the database version to match the original server.
7. Import the database backup.
8. Add a database user account with the same username and password as the original.
9. Provide the user with the full access to the imported database.
10. Use a database administration tool to confirm that the user can login from the localhost.
11. To modify any database connection information, go to the Confluence home directory and edit confluence.cfg.xml. The connection URL is set under hibernate.connection.url. **Ensure it does not point to your production database server.**
12. If you are using internal user management, skip this step. For users who have JIRA or LDAP integration, provide the new server with network or local access to the same hosts as the original.
13. Copy server.xml, atlassian-user.xml, osuser.xml, any patches, and any other customized files velocity or properties files. If you are using internal user management, skip this step. For users who have JIRA or LDAP integration, provide the new server with network or local access to the same hosts as the original. If this is a true test instance, set up a test of your JIRA instance or LDAP server so as not to disrupt production systems and change the server.xml or atlassian-user.xml files to point to the appropriate test servers. Note that it might be acceptable to use a production connection here, as users won't be logging on to the test system in high volume.
14. If appropriate, make sure no emails are sent out from the test system.
15. Start Confluence.
16. Go to **Administration > License Details** and add your development license key. You can generate one at http://my.atlassian.com. There are more details in Getting a License for a Staging Environment.

17. If you configured Confluence as a Windows service, repeat those instructions.
18. Add your development license key.
19. Some customers have experienced problems with Confluence's search functions after performing a migration, or that the content of their `{recently-updated}` macro is not being updated correctly. Errors in the `atlassian-confluence.log` file corroborate such problems. Hence, to avoid these issues, it is strongly recommended that you perform a rebuild of your content indices after performing a migration.

Using XML data backups (only for small to medium sized installations)

If you're not yet using the Production backup strategy, you can migrate Confluence to a different server machine by creating an XML data backup as usual, and then importing that to Confluence on the new server.

1. Create an XML data backup from Confluence as follows:
    a. Choose **Browse** > **Confluence Admin**.
    b. Select **Backup & Restore**.
    c. Check the **Backup Attachments** option and click **Backup**.
2. Identify the version of Confluence that you are currently using. This is displayed at the bottom of each Confluence page.
3. Download Confluence to the new server. Get the version of Confluence that you identified above, but for the operating system of the new server. You may be using either the latest Confluence version, or an older version.
4. Install Confluence on the new server.
5. Go to **Administration** > **License Details** and add your development license key. You can generate a license at http://my.atlassian.com. You can find more details in Getting a License for a Staging Environment.
6. Restore your XML data backup from **Administration** > **Backup and Restore**.
7. If appropriate, make sure that no email contact can be made with the test system.
8. Some customers have experienced problems with Confluence's search functions after performing a migration, or that the content of their `{recently-updated}` macro is not being updated correctly. Errors in the `atlassian-confluence.log` file corroborate such problems. Hence, to avoid these issues, it is strongly recommended that you rebuild your content indices after performing a migration.

Ensuring no contact with production systems

To ensure no contact with external systems, you will need to disable both inbound and outbound mail services.

1. Disable global outbound mail by running the following database query:

```
SELECT * FROM BANDANA WHERE BANDANAKEY =
'atlassian.confluence.smtp.mail.accounts';
```

2. Disable space-level mail archiving by running the following database query:

```
SELECT * FROM BANDANA WHERE BANDANAKEY =
'atlassian.confluence.space.mailaccounts';
```

Change 'SELECT' to 'DELETE' in the above queries once you are sure you want to remove the specified accounts.

Once this is done, you can start your test instance without any mails being sent or retrieved. Think carefully about other plugins which may access production systems (SQL macro, JIRA macro, etc.). If these write content, or create unwanted load on external systems, they should be disabled promptly after starting the test instance.

Blog post on Moving Confluence from Windows to Linux

Ricky Sheaves (calebscreek) has written an interesting blog post on Moving Confluence from Windows to (Ubuntu) Linux.

Merging instances

If you wish to merge two instances, you can consider using the remote import plugin. This plugin is currently unsupported. The supported method would be to export a space and then import each space one by one. The two instances of Confluence must be the same version.

Migrating from HTTPS to HTTP

You may want to migrate from a server secured by SSL to one which is not secured by SSL. For example, this may be useful if you are copying a Confluence instance from a production to a test site.

To migrate from HTTPS to HTTP, undo the HTTPS-specific settings that are described on this page: Adding SSL for Secure Logins and Page Security.

Restoring a Site

CAUTION: Restoring a backup of an entire confluence site (consisting of multiple spaces) will:

- Wipe out all Confluence content in the database. Ensure that your database is backed up.
- Log you out after the restore process. Make sure you know your login details contained in the data being restored.

The information on this page does not apply to Confluence OnDemand.

Atlassian suggests establishing the Production Backup Strategy for a production instance of Confluence as confluence xml backups are not recommended for non-evaluation instances.

Confluence supports **backward compatibility** for site backups. (But **not** for space backups). You can only successfully restore backups of a site from an older version of Confluence to a newer version of Confluence. For example, if you create a site backup in Confluence 2.4.3, it cannot be restored into a Confluence 2.2.2 instance. It can however, be restored into 2.4.5 or 2.5.x, because 2.4.5 and 2.5.x are newer versions of Confluence.

There are two ways to restore a site from a backup file:

1. Restore a site from the Confluence Setup Wizard: This restores the data into a new instance of Confluence.
2. Restore a site from the Administration Console: This restores data into the current instance of Confluence.

If your daily backup zips cannot be restored for whatever reason, but you have backups of both your database and your Confluence home directory, then it is still possible to restore from these backups.

Selective space restore not possible

You cannot select a single space to restore from the entire site backup when the backup contains more than one space.

RELATED TOPICS

No content found for label(s) restoring-data.

Administrators Guide Home Confluence Documentation Home

Restoring a Space

This page tells you how to import the contents of a Confluence space into another Confluence site, via an XML backup file.

You can export the content of a space, including pages, comments and attachments. The process involves converting the data in the space into XML format. The end product is a zip file that contains XML file(s) and optionally, all the attachments in the space. To transfer this data to another Confluence site, you simply restore this zip file as described below.

Confluence will only allow you to restore a space if there is not already a space by that name on the site. If you already have a space with the identical name, you will need to delete or rename the existing space before restoring the new one.

The information on this page does not apply to Confluence OnDemand.

Cannot restore to a different major Confluence release

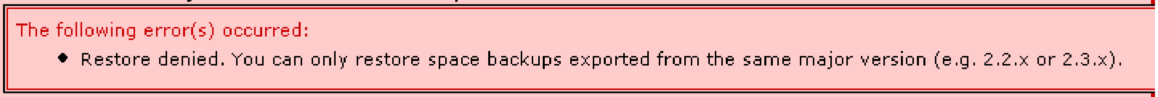
Confluence only supports forward and backward compatibility for space import and export when executed within the **same major version** of Confluence.

Clarifying our terminology: By **major version**, we mean the version defined in the first two sections of the release number. For example, Confluence 2.2 and Confluence 2.3 are different major versions. Confluence 2.2.1 and Confluence 2.2.6 are the same major version.

Restoration Data Must Share the Same Major Version Number
This means that a space export created in one major version of Confluence cannot be imported into a different major version of Confluence. For example, if you create a space export in Confluence 2.3.5, it cannot be imported into a Confluence 2.2.2 site. It can be however imported into 2.3.6. Similarly, a space export created in 2.2.2 can not be imported into 2.3.5. However, it can be restored into a Confluence 2.2.6 site.

If you try to carry out such an operation, an error message similar to the one below will be displayed and the import action will be stopped.

Screenshot: Major Version Clash on Space Restore



The following error(s) occurred:

- Restore denied. You can only restore space backups exported from the same major version (e.g. 2.2.x or 2.3.x).

Workaround for restoring Spaces between Major Releases

You'll need to set up a test server, download and install the same version of confluence as the version you exported the space from, then import the space into this test server. Next upgrade Confluence on your test installation to the right major version so that you can perform the export and import this space into your production confluence successfully. Otherwise, you can try to Change the version of the space export, but please try this on a test site as well.

You need to have System Administrator permissions in order to perform this function.

To restore a space,

1. Choose **Browse** > **Confluence Admin**.
2. Select '**Backup and Restore**' in the 'Administration' section of the left-hand panel.

You can restore data in one of two ways:

1. **Upload a zipped backup to Confluence:**
   - Browse for the backup file.
   - Uncheck '**Build Index**' if you want to create the index at a later stage.
   - Click '**Upload and Restore**'.
2. **Restore a backup from the file system:**
   - Select the backup file from the form field displayed. If you do not see your backup file, make you sure that it has been copied into the `/opt/java/src/confluence/deployments/conf.atlassian.com/home/restore` directory.
   - Uncheck '**Build Index**' if you want to create the index at a later stage.
   - Click '**Restore**'.

RELATED TOPICS

No content found for label(s) restoring-data.

Administrators Guide Home Confluence Documentation Home

Changing the version of a space backup

Confluence prevents the import of space backups which aren't from the same major version. The reason for this is that any schema change between the export and imported version of Confluence will cause the import to fail, leaving you with an incomplete import. Even worse, the failure can be database-dependent, so it may work fine on one particular database but your backup will fail to import later.

Do not import a modified space backup on a production server. Import the modified space backup on a test server, then export from the test server to create a pristine space backup for the new version.

The information on this page does not apply to Confluence OnDemand.

To change the version of a space backup, do the following:

- extract the space backup ZIP file
- edit `exportDescriptor.properties` in a text editor
- change the buildNumber to the buildNumber of the Confluence version you wish to import into
- zip up the modified contents of the backup into a ZIP file again.

This will allow you to import a backup into a test instance of Confluence. After checking the imported space for errors, export it cleanly from the test server and import the fresh backup into your production server.

If your import fails on the test server due to Hibernate errors, this indicates a schema incompatibility and cannot be worked around. You will need to restore your entire site on an old version of Confluence, and export the space from there. See the last section of Restoring a Space for details.

Restoring a Test Instance from Production

See Migrating Confluence Between Servers for a more comprehensive explanation.

Many Confluence administrators will have a production instance running the "live" version of Confluence, as well as a test instance for testing upgrades and so on. In this situation, it's quite common that the two instances are running different versions of Confluence. This document describes how to copy the data from a production instance to a test instance, where the production version may be different to the test version.

Before proceeding with this guide, ensure you have read and understood the normal procedure for upgrading Confluence.

⚠ *The information on this page does not apply to Confluence OnDemand.*

Upgrading a test Confluence instance with production data

Essentially, we are copying both the production home directory and database to the test instance. We then update the database details on the test instance to point to the test database, leaving all other instance metadata (most importantly the Confluence *build number*) the same as production.

1. Shut down your test instance.
2. Restore the production database to the test database server.
3. Create a backup of the `confluence.cfg.xml` file found in the home directory of the test instance.
4. Copy the production confluence-home directory to the test application server.
5. Open the `confluence.cfg.xml` which has been copied in a text editor. Change the database settings to match the test database server. **Ensure you do not point to your production database.** (You can compare with the backup you made in Step 3 if you need to get the database settings. Don't just copy this file – you need the build number unchanged from production to indicate the database is from an older version of Confluence.)

Before starting your test instance, you need to do the following steps to ensure no contact with production systems.

Ensuring no contact with production systems

To ensure no contact with external systems, you will need to disable both inbound and outbound mail services.

1. Disable global outbound mail by running the following database query:

```
SELECT * FROM BANDANA WHERE BANDANAKEY =
'atlassian.confluence.smtp.mail.accounts';
```

2. Disable space-level mail archiving by running the following database query:

```
SELECT * FROM BANDANA WHERE BANDANAKEY =
'atlassian.confluence.space.mailaccounts';
```

Change the 'SELECT *' to a 'DELETE' in the above queries once you are sure you want to remove the specified accounts.

Once this is done, you can start your test instance without any mails being sent or retrieved. Think carefully about other plugins which may access production systems (SQL macro, etc.). These should be disabled promptly after starting the test instance.

You can create a developer license for this server and update the License Details after starting up.

See also

Upgrading Confluence
Migrating Confluence Between Servers
Restoring to a Test Instance of Confluence from Production

Restoring Data from other Backups

Typically, Confluence data is restored from the Administration Console or from the Confluence Setup Wizard.

If you are experiencing problems restoring from an zipped XML backup file, it is still possible to restore provided you have:

1. A backup of your home directory.
2. A backup of your database (if you're using an external database).

Instructions for this method of restoring differ depending on whether you are using the embedded database or an external database (like Oracle, MS SQL Server, MySQL or Postgres).

> *The information on this page does not apply to Confluence OnDemand.*

Embedded Database

If you are running against the embedded database, the database is located inside the `database` folder of your Confluence Home Directory. Hence, all you need to do is:

1. Retrieve the most recent backup of your home directory.
2. Unpack the Confluence distribution and point the `confluence-init.properties` file to this directory.

External Database

If you're using an external database, you need to do the following.

1. Prepare backups of your home directory and database (preferably backups that are dated the same). That is, make sure the home directory is accessible on the filesystem and the database available to be connected to.
2. If this database happens to have a different name, or is on a different server, you need to modify the jdbc url in the `confluence.cfg.xml` file inside the Confluence Home Directory. The value of this property is specified as `hibernate.connection.url`.
3. Unpack the Confluence distribution and point the `confluence-init.properties` file to the home directory.

RELATED TOPICS

Important Directories and Files
Migrating to a Different Database

Administrators Guide Home Confluence Documentation Home

Restoring Data from the Administration Console

Use this option if you want to restore data into your current instance of Confluence. If you want to restore data into a new instance, follow the instructions here.

You need to have System Administrator permissions in order to perform this function.

CAUTION: Restoring a backup of an entire Confluence site (consisting of multiple spaces) will do the following:

- Wipe out all Confluence content in the database. Ensure that your database is backed up.
- Log you out after the restore process. Make sure you know your login details contained in the data being restored.

⚠ *The information on this page does not apply to Confluence OnDemand.*

To restore data from backup,

- Choose **Browse** > **Confluence Admin**.
- Select '**Backup and Restore**' in the 'Administration' section of the left-hand panel.

You can restore data in one of two ways:

1. **Upload a zipped backup to Confluence:**
   - Browse for the backup file.
   - Uncheck '**Build Index**' if you want to create the index at a later stage.
   - Click '**Upload and Restore**'.
2. **Restore a backup from the file system:**
   - Select the backup file from the form field displayed. If you do not see your backup file, make sure that it has been copied into the `/opt/java/src/confluence/deployments/conf.atlassian.com/home/restore` directory.
   - Uncheck '**Build Index**' if you want to create the index at a later stage.
   - Click '**Restore**'.

RELATED TOPICS

No content found for label(s) restoring-data.

Administrators Guide Home Confluence Documentation Home

Retrieve file attachments from a backup

File attachments on pages can be retrieved from a backup without needing to import the backup into Confluence. This is useful for recovering attachments that have been deleted by users.

Both automated and manual backups allow this, as long as the 'Include attachments' property was set. Users wanting to restore pages, spaces or sites should check out the Confluence Administrator's Guide instead.

Before following the instructions for recovering attachments, please review how backups store file and page information.

⚠ *The information on this page does not apply to Confluence OnDemand.*

How Backups Store File and Page Information

The backup zip file contains entities.xml, an XML file containing the Confluence content, and a directory for storing attachments.

Backup Zip File Structure

Page attachments are stored under the attachments directory by page and attachment id. Here is an example listing:

```
Listing for test-2006033012_00_00.zip
\attachments\98\10001
\attachments\98\10002
\attachments\99\10001
entities.xml
```

Inside the attachment directory, each numbered directory inside is one page, and the numbered file inside is one attachment. The directory number is the page id, and the file number is the attachment id. For example, the file \attachments\98\10001 is an attachment with page id 98 and attachment id 10001. You can read entities.xml to link those numbers to the original filename. Entities.xml also links each page id to the page title.

Entities.xml Attachment Object

Inside the entities.xml is an Attachment object written in XML. In this example, the page id is 98, the attachment id is 10001 and the filename is myimportantfile.doc. The rest of the XML can be ignored:

```
<object class="Attachment"
package="com.atlassian.confluence.pages">
<id name="id">98</id>
<property
name="fileName"><![CDATA[myimportantfile.d
oc]]></property>
...
<property name="content" class="Page"
package="com.atlassian.confluence.pages"><
id name="id">10001</id>
</property>
...
</object>
```

Entities.xml Page Object

This XML describes a page. In this example, the page id is 98 and the title is Editing Your Files. The rest of the XML can be ignored:

```
<object class="Page"
package="com.atlassian.confluence.pages">
<id name="id">98</id>
<property name="title"><![CDATA[Editing
Your Files]]></property>
...
</object>
```

Instructions for Recovering Attachments

Each file must be individually renamed and re-uploaded back into Confluence by following the instructions below. Choose one of the three methods:

Choice A - Recover Attachments By Filename

Best if you know each filename you need to restore, especially if you want just a few files:

1. Unzip the backup directory and open entities.xml.
2. Search entities.xml for the filename and find the attachment object with that filename. Locate its page and attachment id.
3. Using the page and attachment id from entities.xml, go to the attachments directory and open that directory with that page id. Locate the file with the attachment id.
4. Rename the file to the original filename and test it.
5. Repeat for each file.
6. To import each file back into Confluence, upload to the original page by attaching the file from within Confluence.

Choice B - Restore Files By Page

Best if you only want to restore attachments for certain pages:

1. Unzip the backup directory and open entities.xml.
2. Search entities.xml for the page title and find the page object with that title. Locate its page id.
3. Go to the attachments directory and open that directory with that page id. Each of the files in the directory is an attachment that must be renamed.
4. Search entities.xml for attachment objects with that page id. Every attachment object for the page will have an attachment id and filename.
5. Rename the file with that attachment id to the original filename and test it.
6. Repeat for each page.
7. To import each file back into Confluence, upload to the original page by attaching the file from within Confluence.

Choice C - Restore All Files

Best if you have a small backup but want to restore many or all the attachments inside:

⛔ Following process is applicable to **space** export only. Site xml backups do not require page id to be updated manually due to the nature of persistent page_id's.

1. Unzip the backup directory and open entities.xml.
2. Go to the attachments directory and open any directory. The directory name is a page id. Each of the files in the directory is an attachment that must be renamed.
3. Search entities.xml for attachment objects with that page id. When one is found, locate the attachment id and filename.
4. Rename the file with that attachment id to the original filename and test it.
5. Find the next attachment id and rename it. Repeat for each file in the directory.
6. Once all files in the current directory are renamed to their original filenames, search entities.xml for the page id, eg directory name. Find the page object with that page id and locate its page title.
7. Rename the directory to the page title and move on to the next directory. Repeat for each un-renamed directory in the attachments directory.
8. To import each file back into Confluence, upload to the original page by attaching the file from within Confluence.

⚠ To obtain detailed information about lost attachments, **location**, **name** and **type** of the attachments, you may use the findattachments script

Troubleshooting failed XML site backups

⚠ XML site backups are only necessary for migrating to a new database. Setting up a test server or Establishing a reliable backup strategy is better done with an SQL dump.

Seeing an error when creating or importing a backup?

Problem	Solution
Exception while creating backup	Follow instructions below
Exception while importing backup	Follow Troubleshooting XML backups that fail on restore instead

⚠ *The information on this page does not apply to Confluence OnDemand.*

Resolve Errors With Creating An XML Backup

The errors may be caused by a slightly corrupt database. If you're seeing errors such as 'Couldn't backup database data' in your logs, this guide will help you correct the error on your own. We strongly recommend that you backup your database and your Confluence home directory beforehand, so that you can restore your site from those if required. If you are unfamiliar with SQL, we suggest you contact your database administrator for assistance.

Preferable solution

The Production Backup Strategy is a very reliable and more efficient way to do backups. If you are running into problems with XML backups - whether memory related or because of problems like the one described here - use the native backup tool as an alternate solution.

To Identify And Correct The Problem

To work out where the data corruption or problems are, increase the status information reported during backup, then edit the invalid database entry:

1. Stop Confluence.
2. If you have an external database, use a database administration tool to create a manual database backup.
3. Backup your Confluence home directory. You will be able to restore your whole site using this and the database backup.
4. Open the `my_confluence_install/confluence/WEB-INF/classes/log4j.properties`and add this to the bottom and save:

```
log4j.logger.com.atlassian.confluence.importexport.impl.XMLDatabinder=D
EBUG, confluencelog
log4j.additivity.com.atlassian.confluence.importexport.impl.XMLDatabind
er=false
```

5. Find your atlassian-confluence.log. Move or delete all existing Confluence logs to make it easier to find the relevant logging output.
6. Restart Confluence and login.
7. Begin a backup so that the error reoccurs.
8. You must now check your log files to find out what object could not be converted into XML format. Open `confluence-home/logs/atlassian-confluence.log`. Scroll to the bottom of the file.
9. Do a search for 'ObjectNotFoundException'. You should see an error similar to this:

```
2005-08-24 00:00:33,743 DEBUG [DOCPRIV2:confluence.importexport.impl.XMLDatabinder] Writing object: com.atlassian.confluence.core.ContentPermission with ID: 5 to XML.
2005-08-24 00:00:33,743 DEBUG [DOCPRIV2:confluence.importexport.impl.XMLDatabinder] Writing property: type
2005-08-24 00:00:33,743 DEBUG [DOCPRIV2:confluence.importexport.impl.XMLDatabinder] Writing property: group
2005-08-24 00:00:33,743 DEBUG [DOCPRIV2:confluence.importexport.impl.XMLDatabinder] Writing property: expiry
2005-08-24 00:00:33,743 DEBUG [DOCPRIV2:confluence.importexport.impl.XMLDatabinder] Writing property: content
[DOCPRIV2:ERROR] LazyInitializer - Exception initializing proxy <net.sf.hibernate.ObjectNotFoundException: No row with the given identifier exists: 2535,
of class: com.atlassian.confluence.core.ContentEntityObject>net.sf.hibernate.ObjectNotFoundException:
No row with the given identifier exists: 2535, of class: com.atlassian.confluence.core.ContentEntityObject
at net.sf.hibernate.ObjectNotFoundException.throwIfNull(ObjectNotFoundException.java:24)
at net.sf.hibernate.impl.SessionImpl.immediateLoad(SessionImpl.java:1946)
at net.sf.hibernate.proxy.LazyInitializer.initialize(LazyInitializer.java:53)
at net.sf.hibernate.proxy.LazyInitializer.initializeWrapExceptions(LazyInitializer.java:60)
at net.sf.hibernate.proxy.LazyInitializer.getImplementation(LazyInitializer.java:164)
at net.sf.hibernate.proxy.CGLIBLazyInitializer.intercept(CGLIBLazyInitializer.java:108)
at com.atlassian.confluence.core.ContentEntityObject$$EnhancerByCGLIB$$cc2f5557.hashCode(<generated>)
at java.util.HashMap.hash(HashMap.java:261)
at java.util.HashMap.containsKey(HashMap.java:339)
at com.atlassian.confluence.importexport.impl.XMLDatabinder.toGenericXML(XMLDatabinder.java:155)
```

10. Open a DBA tool such as DbVisualizer and connect to your database instance. Scan the table names in the schema. You will have to modify a row in one of these tables.
11. To work out which table, open `catalina.out`, check the first line of the exception. This says there was an error writing the `ContentPermission` object with id 5 into XML. This translates as *the row with primary key 5 in the CONTENTLOCK table*needs fixing. To work out what table an object maps to in the database, here's a rough guide:

- Pages, blogposts, comments --> CONTENT table
- attachments --> ATTACHMENTS table
- More information can be found in the schema documentation

12. Now you must find the primary key of the incorrect row in this table. In this case, you can check the first line and see that the row has a primary key of 5.
13. Each property is written to a column, so the last property that was being written has the incorrect value. The row being written to when the exception was thrown was `CONTENT` (line 5) with a value of `2535` (line 6). Now you know the column and value. This value `2535` is the id of an entry that no longer exists.
14. Using a database administrative tool, login ot the Confluence database. Locate the row in the relevant table and correct the entry. Check other rows in the table for the default column value, which may be null, 0 or blank. Overwrite the invalid row value with the default.
15. Restart Confluence.
16. Attempt the backup again. If the backup fails and you are stuck, please lodge a support request with your latest logs.

Troubleshooting "Duplicate Key" related problems

If you are encountering an error message such as:

```
could not insert:
[bucket.user.propertyset.BucketPropertySet
Item#bucket.user.propertyset.BucketPropert
ySetItem@a70067d3]; SQL []; Violation of
PRIMARY KEY constraint
'PK_OS_PROPERTYENTRY314D4EA8'. Cannot
insert duplicate key in object
'OS_PROPERTYENTRY'.; nested exception is
java.sql.SQLException: Violation of
PRIMARY KEY constraint
'PKOS_PROPERTYENTRY_314D4EA8'. Cannot
insert duplicate key in object
'OS_PROPERTYENTRY'.
```

this indicates that the Primary Key constraint 'PK_OS_PROPERTYENTRY_314D4EA8' has duplicate entries in table 'OS_PROPERTYENTRY'.
You can locate the constraint key referring to 'PK_OS_PROPERTYENTRY_314D4EA8' in your table 'OS_PROPERTYENTRY' and locate any duplicate values in it and remove them, to ensure the "PRIMARY KEY" remains unique. An example query to list duplicate entries in the 'OS_PROPERTYENTRY' table is:

```
SELECT
ENTITY_NAME,ENTITY_ID,ENTITY_KEY,COUNT(*)
FROM OS_PROPERTYENTRY GROUP BY
ENTITY_NAME,ENTITY_ID,ENTITY_KEY HAVING
COUNT(*)>1
```

To Help Prevent This Issue From Reoccuring

1. If you are using the embedded database, be aware that it is bundled for evaluation purposes and does not offer full transactional integrity in the event of sudden power loss, which is why an external database is recommended for production use. You should migrate to an external database.
2. If you are using an older version of Confluence than the latest, you should consider upgrading at this point.

RELATED TOPICS

Enabling detailed SQL logging

Administrators Guide Home   Confluence Documentation Home

Troubleshooting XML backups that fail on restore

⚠ XML site backups are only necessary for migrating to a new database. Upgrading Confluence, Setting up a test server or Production Backup Strategy is better done with an SQL dump.

ℹ If migrating from HSQLDB to MySQL, you might have a better experience using the MySQL Migration Toolkit.

Seeing an error when creating or importing a site or space backup?

Problem	Solution
Exception while creating backup	Follow Troubleshooting failed XML site backups instead
Exception while importing backup	Follow instructions below

⚠ *The information on this page does not apply to Confluence OnDemand.*

Resolve Errors When Attempting To Restore An XML Backup

The errors may be caused by a slightly corrupt database. You will need to find the XML backup file entry that is violating the DB rules, modify the entry and recreate the XML backup:

1. On the instance being restored, follow the instructions to disable batched updates (for simpler debugging), log SQL queries and log SQL queries **with parameters** at Enabling Detailed SQL Logging.

2. Once all three changes have been made, restart Confluence.
3. Attempt another restore.
4. Once the restore fails, check your log files to find out what object could not be converted into XML format. For Confluence distribution users, check your Confluence install directory under the `/logs/` and check both `atlassian-confluence.log` and `catalina.out` file. The correct file will contain SQL debug output.
5. Scroll to the bottom of the file and identify the last error relating to a violation of the database constraint. For example:

   ```
   2006-07-13 09:32:33,372 ERROR
   [confluence.importexport.impl.ReverseDatabinder] endElement
   net.sf.hibernate.exception.ConstraintViolationException:
     could not insert: [com.atlassian.confluence.pages.Attachment#38]
   net.sf.hibernate.exception.ConstraintViolationException: could not
   insert: [com.atlassian.confluence.pages.Attachment#38]
   ...
   Caused by: java.sql.SQLException: ORA-01400: cannot insert NULL into
   ("CONFUSER"."ATTACHMENTS"."TITLE")
   at
   oracle.jdbc.driver.DatabaseError.throwSqlException(DatabaseError.java:1
   12)
   at oracle.jdbc.driver.T4CTTIoer.processError(T4CTTIoer.java:331)
   at oracle.jdbc.driver.T4CTTIoer.processError(T4CTTIoer.java:288)
   ```

   This example indicates a row in your attachment table with ID = 38 that has a null title.

6. Go to the server that the backup was created on. You must have a copy of the database from which the backup was created. If you do not have this, use a DBA tool to restore a manual backup of the database.
7. Open a DBA tool and connect to the original database instance and scan the table names in the schema. You will have to modify a row in one of these tables.
8. To work out which table, open `catalina.out`, check the first line of the exception. To work out what table an object maps to in the database, here's a rough guide:
   - Pages, blogposts, comments --> CONTENT table.
   - attachments --> ATTACHMENTS table.
9. To correct the example error, go to the attachment table and find that attachment object with id 38. This will have a a null title. Give a title using the other attachments titles as a guide. You may have a different error and should modify the database accordingly.
10. Once the entry has been corrected, create the XML backup again.
11. Import the backup into the new version.
12. If the import succeeds, revert the changes made in your SQL logging to re-enable disable batched updates and turn off log SQL queries and log SQL queries with parameters.
13. Restart Confluence.

Troubleshooting "Duplicate Entry" for key "cp_" or "cps_"

If you are encountering an error message such as:

```
com.atlassian.confluence.importexport.ImportExportException: Unable to complete import because the data does not match the constraints in the Confluence schema. Cause: MySQLIntegrityConstraintViolationException: Duplicate entry '1475804-Edit' for key 'cps_unique_type'
```

This indicates that the XML export came from a version of Confluence with a corrupt permissions database, caused by some 3rd party plugin. This is an issue that was fixed when CONF-22123 was implemented in Confluence 3.5.2. The simplest workaround is to export the space again after upgrading the instance to 3.5.2 or above. If that is not an option, then either the export will need to be edited manually to remove the duplicate permission entries or the source instance will need to have the offending entries removed. The following SQL queries can be used to look for such entries:

```
SELECT * FROM CONTENT_PERM WHERE USERNAME
IS NULL AND GROUPNAME IS NULL;

SELECT cp.ID, cp.CP_TYPE, cp.USERNAME,
cp.GROUPNAME, cp.CPS_ID, cp.CREATOR,
cp.CREATIONDATE, cp.LASTMODIFIER,
cp.LASTMODDATE
FROM CONTENT_PERM cp
WHERE cp.USERNAME IS NOT NULL AND
cp.GROUPNAME IS NOT NULL;

SELECT cps1.ID, cps1.CONTENT_ID,
cps1.CONT_PERM_TYPE FROM CONTENT_PERM_SET
cps1, CONTENT_PERM_SET cps2
WHERE cps1.ID <> cps2.ID AND
cps1.CONTENT_ID = cps2.CONTENT_ID AND
cps1.CONT_PERM_TYPE = cps2.CONT_PERM_TYPE
ORDER BY cps1.CONTENT_ID,
cps1.CONT_PERM_TYPE, cps1.CREATIONDATE
ASC;

SELECT cp.ID, cp.CP_TYPE, cps.CONTENT_ID,
(SELECT scps.ID FROM CONTENT_PERM_SET scps
WHERE scps.CONTENT_ID = cps.CONTENT_ID AND
scps.CONT_PERM_TYPE = cp.CP_TYPE) AS
suggested_cps_id
FROM CONTENT_PERM cp, CONTENT_PERM_SET cps
WHERE cp.CPS_ID = cps.ID AND
cp.CP_TYPE <> cps.CONT_PERM_TYPE;

SELECT DISTINCT cp1.ID, cp1.CP_TYPE,
cp1.USERNAME, cp1.GROUPNAME, cp1.CPS_ID,
cp1.CREATOR, cp1.CREATIONDATE,
cp1.LASTMODIFIER, cp1.LASTMODDATE
FROM CONTENT_PERM cp1, CONTENT_PERM_SET
cps1, CONTENT_PERM cp2, CONTENT_PERM_SET
cps2
WHERE
cp1.CPS_ID = cps1.ID AND
cp2.CPS_ID = cps2.ID AND
cp1.ID <> cp2.ID AND
cps1.CONTENT_ID = cps2.CONTENT_ID AND
cp1.CP_TYPE = cp2.CP_TYPE AND
cp1.USERNAME = cp2.USERNAME
ORDER BY cp1.CPS_ID, cp1.CP_TYPE,
cp1.USERNAME, cp1.CREATIONDATE;

SELECT DISTINCT cp1.ID, cp1.CP_TYPE,
cp1.USERNAME, cp1.GROUPNAME, cp1.CPS_ID,
cp1.CREATOR, cp1.CREATIONDATE,
cp1.LASTMODIFIER, cp1.LASTMODDATE
```

```
FROM CONTENT_PERM cp1, CONTENT_PERM_SET
cps1, CONTENT_PERM cp2, CONTENT_PERM_SET
cps2
WHERE
cp1.CPS_ID = cps1.ID AND
cp2.CPS_ID = cps2.ID AND
cp1.ID <> cp2.ID AND
cps1.CONTENT_ID = cps2.CONTENT_ID AND
cp1.CP_TYPE = cp2.CP_TYPE AND
cp1.GROUPNAME = cp2.GROUPNAME
ORDER BY cp1.CPS_ID, cp1.CP_TYPE,
cp1.GROUPNAME, cp1.CREATIONDATE;
```

```
SELECT * FROM CONTENT_PERM_SET
WHERE ID NOT IN (SELECT DISTINCT CPS_ID
FROM CONTENT_PERM);
```

Remove all matching entries and perform the export again.

Troubleshooting "Duplicate Key" related problems

If you are encountering an error message such as:

```
could not insert:
[bucket.user.propertyset.BucketPropertySet
Item#bucket.user.propertyset.BucketPropert
ySetItem@a70067d3]; SQL []; Violation of
PRIMARY KEY constraint
'PK_OS_PROPERTYENTRY314D4EA8'. Cannot
insert duplicate key in object
'OS_PROPERTYENTRY'.; nested exception is
java.sql.SQLException: Violation of
PRIMARY KEY constraint
'PKOS_PROPERTYENTRY_314D4EA8'. Cannot
insert duplicate key in object
'OS_PROPERTYENTRY'.
```

This indicates that the Primary Key constraint 'PK_OS_PROPERTYENTRY_314D4EA8' has duplicate entries in table 'OS_PROPERTYENTRY'.
You can locate the constraint key referring to 'PK_OS_PROPERTYENTRY_314D4EA8' in your table 'OS_PROPERTYENTRY' and locate any duplicate values in it and remove them, to ensure the "PRIMARY KEY" remains unique. An example query to list duplicate entries in the 'OS_PROPERTYENTRY' table is:

```
SELECT
ENTITY_NAME,ENTITY_ID,ENTITY_KEY,COUNT(*)
FROM OS_PROPERTYENTRY GROUP BY
ENTITY_NAME,ENTITY_ID,ENTITY_KEY HAVING
COUNT(*)>1
```

Troubleshooting "net.sf.hibernate.PropertyValueException: not-null" related problems

If you're receiving a message like:

```
ERROR [Importing data task]
[confluence.importexport.impl.ReverseDatabinder] endElement
net.sf.hibernate.PropertyValueException:
not-null property references a null or
transient value:
com.atlassian.user.impl.hibernate.DefaultHibernateUser.name
```

This means there's an unexpected null value in a table. In the above example, the error is in the name column in the USERS table. We've also seen them in the ATTACHMENTS table.

Remove the row with the null value, redo the xml export, and reimport.

To Help Prevent this Issue from Recurring

1. If you are using the embedded database, be aware that it is bundled for evaluation purposes and does not offer full transactional integrity in the event of sudden power loss, which is why an external database is recommended for production use. You should migrate to an external database.
2. If you are using an older version of Confluence than the latest, you should consider upgrading at this point.

> ⚠ The problem with different settings for case sensitivity varies between databases. The case sensitivity of the database is usually set through the collation that it uses. Please vote on the existing issue

RELATED TOPICS

Troubleshooting failed XML site backups
Confluence Administrator's Guide

Migrating from HSQLDB to MySQL

> ⚠ If you've gone through Migrate to Another Database and cannot migrate because of a failed xml backup, this page might help.

Disclaimer

MySQL Migration Toolkit is released by the makers of MySQL and as such, problems with the software should be directed to them. Atlassian Support does not offer support for the Migration Toolkit, nor do we provide support for this migration path. These instructions are offered for strictly informational purposes, and your mileage may vary.

Backup Reminder

Please backup your database and your home folder before attempting this.

The information on this page does not apply to Confluence OnDemand.

Resources needed

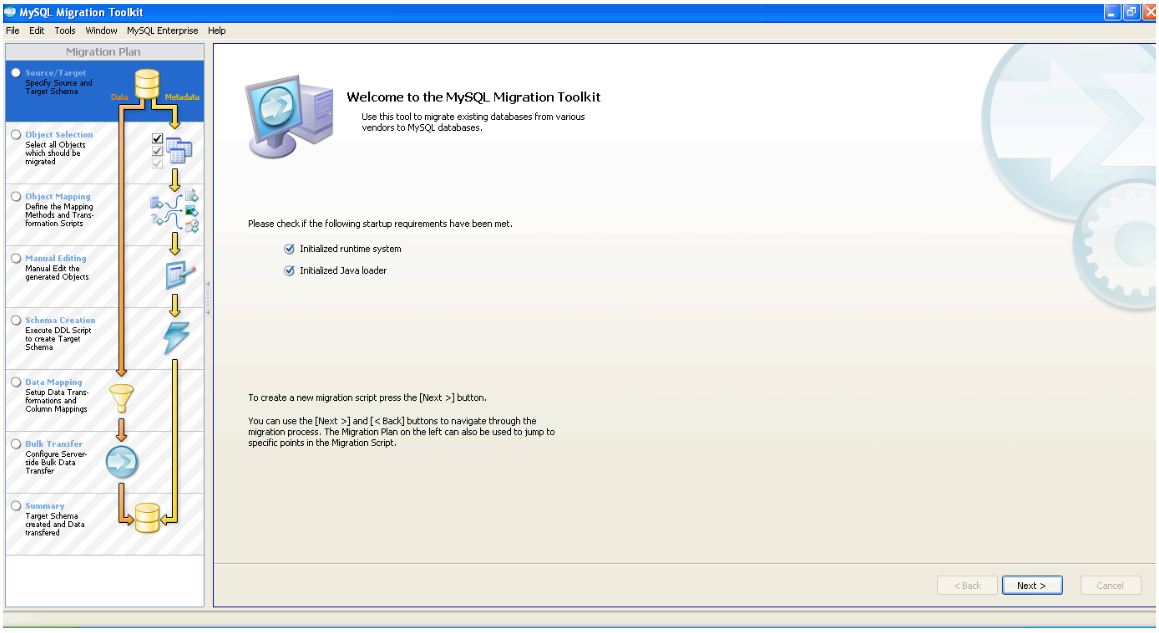
- Empty MySQL DB with appropriate credentials to allow creation, deletion, and insertion of tables and rows.
- A Windows machine that can both communicate to the Confluence server and the destination DB.
- MySQL Migration Toolkit
- HSQL Database Engine

Preparation for migrating to MySQL from HSQLDB

1. Shutdown Confluence
2. Make a copy of the confluence home folder for backup purposes
3. Install the Migration Toolkit
4. Unzip the hsqldb package.
5. Copy the hsqldb.jar from hsqldb/lib into C:\Program Files\MySQL\MySQL Tools for 5.0\java\lib
6. Start the MySQL Migration Toolkit

Running the Migration Toolkit

You should be presented with the following screen.


MySQL Migration Toolkit
File Edit Tools Window MySQL Enterprise Help
Migration Plan
Source/Target
Specify Source and Target Schema
Data
Metadata
Object Selection
Select all Objects which should be migrated
Object Mapping
Define the Mapping Methods and Transformation Scripts
Manual Editing
Manual Edit the generated Objects
Schema Creation
Execute DDL Script to create Target Schema
Data Mapping
Setup Data Transformations and Column Mappings
Bulk Transfer
Configure Server-side Bulk Data Transfer
Summary
Target Schema created and Data transfered
< Back
Next >
Cancel

Welcome to the MySQL Migration Toolkit

Use this tool to migrate existing databases from various vendors to MySQL databases.

Please check if the following startup requirements have been met.

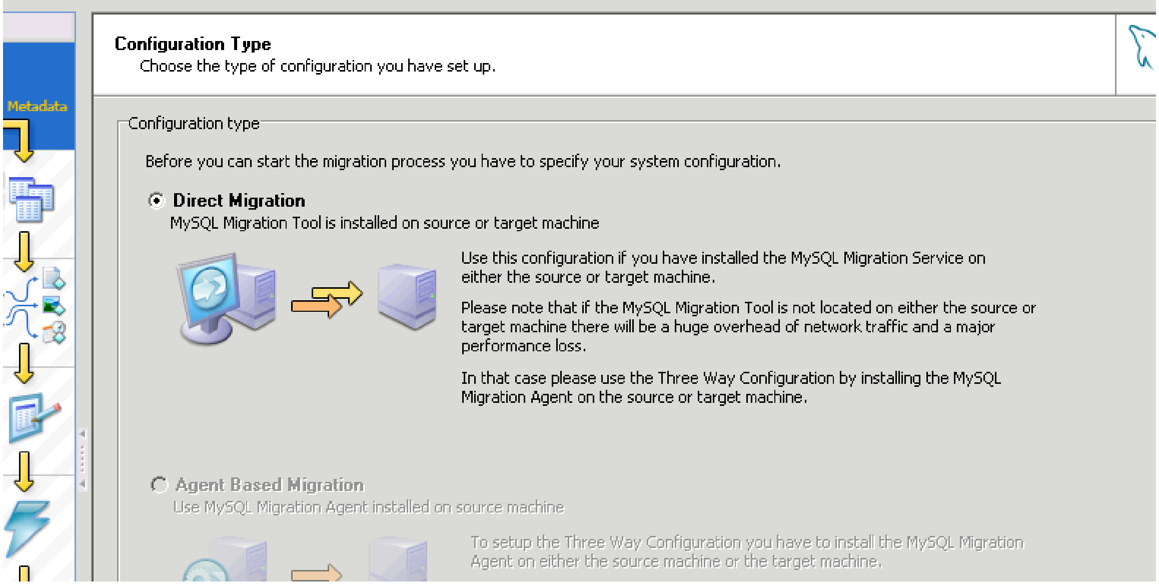
☑ Initialized runtime system

☑ Initialized Java loader

To create a new migration script press the [Next >] button.

You can use the [Next >] and [< Back] buttons to navigate through the migration process. The Migration Plan on the left can also be used to jump to specific points in the Migration Script.

Choose Direct Migration



Configuration Type
Choose the type of configuration you have set up.

Configuration type

Before you can start the migration process you have to specify your system configuration.

● **Direct Migration**
MySQL Migration Tool is installed on source or target machine

Use this configuration if you have installed the MySQL Migration Service on either the source or target machine.

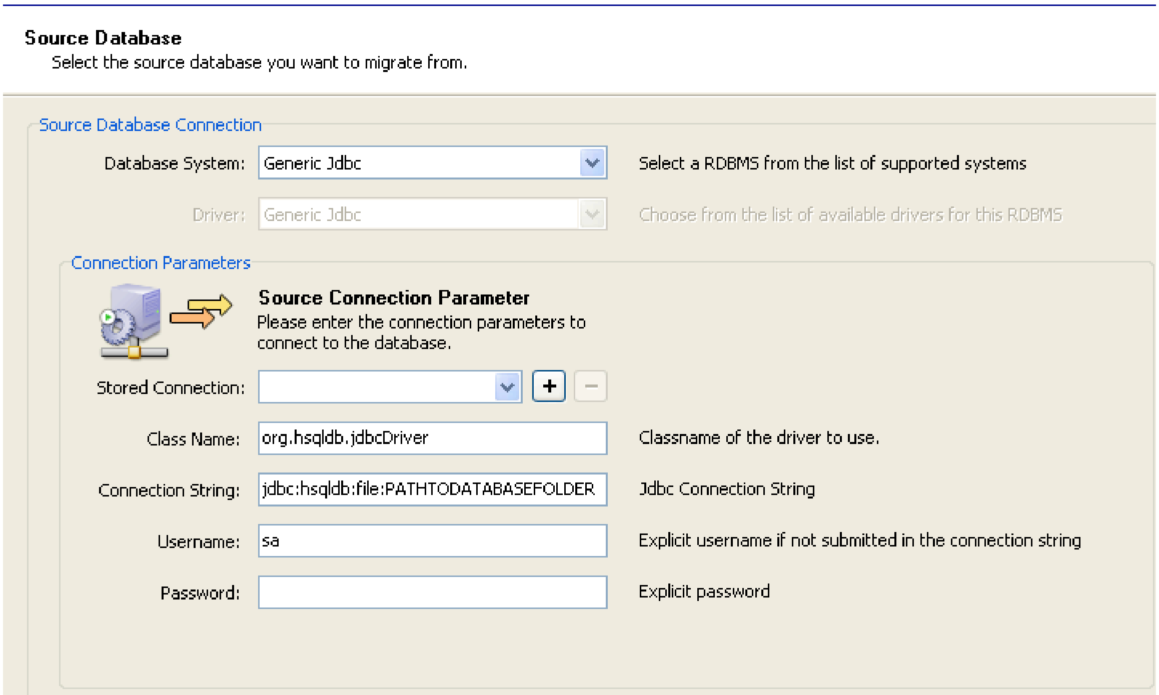
Please note that if the MySQL Migration Tool is not located on either the source or target machine there will be a huge overhead of network traffic and a major performance loss.

In that case please use the Three Way Configuration by installing the MySQL Migration Agent on the source or target machine.

○ **Agent Based Migration**
Use MySQL Migration Agent installed on source machine

To setup the Three Way Configuration you have to install the MySQL Migration Agent on either the source machine or the target machine.

Source Database



Source Database
Select the source database you want to migrate from.

Source Database Connection

Database System: Generic Jdbc — Select a RDBMS from the list of supported systems

Driver: Generic Jdbc — Choose from the list of available drivers for this RDBMS

Connection Parameters

Source Connection Parameter
Please enter the connection parameters to connect to the database.

Stored Connection:

Class Name: org.hsqldb.jdbcDriver — Classname of the driver to use.

Connection String: jdbc:hsqldb:file:PATHTODATABASEFOLDER — Jdbc Connection String

Username: sa — Explicit username if not submitted in the connection string

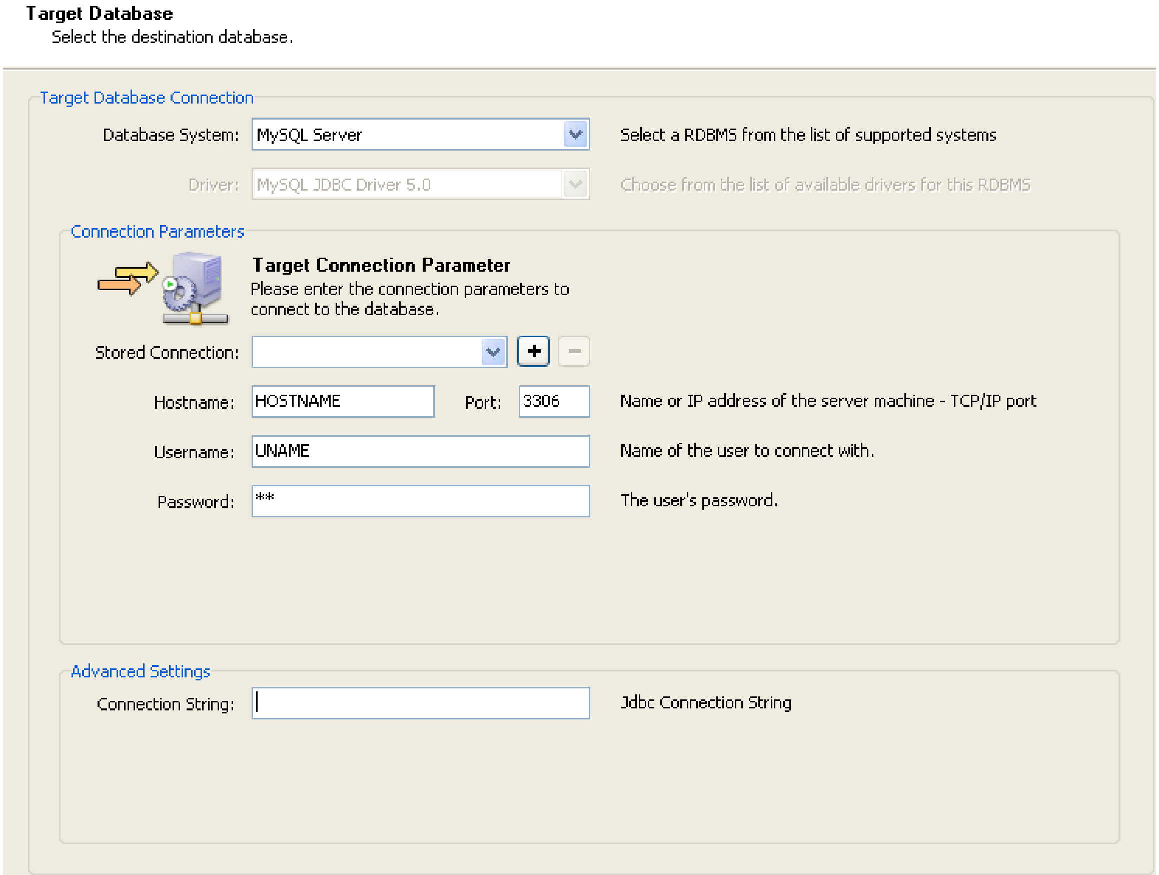
Password: — Explicit password

Database System:	Generic JDBC
Connection String:	jdbc:hsqldb: file:PATHTODATABASEFOLDER\confluencedb\\
Username:	sa
Password:	*No password. Leave this field blank*

Destination Database

Please make sure that the computer that is running MySQL Toolkit is able to access the MySQL server and that the user listed has the ability to create, drop, insert, and update tables.

If your MySQL user has a $ character in the password (such as 'pa$sword'), please change the password or create a temporary account with full permissions. If you do not, the toolkit will throw an "Illegal group reference" error and you will not be able to proceed with the migration.



Target Database
Select the destination database.

Target Database Connection

Database System: MySQL Server — Select a RDBMS from the list of supported systems

Driver: MySQL JDBC Driver 5.0 — Choose from the list of available drivers for this RDBMS

Connection Parameters

Target Connection Parameter
Please enter the connection parameters to connect to the database.

Stored Connection:

Hostname: HOSTNAME Port: 3306 — Name or IP address of the server machine - TCP/IP port

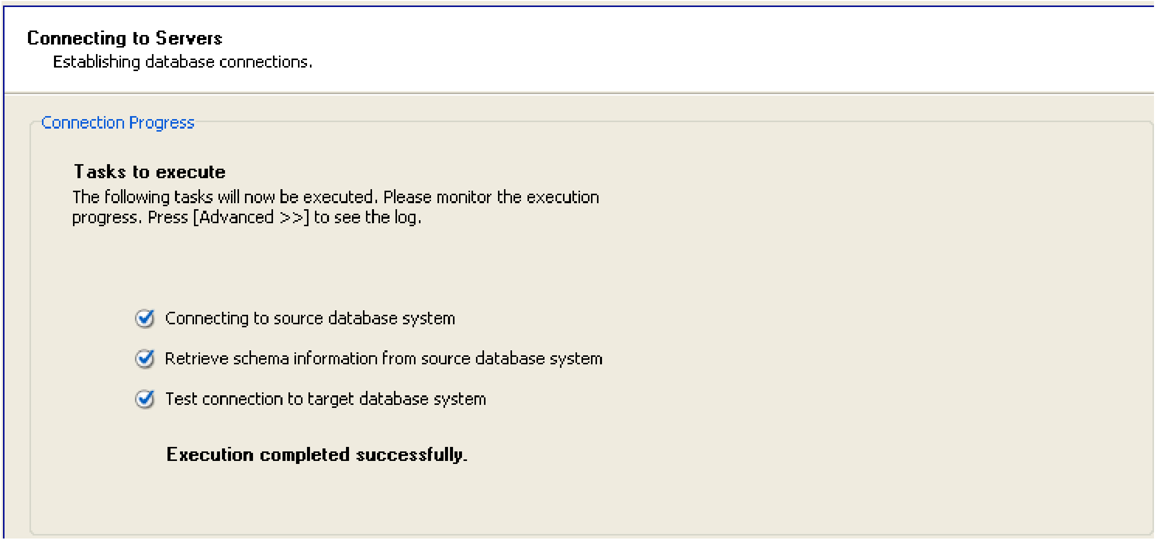
Username: UNAME — Name of the user to connect with.

Password: ** — The user's password.

Advanced Settings

Connection String: — Jdbc Connection String

Connecting to Servers



Connecting to Servers
Establishing database connections.

Connection Progress

Tasks to execute
The following tasks will now be executed. Please monitor the execution progress. Press [Advanced >>] to see the log.

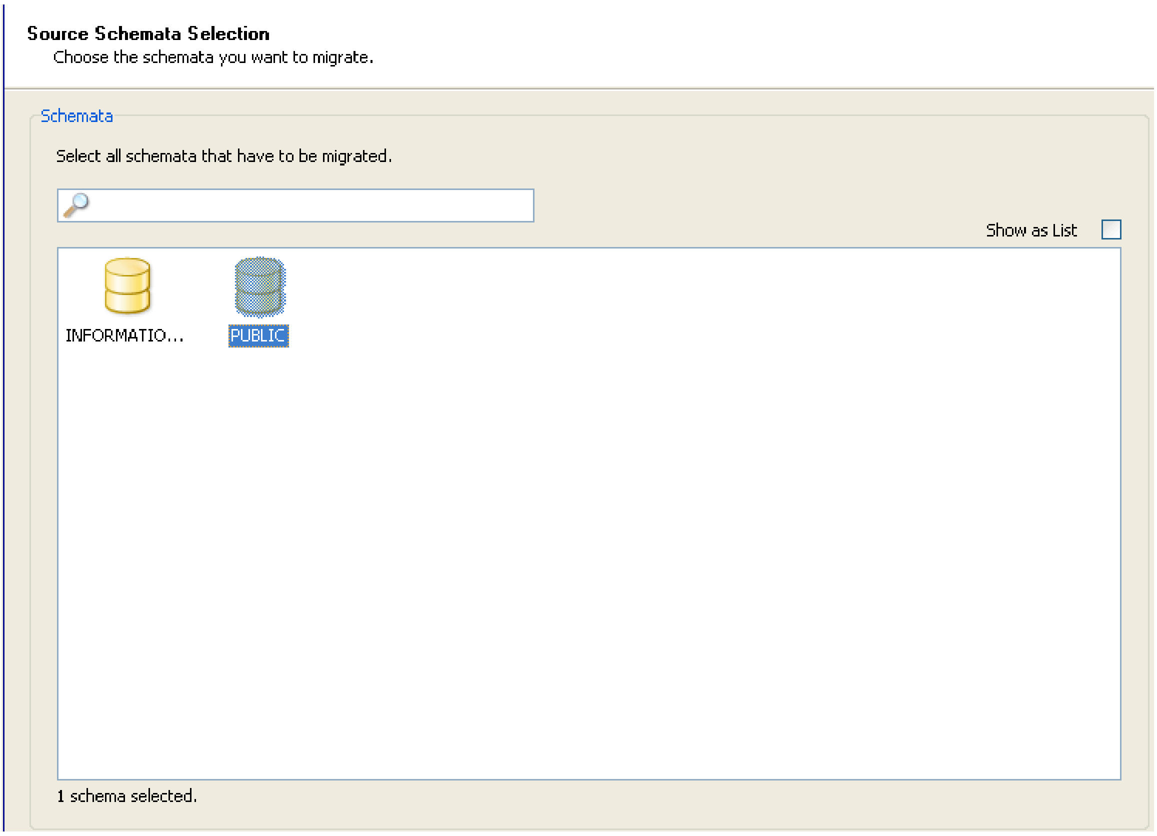
☑ Connecting to source database system
☑ Retrieve schema information from source database system
☑ Test connection to target database system

Execution completed successfully.

You should see the toolkit trying to connect. If you have problems, please click on the advanced options and sql will show you debugging information. Click Advanced to see the log. If you see "Java Heap Space: Out of Memory", you can start the *MySQL Migration Toolkit* with a -Xmx flag to allocate more memory to the JVM.

After this screen you should come to reverse engineering. Click next.

Source Schemata Selection



Source Schemata Selection
Choose the schemata you want to migrate.

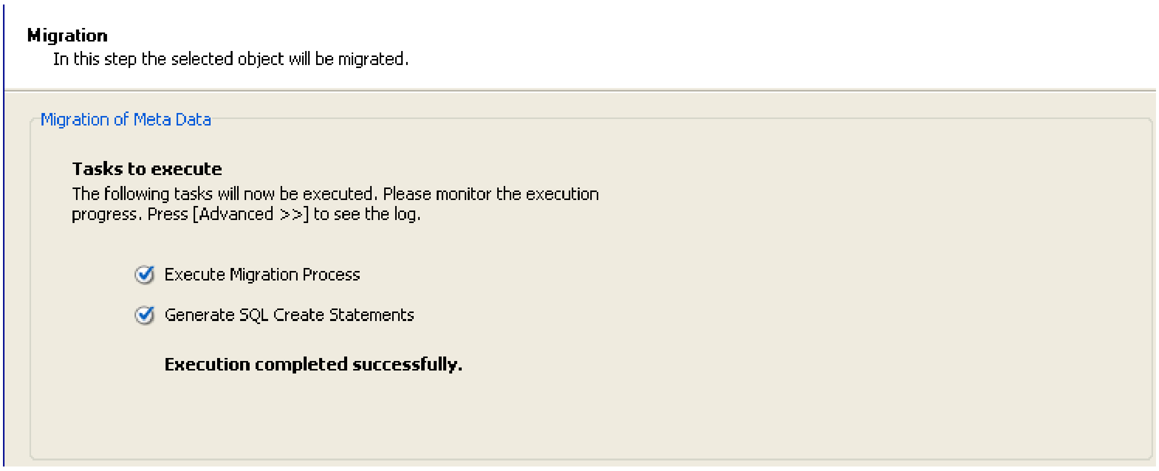
Schemata

Select all schemata that have to be migrated.

1 schema selected.

You should see 2 databases, **INFORMATION_SCHEMA** and **PUBLIC**. Choose **PUBLIC**

Object Type Selection



Migration
In this step the selected object will be migrated.

Migration of Meta Data

Tasks to execute
The following tasks will now be executed. Please monitor the execution progress. Press [Advanced >>] to see the log.

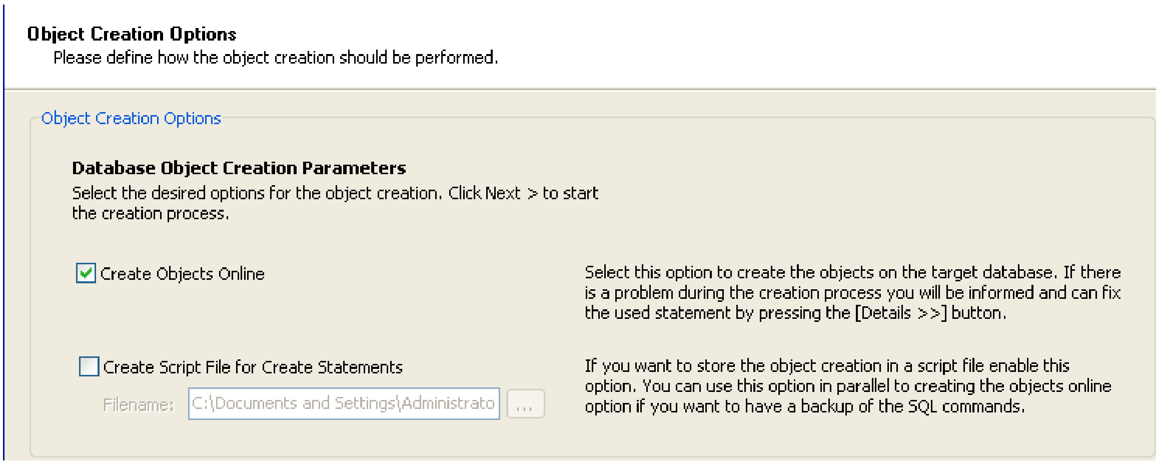
✓ Execute Migration Process

✓ Generate SQL Create Statements

Execution completed successfully.

Click Next.

Object Type Mapping



Object Creation Options
Please define how the object creation should be performed.

Object Creation Options

Database Object Creation Parameters
Select the desired options for the object creation. Click Next > to start the creation process.

☑ Create Objects Online

Select this option to create the objects on the target database. If there is a problem during the creation process you will be informed and can fix the used statement by pressing the [Details >>] button.

☐ Create Script File for Create Statements

Filename: C:\Documents and Settings\Administrato

If you want to store the object creation in a script file enable this option. You can use this option in parallel to creating the objects online option if you want to have a backup of the SQL commands.

Click **Show Details** on both sections. For **Migration Method for Type Schema**, choose **Multilanguage**. For **Mi gration Method for Type Table**, choose **Data Consistancy/Multilanguage**

Click **Advanced**. Check **Enabled Detailed Mappings in Next Step**

Detailed Object Mapping

Click to rename the **destination database** to be the one set aside to migrate to.

From this point on, you should be able to click next all the way through to finish the migration.

Rebuilding the Ancestor Table

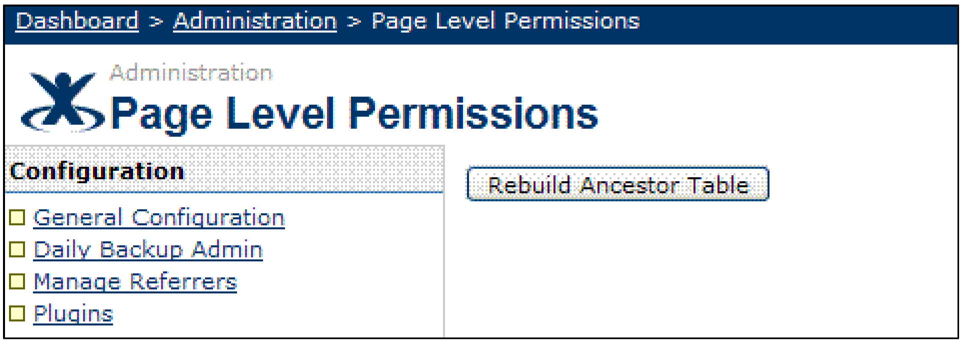
In Confluence, the ancestor table defines what pages are ancestors or descendants of other pages (which can be used by search restrictions with the ancestorids restriction). Occasionally, the ancestor table will become out of sync. When this happens, you can rebuild the table to restore everything to normal.

Simply access this URL:

```
http://yoursite/admin/permissions/pagepermsadmin.action
```

⚠ *The information on this page does not apply to Confluence OnDemand.*

Screenshot: Page Level Permissions



RELATED TOPICS

Administrators Guide Home Confluence Documentation Home

Viewing and Editing License Details

When you upgrade or renew your Confluence license, you will receive a new license key. You will need to update your Confluence installation with the new license key.

You can access your license key via http://my.atlassian.com

On this page:

The information on this page does not apply to Confluence OnDemand.

Updating your License Details

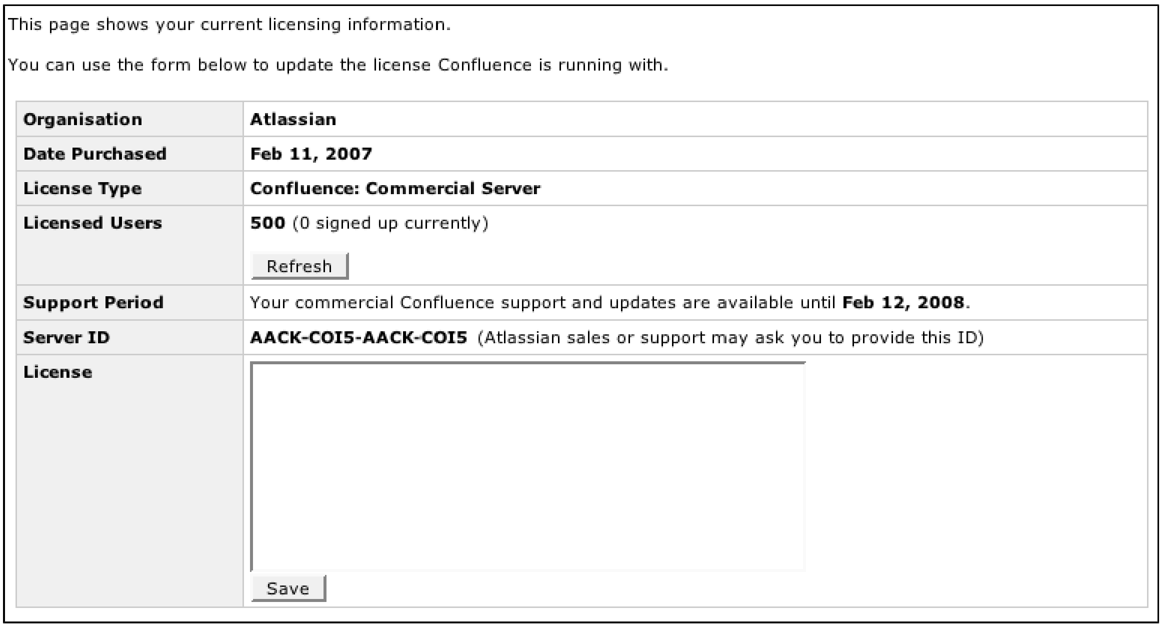
To update your Confluence license,

1. Log into Confluence as a user with Confluence Administrator or System Administrator permissions.
2. Choose **Browse** > **Confluence Admin**.
3. Click '**License Details**' under the heading '**Administration** in the left-hand panel.
4. Enter your new license details into the '**License**' field and click the '**Save**' button.

If you are running a Confluence cluster, you will need to:

- Update each server's Confluence license separately.
- Ensure that the new license has enough nodes to cover all servers that are currently running in your cluster. (To check the number of active servers in your cluster, see the Cluster Administration page.)

Screenshot : License Details



This page shows your current licensing information.

You can use the form below to update the license Confluence is running with.

Organisation	**Atlassian**
Date Purchased	**Feb 11, 2007**
License Type	**Confluence: Commercial Server**
Licensed Users	**500** (0 signed up currently) Refresh
Support Period	Your commercial Confluence support and updates are available until **Feb 12, 2008**.
Server ID	**AACK-COI5-AACK-COI5** (Atlassian sales or support may ask you to provide this ID)
License	Save

Viewing your License Details

The '**License Details**' page tells you:

- How many users your Confluence instance is licensed to support, and how many are currently registered.

  Note: The number of registered users only includes users who have '**can use Confluence**' permission. Deactivated users are not included.
  Click the '**Refresh**' button to make sure you see the latest count.
- What type of license you have (e.g. Commercial, Academic, Community).
- How much time remains in your one-year support and upgrades period (for full licenses) or 30-day trial (for trial licenses).
- Your server ID, which:
  - is generated when you install Confluence for the first time
  - exists for the life of the Confluence instance
  - survives an upgrade
  - is held in the database
  - is not bound to a specific license
  - is the same for all servers in a cluster.

To view the details of your Confluence license,

1. Log into Confluence as a user with Confluence Administrator or System Administrator permissions.
2. Choose **Browse** > **Confluence Admin**.
3. Click '**License Details**' under the heading '**Administration** in the left-hand panel.

Downgrading your Confluence License

If you need to downgrade your Confluence license to one which allows fewer users, please make sure first that your new license covers your current user base.

- View your license details as described above.
- Verify that the number of users '**signed up currently**' is lower than the number allowed by the new license.
- If you currently have more users signed up than the new license allows, please follow these instructions on removing users from your Confluence site.

RELATED TOPICS

No content found for label(s) system-information,license.

Administrators Guide Home Confluence Documentation Home

Viewing System Information

The System Information screen provides information about Confluence's configuration, and the environment in which Confluence has been deployed. Your system configuration information is helpful to us when diagnosing errors you may face using Confluence. If you file a support request or bug report, the more detail you can provide about your installation and environment the faster we will be able to help.

To view your system information,

1. Choose **Browse** > **Confluence Admin**.
2. Click '**System Configuration**' in the 'Administration' section.

✓ The handy **Memory Graph** helps you keep track of Confluence's memory usage.

> ⚠ *The information on this page does not apply to Confluence OnDemand.*

RELATED TOPICS

Cache Statistics
Viewing Site Statistics
Viewing and Editing License Details
Viewing and Managing Installed Plugins
Live Monitoring Using the JMX Interface
Tracking Customisations Made to your Confluence Installation

Administrators Guide Home Confluence Documentation Home

Live Monitoring Using the JMX Interface

With the JMX interface (introduced in Confluence 2.8), you can monitor the status of your Confluence instance in real time. This will provide you with useful data such as the resource usage of your instance and its database latency, allowing you to diagnose problems or performance issues. To read the JMX data, you will need to use a JMX client.

Disable JMX

> ⚠ If you experience any problems during Confluence startup that are related to JMX, it is possible to disable the JMX registration process. Please place jmxContext.xml in your `<confluence-install>/confluence/WEB-INF/classes` folder to do so.

> ⚠ *The information on this page does not apply to Confluence OnDemand.*

What is JMX?

JMX (Java Management eXtensions) is a technology for monitoring and managing Java applications. JMX uses objects called MBeans (Managed Beans) to expose data and resources from your application.

1. Enabling JMX Remote with Tomcat

By default, Confluence uses the Apache Tomcat web server. To use JMX, you must enable it on your Tomcat server, by carrying out the steps under the Apache Tomcat documentation, entitled Enabling JMX Remote. With those steps completed, restart your Tomcat server.

For the stand-alone, add the startup parameter -Dcom.sun.management.jmxremote to setenv.sh or setenv.bat. See instructions for the Windows Service - enter it in the same place as PermGen Memory.

2. Selecting your JMX Client

You need to use a JMX client in order to view the JMX output from Confluence. JConsole is a readily available JMX client that is included with the supported Java Developer Kit (version 5 onwards). The full name is the '*Java Monitoring and Management Console*', but we will refer to it as JConsole for the purposes of this document.

3. Adding the JMX Client to your Path

You must add the location of the JConsole binary file to your path environment variable. As JConsole resides in the 'bin' (binaries) folder under your Java directory, the path should resemble something like this:

```
JDK_HOME/bin/
```

In this example, replace 'JDK_HOME' with the full system path to your Java directory.

4. Configuring JConsole

To configure JConsole:

1. Run the JConsole application.
2. You will be prompted to create a new connection. Choose **remote process** and enter the hostname of your Confluence instance and a port of your choosing.

   > ✓ To connect easily, add the startup parameters to setenv.bat or setenv.sh:
   > -Dcom.sun.management.jmxremote -Dcom.sun.management.jmxremote.port=8086
   > -Dcom.sun.management.jmxremote.authenticate=false
   > Port 8086 is unlikely to be used. Then, connect remotely using port 8086.

   > ⚠ JConsole, or any JMX client, will not see applications which are not owned by the same user. For example under Windows, if an application is started as a service, it is the System User which owns the process, and not the Current User.

3. Click **Connect**.

Note: Other JMX clients besides JConsole can read JMX information from Confluence.

What can I monitor with JMX?

The JMX interface allows you to see live internal information from your Confluence instance, via the following MBeans:

IndexingStatistics

This MBean shows information related to search indexing.

Property name	**Function**	**Values**
Flushing	Shows state of cache (i.e. flushing, or not).	True/False
LastElapsedMilliseconds	Time taken during last indexing.	Milliseconds
LastElapsedReindexing	Time taken during last re-indexing.	Milliseconds
TaskQueueLength	Shows number of tasks in the queue.	Integer

SystemInformation

This MBean shows information related to database latency. It also contains most of the information presented on the System Information page.

Property name	Function	Values
DatabaseExampleLatency	Shows the latency of an example query performed against the database.	Milliseconds

RequestMetrics

This MBean shows information related to system load and error pages served.

Property name	Function	Values
AverageExecutionTimeForLastTenRequests	Average execution time for the last ten requests.	Milliseconds
CurrentNumberOfRequestsBeingServed	Number of requests being served at this instant.	Integer
ErrorCount	Number of times the Confluence error page was served.	Integer
NumberOfRequestsInLastTenSeconds	Obviously, the Number Of Requests In the Last Ten Seconds.	Integer

MailServer-SMTPServer

This MBean shows information related to email dispatch attempts and failures. There will be an MBean for every SMTP Mailserver that has been configured in the Confluence instance.

Property name	Function	Values
EmailsAttempted	The number of email messages Confluence has tried to send.	Integer
EmailsSent	The number of email messages sent successfully.	Integer

MailTaskQueue

This MBean shows information related to the email workload.

Property name	Function	Values
ErrorQueueSize	Number of errors in the queue.	Integer
Flushing	Shows state (i.e. flushing, or not)	True/False
FlushStarted	Time that operation began.	Time
RetryCount	The number of retries that were performed.	Integer

TaskSize	Number of email messages queued for dispatch.	Integer

SchedulingStatistics

This MBean shows information related to current jobs, scheduled tasks and the time that they were last run.

High CPU consuming threads

For Java 1.6, add the Top Threads Plugin to monitor whether CPU is spiking. Download it to a directory and run JConsole like this:
JConsole -pluginpath /pathto/topthreads.jar

This works only with JDK 1.6, but that can be on the remote machine if the server is running a lower version.

> Please note, adding live monitoring to a production instance may itself have an impact on performance.

Related Topics

- Viewing System Information
- Cache Statistics
- Viewing and Editing License Details
- Viewing and Managing Installed Plugins

Tracking Customisations Made to your Confluence Installation

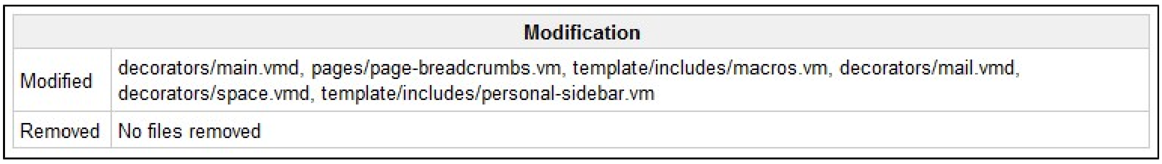
The '**Modification**' section of the Confluence '**System Information**' screen lists the files that have been changed since your Confluence application was installed. You will find this information particularly useful when upgrading Confluence to a new version, because you will need to re-apply all customisations after the upgrade.

> *The information on this page does not apply to Confluence OnDemand.*

To see the modifications made to files in your Confluence installation,

1. Choose **Browse** > **Confluence Admin**.
2. Select '**System Information**' in the 'Administration' section of the left-hand panel.
3. Scroll down to the section titled '**Modification**'.

Screenshot: Modifications tracker on the Confluence System Information screen



Modification	
Modified	decorators/main.vmd, pages/page-breadcrumbs.vm, template/includes/macros.vm, decorators/mail.vmd, decorators/space.vmd, template/includes/personal-sidebar.vm
Removed	No files removed

Notes

- The modification tracker does not detect changes to class files from the `confluence.jar` or other JAR files. If you modify classes, the Confluence modification detection does not report the modification. See issue CONF-20993.

RELATED TOPICS

Administrators Guide Home Confluence Documentation Home

Viewing Site Statistics

Note that the site activity information is **disabled by default**. See notes below.

If enabled, the global activity screen displays statistics on the activity in your Confluence site. These include:

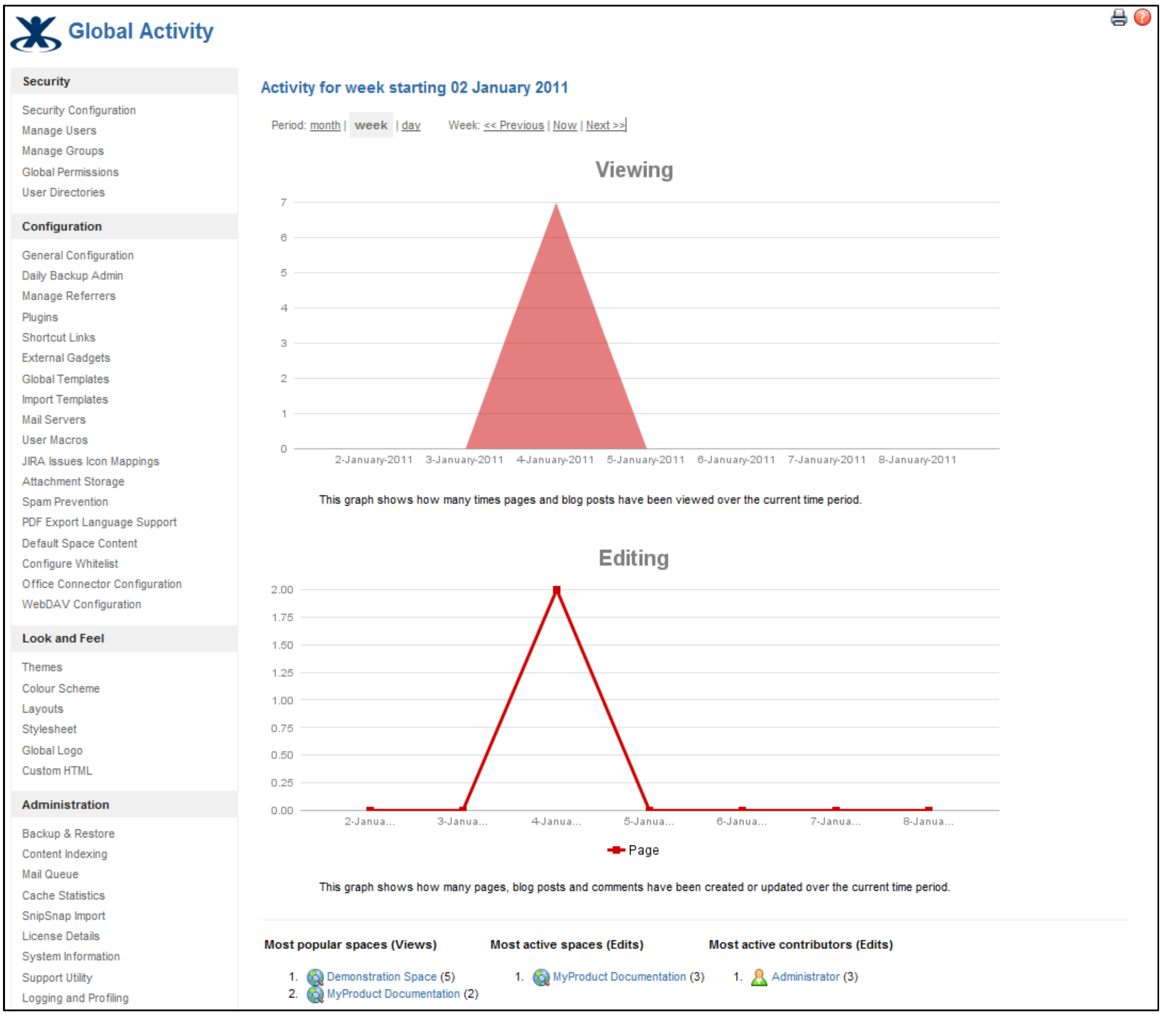
- How many pages and blog posts have been viewed, added or updated over a given period.
- Which spaces are the most popular (most frequently viewed).
- Which spaces are the most active (most frequently edited).
- Which people are the most active contributors/editors of content.

> ⚠ *The information on this page does not apply to Confluence OnDemand.*

To view the activity on your site,

1. Choose **Browse** > **Confluence Admin**.
2. Click '**Global Activity**' in the 'Administration' section of the left-hand panel.

Screenshot: Global Activity



Activity for week starting 02 January 2011

This graph shows how many times pages and blog posts have been viewed over the current time period.

This graph shows how many pages, blog posts and comments have been created or updated over the current time period.

Most popular spaces (Views)

1. Demonstration Space (5)
2. MyProduct Documentation (2)

Most active spaces (Edits)

1. MyProduct Documentation (3)

Most active contributors (Edits)

1. Administrator (3)

The top ten most popular and most active pages and/or blog posts will be listed, with a link to each.

Notes

- The Confluence Usage Stats plugin, which provides the 'Global Activity' screen, is known to cause performance problems on large installations. This plugin is **disabled by default**. A status report on the progress of the performance issues with this plugin is available in this issue: USGTRK-15.

- Your Confluence system administrator can enable the plugin, but please be aware of the possible impact upon your site's performance.
- The plugin is sometimes called 'Confluence Usage Tracking'.
- If your Confluence site is clustered, the global activity information will not be available.

RELATED TOPICS

How Do I Get More Statistics From Confluence?
Cache Statistics
Viewing Space Activity
Live Monitoring Using the JMX Interface
Installing and Configuring Plugins

Administrators Guide Home Confluence Documentation Home

Viewing System Properties

After adding memory, setting a proxy or changing other Java options, it can be difficult to diagnose whether the system has picked them up. This page tells you how to view the system properties that your Confluence site is using.

> ⚠ *The information on this page does not apply to Confluence OnDemand.*

In Confluence 3.0.2 and Later

You can see the expanded system properties on the 'System Information' screen of the Confluence Administration Console.

To see the system properties recognised by your Confluence installation:

1. Choose **Browse** > **Confluence Admin**.
2. Select **System Information** in the 'Administration' section of the left-hand panel.
3. Scroll down to the section titled 'System Properties'.

In Confluence Versions Earlier than 3.0.2

To find out more about what properties are being picked up, download the file systemproperties.jsp (attached to this page). Place it in your `<confluence-install>/confluence/admin` directory. Access the following URL:

```
http://<yourbaseurl>/admin/systempropertie
s.jsp
```

No restart of Confluence is required.

Installing Patched Class Files

Atlassian support or the Atlassian bug-fixing team may occasionally provide patches for critical issues that have been resolved but have not yet made it into a release. Those patches will be class files which are attached to the relevant issue in our JIRA bug-tracking system.

> ⚠ *The information on this page does not apply to Confluence OnDemand.*

Installation Instructions for the Confluence Distribution

Follow these steps to install a patched class file:

1. Shut down your confluence instance.
2. Copy the supplied class files to `<installation-directory>/confluence/WEB-INF/classes/<subdirectories>`, where:
   - `<installation-directory>` must be replaced with your Confluence Installation directory. (If you need more information, read about the Confluence Installation Directory.)
   - `<subdirectories>` must be replaced by the value specified in the relevant JIRA issue. This value will be different for different issues. In some cases, the subdirectories will not exist and you will need to create them before copying the class files. Some issues will contain the patch in the form of a ZIP file which will contain the desired directory structure.
3. Restart your Confluence instance for the changes to become effective.

ℹ Class files in the `/WEB-INF/classes` directory of a web application will be loaded before classes located in JAR files in the `/WEB-INF/lib` directory. Therefore, classes in the first directory will effectively replace classes of the same name and package which would otherwise be loaded from the JAR files.

RELATED TOPICS

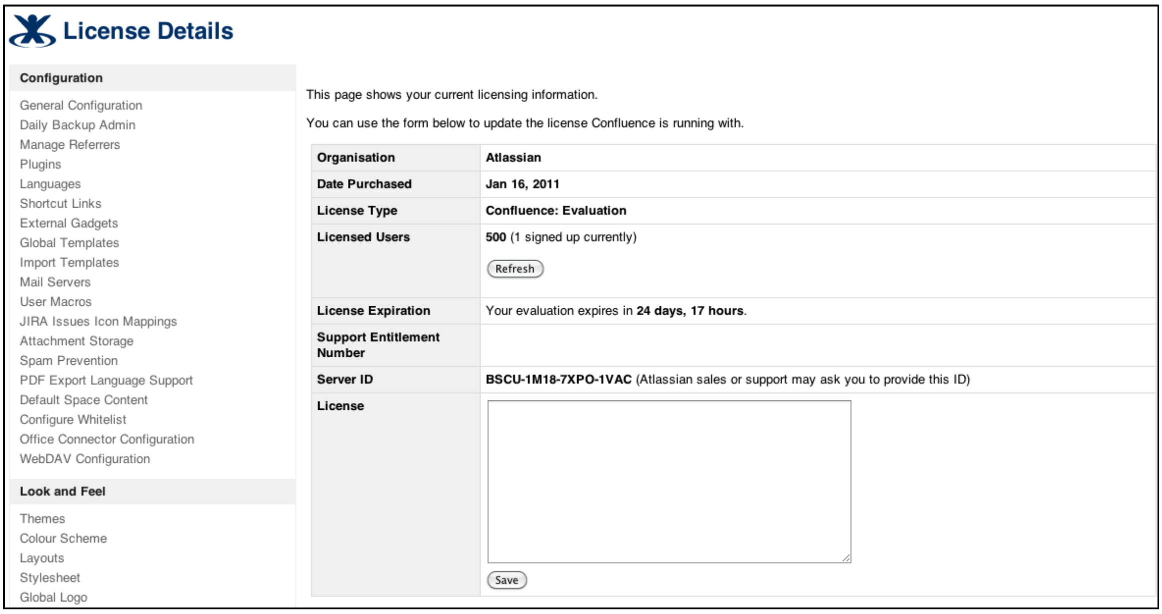
Editing Files within JAR Archives
Where are the files that used to be in my Confluence installation directory?

Administrators Guide Home Confluence Documentation Home

Finding Your Confluence Support Entitlement Number (SEN)

There are three ways to find you Support Entitlement Number (SEN):

▾ Method 1: Check in the Confluence Administration Interface
Select `Administration >> License Details`. The SEN is shown:



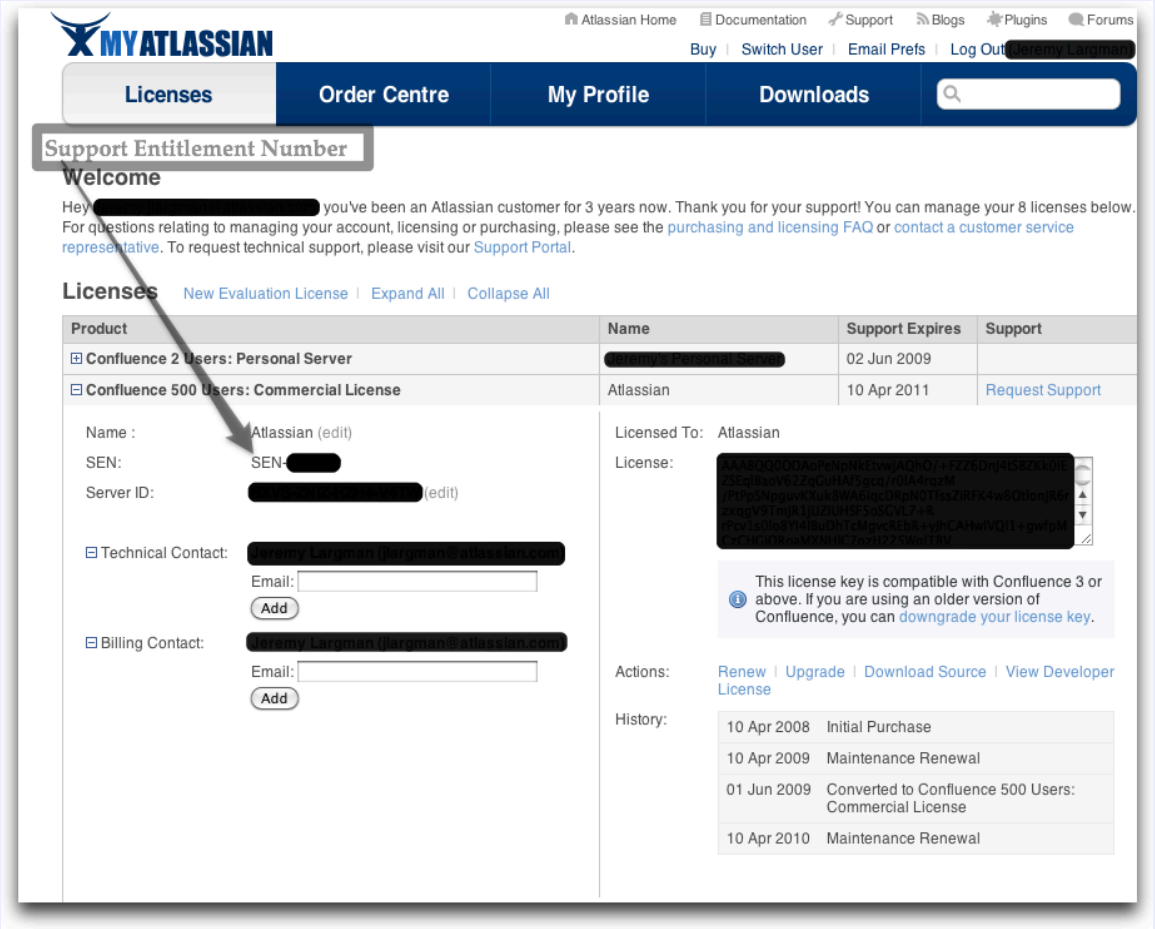
This page shows your current licensing information.

You can use the form below to update the license Confluence is running with.

Organisation	**Atlassian**
Date Purchased	**Jan 16, 2011**
License Type	**Confluence: Evaluation**
Licensed Users	**500** (1 signed up currently)
License Expiration	Your evaluation expires in **24 days, 17 hours**.
Support Entitlement Number	
Server ID	**BSCU-1M18-7XPO-1VAC** (Atlassian sales or support may ask you to provide this ID)
License	

▾ Method 2: Log into my.atlassian.com as the Account Holder or Technical Contact

Unable to render content due to system error: null



Welcome

Hey [redacted] you've been an Atlassian customer for 3 years now. Thank you for your support! You can manage your 8 licenses below. For questions relating to managing your account, licensing or purchasing, please see the purchasing and licensing FAQ or contact a customer service representative. To request technical support, please visit our Support Portal.

Licenses New Evaluation License | Expand All | Collapse All

Product	Name	Support Expires	Support
⊞ Confluence 2 Users: Personal Server	[redacted]	02 Jun 2009	
⊟ Confluence 500 Users: Commercial License	Atlassian	10 Apr 2011	Request Support

Name : Atlassian (edit)

SEN: SEN-[redacted]

Server ID: [redacted] (edit)

⊟ Technical Contact: [redacted]

Email: Add

⊟ Billing Contact: [redacted]

Email: Add

Licensed To: Atlassian

License: [redacted]

This license key is compatible with Confluence 3 or above. If you are using an older version of Confluence, you can downgrade your license key.

Actions: Renew | Upgrade | Download Source | View Developer License

History:

10 Apr 2008	Initial Purchase
10 Apr 2009	Maintenance Renewal
01 Jun 2009	Converted to Confluence 500 Users: Commercial License
10 Apr 2010	Maintenance Renewal

Method 3: Atlassian Invoice

Your Support Entitlement Number (SEN) appears on the third page of your Atlassian Invoice.

See Finding Your Support Entitlement Number in the support space for more general information about how Atlassian Support uses this number.

The information on this page does not apply to Confluence OnDemand.

Configuring Confluence

The pages listed below contain instructions on configuring Confluence. If you cannot find what you are looking for, try the search box in the left-hand navigation panel.

- Site Configuration
  - Configuring the Site Home Page
  - Configuring the Administrator Contact Page
  - Editing the Site Title
  - Editing the Global Logo
  - Configuring the Server Base URL
  - Customising Default Space Content
  - Configuring the Destination of View Space Links
  - Editing the Site Welcome Message
  - Configuring the What's New Dialog
- Configuring Encoding
  - Character encodings in Confluence

    - Troubleshooting Character Encodings
      - "€" Euro character not displaying properly
      - MySQL 3.x Character Encoding Problems
  - Configuring Mail
    - Configuring a Server for Outgoing Mail
    - Configuring the Recommended Updates Email Notification
    - The Mail Queue
  - Optional Settings
    - Attachment Storage Configuration
      - Hierarchical File System Attachment Storage
    - Configuring a WebDAV client for Confluence
    - Configuring Quick Navigation
    - Enabling OpenSearch
    - Enabling the Did You Mean Feature
    - Enabling the Remote API
    - Enabling Threaded Comments
    - Enabling Trackback
  - Other Settings
    - Configuring Attachment Size
    - Configuring Character Encoding
    - Configuring HTTP Timeout Settings
    - Configuring Indexing Language
    - Configuring Number Formats
    - Configuring Shortcut Links
    - Configuring Time and Date Formats
  - Configuring System Properties
    - Recognised System Properties
  - Configuring a Large Confluence Installation
  - Configuring Logging
  - Registering External Gadgets
    - Configuring a URL Whitelist for Gadgets

RELATED TOPICS

Tracking Customisations Made to your Confluence Installation
Confluence Configuration Guide

Administrators Guide Home Confluence Documentation Home

Site Configuration

- Configuring the Site Home Page
- Configuring the Administrator Contact Page
- Editing the Site Title
- Editing the Global Logo
- Configuring the Server Base URL
- Customising Default Space Content
- Configuring the Destination of View Space Links
- Editing the Site Welcome Message
- Configuring the What's New Dialog

Configuring the Site Home Page

You can configure Confluence to send users to any of the space home pages on the site when they log in, rather than to the dashboard.

To configure the site-wide home page:

1. Go to the '**Administration Console**' and click '**General Configuration**' in the left-hand panel.
2. Click '**Edit**' next to the '**Site Configuration**' panel.
3. Select a space from the '**Site Homepage**' dropdown menu. When users log in, Confluence will open the home page of the space you choose here.
    a. The spaces available to set as the site home page will depend on the access permissions of the space and the site.
        i. The site home page must be accessible to the '**confluence-users'** group
        ii. If the site allows anonymous access, the site home page must also be accessible to **anonymous users**, that is, people who have not logged in to Confluence.
4. Ensure that the '**View Space Goes to Browse Space**' option is set to '**Off**' if you want users to be sent to the space **home page** and not the **space summary page**.
5. Click the '**Save**' button at the bottom of the screen.

Notes

- The user's personal settings will override the global setting.

Related Topics

No content found for label(s) site-configuration.

Administrators Guide Home Confluence Documentation Home

Configuring the Administrator Contact Page

The administrator contact page is a form that allows a user of Confluence to send a message to the administrators of their Confluence site. (In this context, administrators are those users who are members of the *'confluence-administrators'* group. See the explanation of site administrators.)

The title of the administrator contact page is 'Contact Site Administrators'. Typically, Confluence users may get to this page by clicking a link on an error screen such as the '500 error' page.

On this page:

Customising the Administrator Contact Message

You can customise the message that is presented to the user on the '**Contact Site Administrators**' page.

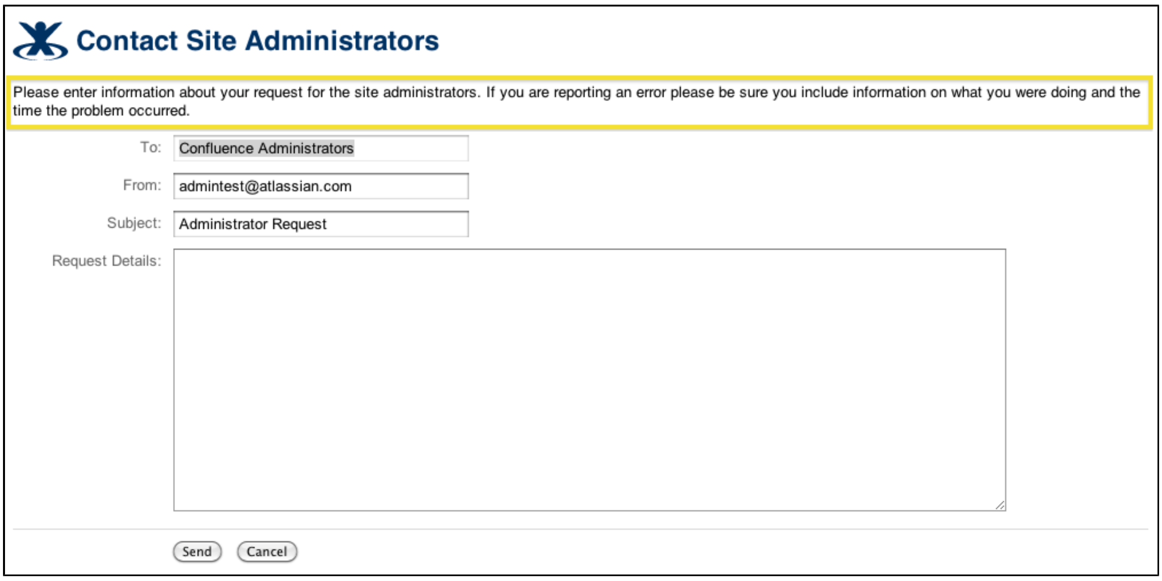
To edit the administrator contact message:

1. Go to the 'Administration Console' and click **General Configuration** in the left-hand panel.
2. Click **Edit** at the top of the 'Site Configuration' section.
3. Enter your text in the **Custom Contact Administrators Message** box. You can enter any text or Confluence wiki markup.
4. Click **Save**.

The Default Administrator Contact Message

By default, the 'contact administrators message' looks much like the highlighted area in the screenshot below, starting with 'Please enter information...'.

Screenshot: The default 'Contact Site Administrators' message



Contact Site Administrators

Please enter information about your request for the site administrators. If you are reporting an error please be sure you include information on what you were doing and the time the problem occurred.

To: Confluence Administrators

From: admintest@atlassian.com

Subject: Administrator Request

Request Details:

To restore the message to its default simply remove the custom message you entered when following the instructions above, so that the 'Custom Contact Administrators Message' field is empty.

Customisation Examples

When entering the 'Custom Contact Administrators Message', you can use text and Confluence wiki markup.

This is similar to entering your own text and markup for the 'Site Welcome Message'. For examples of the kind of customisations possible, take a look at the guide to editing the site welcome message.

Disabling the Administrator Contact Form

If you prefer to disable the ability for users to send an email message to the site administrators, you can disable the form portion of this screen. You can only disable the form if you first provide a 'Custom Contact Administrators Message' as described above.

To enable or disable the administrator contact form:

1. Go to the 'Administration Console' and click **General Configuration** in the left-hand panel.
2. Click **Edit** at the top of the 'Site Configuration' section.
3. Select **on** or **off** for the 'Contact Administrators Form'.
4. Click **Save**.

Configuring Spam Prevention

You can configure Confluence to use Captcha to help prevent spam, including the spamming of Confluence administrators. The administrator contact form is covered by the site-wide Captcha settings as documented in Configuring Captcha for Spam Prevention.

Related Topics

Contacting Confluence Administrators

Configuring Captcha for Spam Prevention

Editing the Site Title

The site title appears in your browser's title bar. By default, it is set to 'Confluence'.

To change the title of your Confluence site:

1. Go to the '**Administration Console**' and click '**General Configuration**' in the left-hand panel.
2. Click '**Edit**' at the top of the '**Site Configuration**' screen.
3. Enter a new title for your site in the input field next to '**Site Title**'.
4. Click '**Save**'.

Related Topics

No content found for label(s) site-configuration.

Administrators Guide Home Confluence Documentation Home

Editing the Global Logo

By default, the global logo appears beside the page title on all pages in the site. You can disable the logo or replace it with one of your own.

You need to be a Confluence Administrator to configure the global logo.

To configure the global logo:

1. Choose **Browse** > **Confluence Admin**.
2. Click **Global Logo**, under 'Look and Feel' in the left panel.
3. Click **Off** to disable the current logo, or click **Browse** to upload a new logo.

Related Topics

No content found for label(s) site-configuration.

Administrators Guide Home Confluence Documentation Home

Configuring the Server Base URL

The **Server Base URL** is the URL via which users access Confluence. The base URL **must** be set to the same URL by which browsers will be viewing your Confluence site.

Confluence will automatically detect the base URL during setup, but you may need to set it manually if your site's URL changes or if you set up Confluence from a different URL to the one that will be used to access it publicly.

ℹ You need to have System Administrator permissions in order to perform this function.

> ⚠ *The information on this page does not apply to Confluence OnDemand.*

To configure the Server Base URL:

1. In Confluence, open the '**Browse**' menu and select '**Confluence Admin**'. The 'Administration Console' will open.
2. Click '**General Configuration**' in the left-hand panel.
3. Click the '**Edit**' button next to '**Site Configuration**'.
4. Enter the new URL in the '**Server Base URL**' text box.

5. '**Save**' your changes.

Example

If Confluence is installed to run in a non-root context path (that is, it has a context path), then the server base URL should include this context path. For example, if Confluence is running at:

```
http://www.foobar.com/confluence
```

then the server base URL should be:

```
http://www.foobar.com/confluence
```

Notes

- **Using different URLs.** If you configure a different base URL or if visitors use some other URL to access Confluence, it is possible that you may encounter errors while viewing some pages.
- **Changing the context path.** If you change the context path of your base URL, you may also need to edit the web server's `server.xml`file to reflect the new path:
    1. Stop the Confluence server.
    2. Go to your Confluence 'destination directory'. This is the directory where the Confluence installation files are stored. For example, `C:\Program Files\Atlassian\Confluence`. Let's call this directory '`{CONFLUENCE_INSTALLATION}`'.
    3. Edit the configuration file at `{CONFLUENCE_INSTALLATION}\conf\server.xml`.
    4. Change the value of the `path` attribute in the `Context` element to reflect the context path. For example, if Confluence is running at `http://www.foobar.com/confluence`, then your `path` attribute should look like this:

       ```
       <Contextpath="/confluence" docBase="../confluence" debug="0" reloadable="
       ```
    5. Save the file.

RELATED TOPICS

No content found for label(s) site-configuration.

Customising Default Space Content

Confluence Administrators can define **default content for a space home page**. This content will appear on the home page whenever someone adds a new space. You can define different content for global spaces and for personal spaces.

The default content will appear only for new spaces created after you have defined the content. Content in existing home pages will not be changed.

To define default content for home pages in global spaces:

1. Go to the '**Administration Console**' and click '**Default Space Content**' under 'Configuration' in the left-hand panel.
2. The '**Space Home Pages**' tab will open on the 'Default Space Content' page. Enter the content which you want to appear on the home page for new global spaces. You can use special characters within the content as variables (place holders). Confluence will replace the curly brackets and digits with the corresponding information as shown below:

- **{0}** — The space name.

3. Click the '**Save**' button.

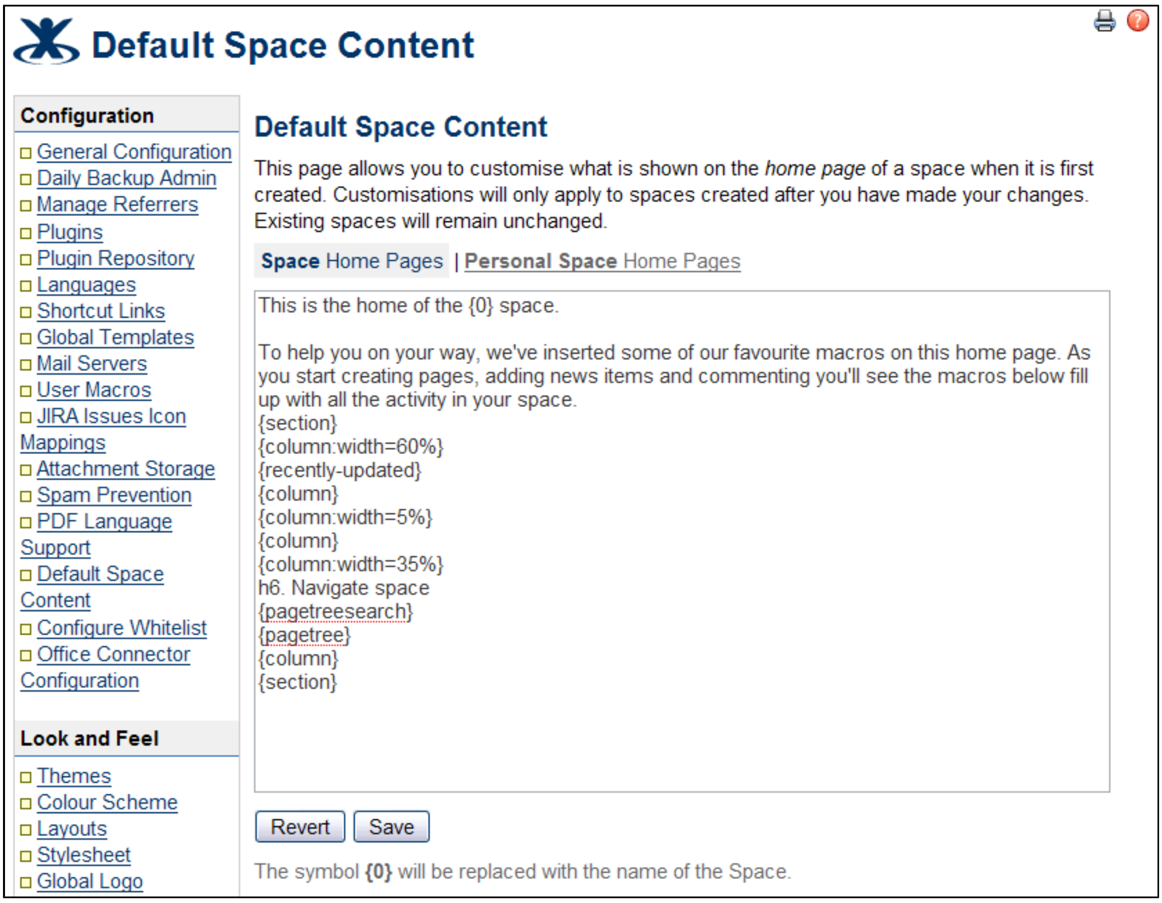
To define default content for home pages in personal spaces:

1. Go to the '**Administration Console**' and click '**Default Space Content**' under 'Configuration' in the left panel.
2. The 'Space Home Pages' tab will open on the 'Default Space Content' page. Click the '**Personal Space Home Pages**' tab.
3. Enter the content which you want to appear on the home page for new personal spaces. You can use special characters within the content as variables (place holders). Confluence will replace the curly brackets and digits with the corresponding information as shown below:
   - **{0}** — The space owner's full name.
   - **{1}** — The space owner's e-mail address.
   - **{2}** — Any personal information the space owner has entered on their user profile in the 'Information about me' section.
4. Click the '**Save**' button.

You can also undo all customisations of the default home page content, and go back to the default content as originally supplied with Confluence.

To restore the original default content:

1. Go to the '**Administration Console**' and click '**Default Space Content**' under 'Configuration' in the left panel.
2. Select either the 'Space Home Pages' tab or the '**Personal Space Home Pages**' tab, as required.
3. Click the '**Revert**' button.



Default Space Content

Default Space Content

This page allows you to customise what is shown on the *home page* of a space when it is first created. Customisations will only apply to spaces created after you have made your changes. Existing spaces will remain unchanged.

```
This is the home of the {0} space.

To help you on your way, we've inserted some of our favourite macros on this home page. As you start creating pages, adding news items and commenting you'll see the macros below fill up with all the activity in your space.
{section}
{column:width=60%}
{recently-updated}
{column}
{column:width=5%}
{column}
{column:width=35%}
h6. Navigate space
{pagetreesearch}
{pagetree}
{column}
{section}
```

The symbol **{0}** will be replaced with the name of the Space.

Screenshot above: Defining default space content

Related Topics

No content found for label(s) site-configuration.

Administrators Guide Home Confluence Documentation Home

Configuring the Destination of View Space Links

By default, when you click a space link in order to view the space, you are taken to the space's home page. If you wish, you can configure Confluence to redirect all space links on the site to the '**Browse Space**' view of the space instead.

To direct the space link to the 'browse space' view:

1. Go to the '**Administration Console**' and click '**General Configuration**' in the left-hand panel.
2. Click '**Edit**' at the top of the '**Site Configuration**' screen.
3. Select '**On**' next to '**View Space goes to Browse Space**'.
4. Click '**Save**'.

Related Topics

No content found for label(s) site-configuration.

Administrators Guide Home Confluence Documentation Home

Editing the Site Welcome Message

The site welcome message appears at the top left of the Confluence dashboard, between the site logo and the list of spaces. You can use it to display an introduction to the site or a message of the day.

To edit the site welcome message:

1. Go to the **Administration Console** and click **General Configuration** in the left-hand panel.
2. Click **Edit** at the top of the **Site Configuration** section.
3. Type into the **Site Welcome Message** box. You can enter text or Confluence wiki markup.
4. Click **Save**.

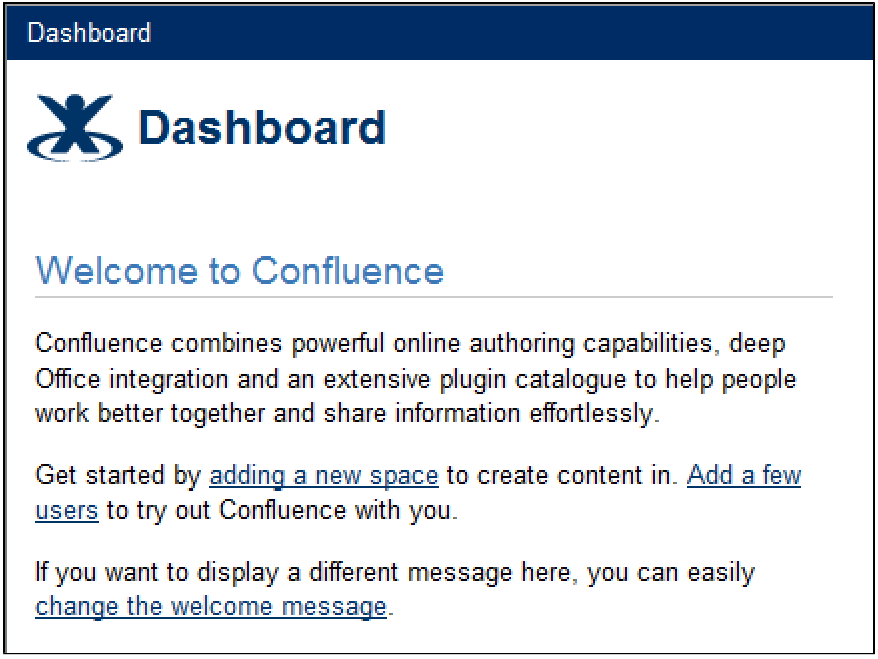
On this page:

The Default Site Welcome Message

By default, the site welcome message looks more or less like the screenshot below, starting with the words **Welcome to Confluence** and ending above the list of spaces.

To restore the default site welcome message and remove your customised message, just delete the text in the **Site Welcome Message** text box. Provided that you have not customised Confluence, your Confluence users will see the default message if there is no text in the **Site Welcome Message** text box in your Administration Console.

Screenshot: Site welcome message at top left of the dashboard



Dashboard

Welcome to Confluence

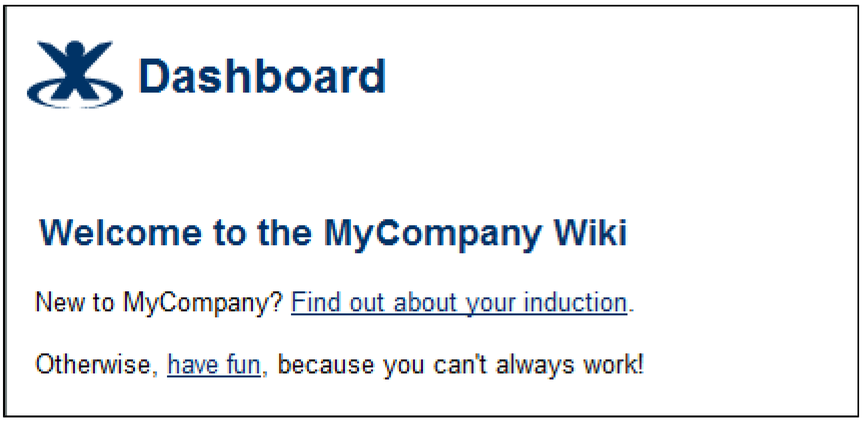
Confluence combines powerful online authoring capabilities, deep Office integration and an extensive plugin catalogue to help people work better together and share information effortlessly.

Get started by adding a new space to create content in. Add a few users to try out Confluence with you.

If you want to display a different message here, you can easily change the welcome message.

Example 1. Adding a Simple Welcome Message

Let's say you want to display a simple message like this at the top of your dashboard:



Dashboard

Welcome to the MyCompany Wiki

New to MyCompany? Find out about your induction.

Otherwise, have fun, because you can't always work!

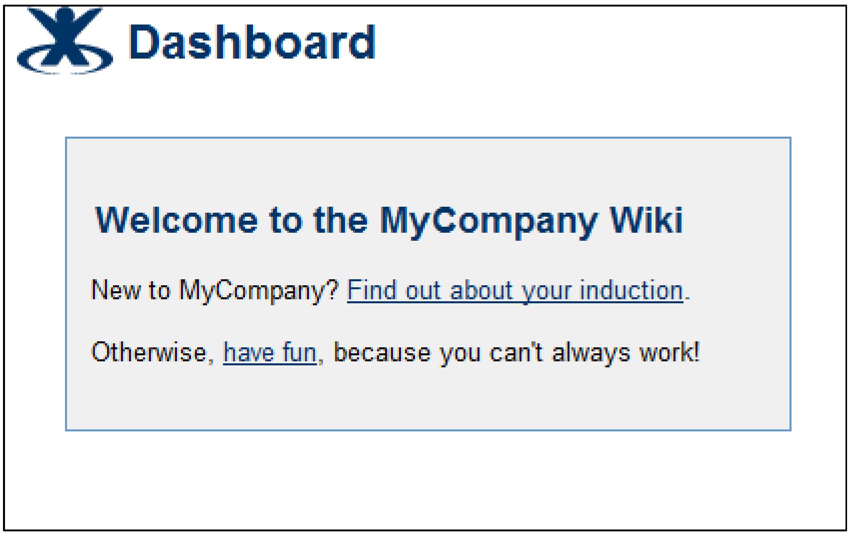
To produce the above welcome message, follow the step-by-step instructions above and add the following wiki markup into the **Site Welcome Message** text box:

```
h2. Welcome to the MyCompany Wiki

New to MyCompany? [Find out about your
induction|DS:Company Induction].

Otherwise, [have fun|DS:Have Fun], because
you can't always work!
```

ⓘ In our example, the links point to two pages in the Confluence Demonstration Space, 'DS'. If your Confluence site does not have a 'DS' space, the links will be broken. That's OK, because you will want to replace them with links to your own pages anyway. This is just an example.

Example 2. Formatting your Welcome Message

Now let's say you want to put the words into a panel and add some spacing, so that your dashboard looks like this:



Dashboard

Welcome to the MyCompany Wiki

New to MyCompany? Find out about your induction.

Otherwise, have fun, because you can't always work!

To produce the above welcome message, follow the step-by-step instructions above and add the following wiki markup into the **Site Welcome Message** text box:

```
{panel}
h2. Welcome to the MyCompany Wiki

New to MyCompany? [Find out about your
induction|DS:Company Induction].

Otherwise, [have fun|DS:Have Fun], because
you can't always work!
\\
\\
{panel}
\\
```

Example 3: Including Content from Another Page

It may be easier to write your welcome message on a normal Confluence page and include the page into the **Sit**

e Welcome Message text box. Using a normal page means that you can:

- Write the message using the editor rather than wiki markup.
- Preview the content of the welcome message before saving it, using the page editor's preview feature.
- Allow other people, who are not Confluence administrators, to edit the welcome message.

To include content from another page:

1. Create a Confluence page as usual and add your welcome message as the page content. Remember to limit the size of the content, because it must fit nicely onto the dashboard. For this example, let's assume you put your page in the 'DS' space and the title of your page is 'Dashboard Welcome Message'.
2. Add page permissions or space permissions to suit your requirements. You may want to restrict the editing of the page to a group of people, or you may want to allow any employee to edit the page. This will determine who can update the welcome message on the dashboard.
3. Follow the step-by-step instructions above and add the following wiki markup into the **Site Welcome Message** text box:

   ```
   {include:DS:Dashboard Welcome Message}
   ```

   ℹ In the above example we use the `{include}` macro to display the content from the given page. See the guide to the include macro. In our example, the space key 'DS' and the page name 'Dashboard Welcome Message' are variables. You can use any space and page you like.
4. Save the site welcome message. The dashboard will display the content of the page immediately. Similarly, if you or anyone else edits the page, the welcome message on the dashboard will change as soon as you save the page.

Example 4. Adding Blog Posts Filtered by Labels to your Welcome Message

Looking for more advanced ideas?

This video shows you how to display a list of blog posts on your dashboard and how to choose the blog posts by labelling them.

Video title: '*Bring "Must Read" Content to the Dashboard*'

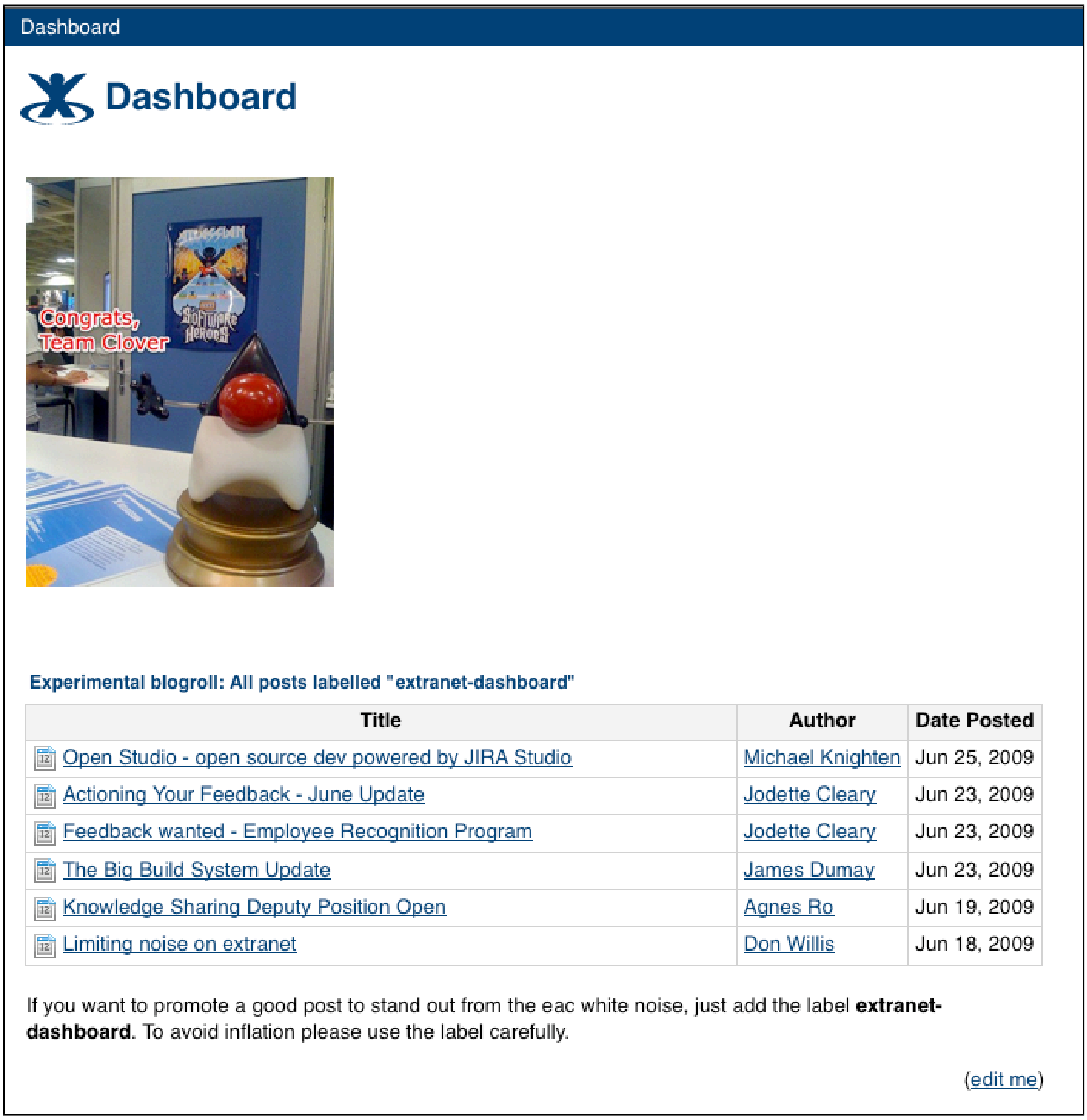
Summary of the procedure shown in the video:

1. Create a page containing the `{blog-posts}` macro. Choose to display only the blog posts that are labelled with '**dashboard-blog**'. (This is just an example of a label. You can choose any label text you like.) See the guide to the Blog Posts macro.
2. Add the label to a blog post. (In the video, we just add the label to one blog post. You will probably want to add it to a number of posts.)
3. Edit your site welcome message to include the above page, using the include macro.

app.episodic.com

How We Use the Site Welcome Message at Atlassian

Atlassian makes great use of the welcome message on our internal Confluence wiki. Here is an example of the dashboard as it appeared on a certain day:



Dashboard

Dashboard

Experimental blogroll: All posts labelled "extranet-dashboard"

Title	Author	Date Posted
Open Studio - open source dev powered by JIRA Studio	Michael Knighten	Jun 25, 2009
Actioning Your Feedback - June Update	Jodette Cleary	Jun 23, 2009
Feedback wanted - Employee Recognition Program	Jodette Cleary	Jun 23, 2009
The Big Build System Update	James Dumay	Jun 23, 2009
Knowledge Sharing Deputy Position Open	Agnes Ro	Jun 19, 2009
Limiting noise on extranet	Don Willis	Jun 18, 2009

If you want to promote a good post to stand out from the eac white noise, just add the label **extranet-dashboard**. To avoid inflation please use the label carefully.

(edit me)

The welcome message itself contains just an {include} macro:

```
{include:STAFF:Extranet Homepage}
```

The include macro allows you to include the content an entire page onto another page. This particular page lives in the STAFF space, where anyone can edit it. It usually shows some amusing picture or company-wide notice. The featured photo generally changes once a week or so – whenever someone feels like changing it. The page itself has over 600 edits by many different people.

The page also includes an edit link, for quick access to change the welcome message. We have the Composition plugin installed which allows you to use the {float} macro.

Our wiki markup in the 'Extranet Homepage' page looks something like this:

```
!Clover Dukey.jpg|width=200!

{nodisplay}
This is the content that goes on the
Extranet homepage, above the spaces list.

NOTE: KEEP YOUR PICTURES SMALL (<80KB) --
USE JPG FOR PICTURES, WIDTH 400
{nodisplay}
h4. Experimental blogroll: All posts
labelled "extranet-dashboard"

{blog-posts:content=titles|labels=extranet
-dashboard|spaces=@all|max=10}
If you want to promote a good post to
stand out from the eac white noise,
just add the label *extranet-dashboard*.
To avoid inflation please use the
label carefully.

{float-right}
([edit
me|http://extranet.atlassian.com/pages/edi
tpage.action?pageId=603422736])
{float-right}
```

Related Topics

No content found for label(s) site-configuration.

Administrators Guide Home Confluence Documentation Home

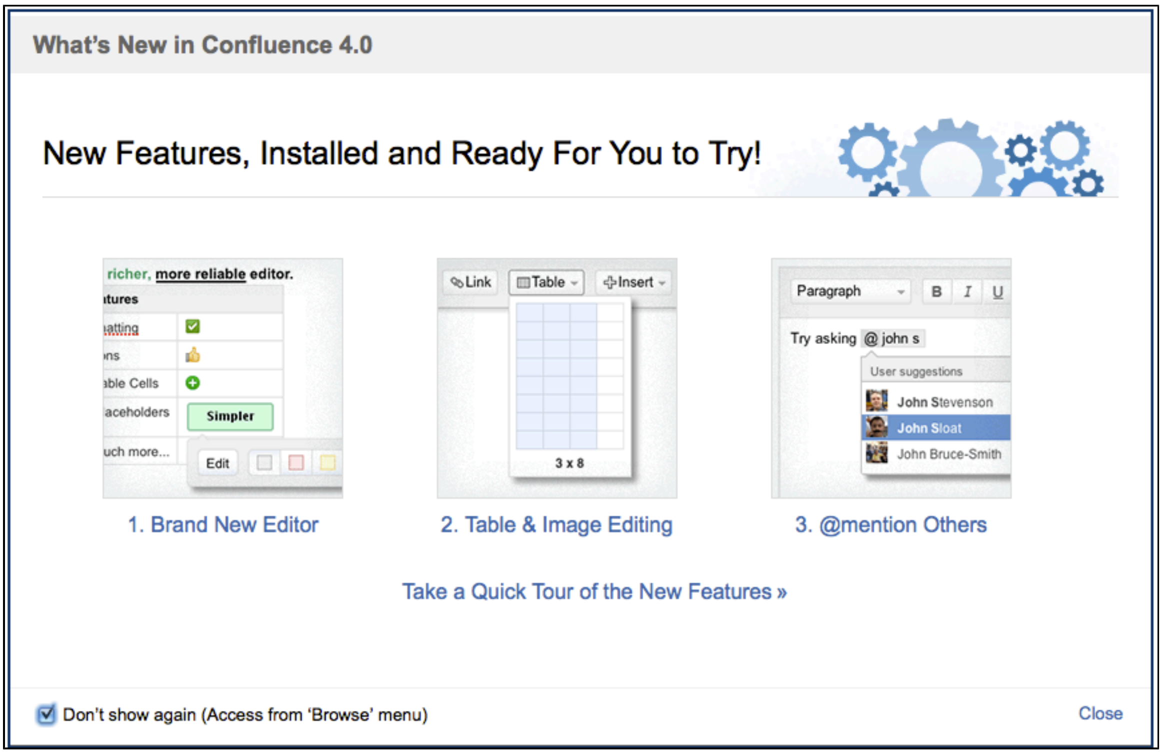
Configuring the What's New Dialog

The 'What's New' dialog automatically displays when a user first logs in after a major Confluence upgrade (e.g. upgrading to Confluence 4.0). The dialog displays a summary of the new features for the release, sourced from our website (by default).

Confluence administrators can configure the behaviour of the 'What's New' dialog, as follows:

- Change the URL that the 'What's New' dialog retrieves information from.
- Disable the dialog.

On this page:



What's New in Confluence 4.0

New Features, Installed and Ready For You to Try!

Take a Quick Tour of the New Features »

☑ Don't show again (Access from 'Browse' menu)

Screenshot above: An example of the 'What's New' dialog

Changing the 'What's New' Dialog URL

The 'What's New' dialog URL is stored in your Confluence `help-paths.properties` file. This URL is a concatenation of the `help.prefix` property with the `help.whats.new.iframe.link`.

Before you begin:

- The `help.prefix` property also defines the base URL for Confluence help links, i.e. help links in the Confluence application.

To change the 'What's New' Dialog URL:
Follow the instructions in the 'Changing the Links for Individual Help Pages' section on Local Confluence Documentation. You will need to update the '`help.prefix`' and '`help.whats.new.iframe.link`' properties, as desired.

For example, you may have installed your Confluence documentation behind a firewall at `http://www.example.com/` and created a page `http://www.example.com/whatsnew` that you use for change management. In this case, you would do the following:

- Set `help.prefix` to `http://www.example.com/`
- Set `help.whats.new.iframe.link` to `whatsnew`

There is an additional property '`help.whats.new.full.link`'. This is only used if the content pointed to by the updated URL isn't loaded in 10 seconds, in which case a 'timeout' screen is displayed with a link to the full 'What's New' content. For locally-hosted pages you can just set this property to the same value as `help.whats.new.iframe.link`.

Disabling the 'What's New' Dialog

The 'What's New' dialogue is enabled via a plugin. To disable the 'What's New' dialogue, you need to disable the '**Confluence What's New**' plugin in Confluence.

To disable the 'Confluence What's New' plugin:
Follow the instructions on Disabling or Enabling a Plugin. Please note, the '**Confluence What's New**' plugin is a 'System Plugin'. Click '**Show System Plugins**' on the Plugins administration page to display the system plugins.

Notes

Related Topics

Disabling or Enabling a Plugin
Local Confluence Documentation

Configuring Encoding

Confluence allows the configuration of which character encoding is used to deliver pages.

> ⚠ While different character encodings are supported, we strongly recommend that **UTF-8** is used. Confluence is heavily tested on UTF-8, and users are likely to have less problems with this encoding than others.

> ⚠ **Mac Users**
>
> Mac Users please note that **MacRoman** encoding is compatible with UTF-8. You do not need to change your encoding settings if you are already using MacRoman.

To avoid problems with character encoding, make sure the encoding used across the different components of your system are the same:

- Configuring Database Character Encoding
- Application Server URL encoding
- Confluence Character Encoding

If you are having problems with the character encoding in Confluence, please see the Troubleshooting Character Encodings page.

> ⚠ *The information on this page does not apply to Confluence OnDemand.*

Character encodings in Confluence

Character encoding advice

In general, **always set all character encodings to UTF-8**. That includes database, JDBC drivers, application server, filesystem and Confluence.

In certain isolated cases (e.g. Microsoft Windows), it might not be possible to use a fully Unicode filesystem (that is, a default Windows install doesn't support Unicode filenames properly). If so, stick with UTF-8 for the other two and be aware that your operating system might have limitations around international attachments (pre-2.2), backup and restore of international data, etc.

The remainder of the document explains the encoding settings that are applicable in Confluence and how they relate to application behaviour.

> ⚠ *The information on this page does not apply to Confluence OnDemand.*

Where character encoding is used

There are three places that character encoding matters to Confluence:

1. **Database encoding** - usually the most important; it is where almost all user data is stored.
2. **Filesystem encoding** - important for attachment storage (pre-2.2), reading Velocity templates and writing exported files.
3. **HTTP request and response encoding** - important for form parsing, correct rendering by the browser and browser interpretation of encoded URLs.

Problems generally arise when Confluence thinks one of the above encoding is different to what it actually is. For example, Confluence might believe the database is using ISO-8859-1 encoding, when in fact it is UTF-8 encoded.

Java character encoding

Java *always* uses the multibyte UTF-16 character encoding for all `String` data*. This means that each of the encodings above defines how, at that particular point, characters are converted to and from Java's native UTF-16 format into some other format that the browser, filesystem or database might understand.

So when a request comes in to Confluence, we convert it from the request encoding to UTF-16. Then we store that data into the database, converting from UTF-16 to the database's encoding. Retrieving information from the database and sending it back to the browser is the same process in the opposite direction.

*A `char` represents single Unicode code point from the Base Multilingual Plane (BMP), encoded as UTF-16. Multiple `chars` are used as surrogate pairs for characters beyond U+FFFF.

Problems with character encodings

If Confluence has the wrong idea about encoding for one of the above, it manifests itself in different ways:

1. Incorrect database encoding - user data is corrupted between saving and restoring from the database. This often happens after a delay, as we cache data as it is written to the database and only later retrieve the corrupted copy from the database.
2. Incorrect/non-Unicode filesystem encoding - international filenames break attachment download/upload/removal (pre-2.2); exports break with international content or attachments.
3. Incorrect HTTP encoding - incorrect encoding selected by browser, resulting in incorrect rendering of characters. Changing browser encoding causes page to render properly. Broken URLs when linking to pages or attachments with non-ASCII characters.

Configuration of character encodings

The **Confluence character encoding** is a configuration setting found in `Administration > General Configuration`, and at runtime available in Settings.defaultEncoding. It is subsequently used in the following parts of the system:

- ConfluenceWebWorkConfiguration sets `webwork.i18n.encoding` to the this encoding, which WebWork uses in the response Content-Type header.
- AbstractEncodingFilter sets the HTTP request encoding to this encoding. This seems unnecessary, since the Content-Type header from the client should include the encoding used. This affects form submissions and file uploads.
- VelocityUtils reads in Velocity templates using this encoding when reading templates from disk.

- AbstractXmlExporter creates its output using this encoding.
- GeneralUtil uses this encoding when doing URLEncode and URLDecode. Different browsers have different support for character sets in URLs, so it's uncertain how much benefit this provides.

In summary, changing the Confluence character encoding will change your **HTTP request and response encoding** and your **Filesystem encoding** as used by exports and velocity templates.

The **database encoding** is the responsibility of your JDBC drivers. The drivers are responsible for reading and writing from the database in its native encoding and translating this data to and from Java Strings (which are UTF-16). For some drivers, such as MySQL, you must set Unicode encoding explicitly in the JDBC URL. For others, the driver is smart enough to determine the database encoding automatically.

Ideally, your database itself should be in a Unicode encoding (and we recommend doing this for the simplest configuration), but that is not necessary as long as:

- the database encoding supports all the characters you want to store in Confluence
- your JDBC drivers can properly convert from the database encoding to UTF-16 and vice-versa.

The **filesystem encoding** is mostly ignored by Confluence, except for the cases where the above configuration setting above plays a part (exports, velocity). When attachments are uploaded, they are written as a stream of bytes directly to the filesystem. It is the same when they are downloaded: the bytes from the file InputStream are written directly to the HTTP response.

In some places in Confluence, we use the *default filesystem encoding* as determined by the JVM and stored in the `file.encoding` system property (it can be overridden by setting this property at startup). This encoding is used by the Java InputStreamReader and InputStreamWriter classes by default. This encoding should probably never be used; for consistent results across all filesystem access we should be using the encoding set in the General Configuration.

In certain cases we explicitly hard-code the encoding used to read or write data to the filesystem. Two important examples are:

- importing Mbox mailboxes which are known to be ISO-8859-1
- Confluence Bandana config files are always stored as UTF-8.

Some application servers, Tomcat for example, have an encoding setting that modifies Confluence URLs before they reach the application. This can prevent access to international pages and attachments (really anything with international characters in the URL). See configuring your Application Server URL encoding.

RELATED TOPICS:

- Configuring Database Character Encoding
- Troubleshooting Character Encodings

Troubleshooting Character Encodings

Often users may have problems with certain characters in a Confluence instance. Symptoms may include:

- Non-ASCII characters appearing as question marks (?)
- Page links with non-ASCII characters not working
- Single characters being displayed as two characters
- Garbled text appearing

In most cases, it is due to a mis-configuration in one of the components that Confluence uses.

> ⚠ *The information on this page does not apply to Confluence OnDemand.*

Follow these steps to diagnose the problem:

1. Run the encoding test

Confluence includes an encoding test that can reveal problems with your configuration.

To perform the test, access the Encoding Test page via the `<confluence base-url>/admin/encodingtest.action` page on your Confluence instance. You will be required to copy and paste a line of text and submit a form. The test will take the text and pass it through Confluence, the application server and the database, and return the results.

You should also test pasting some sample text (Japanese for example) if you are experiencing problems with a specific language.

Example:

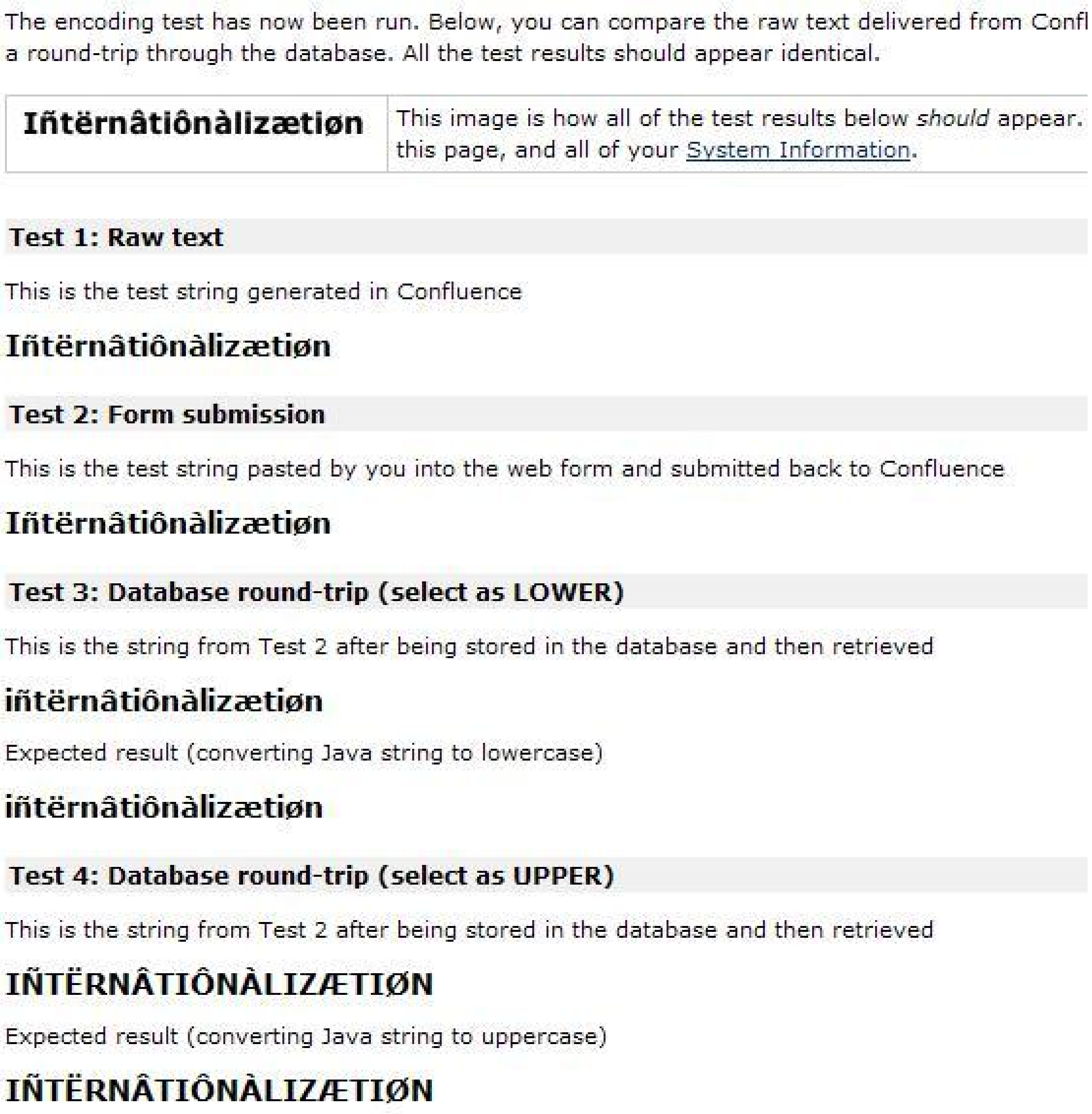
```
http://confluence.atlassian.com/admin/encodingtest.action
```

or

```
http://<host address>:<port>/admin/encodingtest.action
```

⛔ If the text displayed in the encoding test is different to what was entered, then there are problems with your character encoding settings.

A successful test looks like the following:



The encoding test has now been run. Below, you can compare the raw text delivered from Confl
a round-trip through the database. All the test results should appear identical.

Iñtërnâtiônàlizætiøn	This image is how all of the test results below *should* appear. this page, and all of your System Information.

Test 1: Raw text

This is the test string generated in Confluence

Iñtërnâtiônàlizætiøn

Test 2: Form submission

This is the test string pasted by you into the web form and submitted back to Confluence

Iñtërnâtiônàlizætiøn

Test 3: Database round-trip (select as LOWER)

This is the string from Test 2 after being stored in the database and then retrieved

iñtërnâtiônàlizætiøn

Expected result (converting Java string to lowercase)

iñtërnâtiônàlizætiøn

Test 4: Database round-trip (select as UPPER)

This is the string from Test 2 after being stored in the database and then retrieved

IÑTËRNÂTIÔNÀLIZÆTIØN

Expected result (converting Java string to uppercase)

IÑTËRNÂTIÔNÀLIZÆTIØN

⚠ **MySQL 3.x**

MySQL 3.x is known to have some problems with the upper- and lower-casing of some characters, and may fail the last two tests. For more information, see MySQL 3.x Character Encoding Problems.

2. Ensure the same encoding is used across all components

As mentioned in the Configuring Encoding document, the same character encoding should be used across the database, application server and web application (Confluence).

- To change the character encoding used in **Confluence**, see Configuring Character Encoding.
- To change the character encoding used in the **application server**, please ensure you set the Application Server URL encoding and view your application server's documentation on any other settings required to enable your encoding.
- To change the character encoding used in the **database**, see Configuring Database Character Encoding.

3. Requesting support

If there are still problems with character encoding after following the above steps, create a support request, and our support staff will aid in solving your problem.

Entering in the following details will help us to identify your problem:

- Attach screenshots of the problem
- Attach the results of the encoding test (above)
- Select which application server (and version) you are using
- Select which database (and version) you are using
- Copy the contents of the System Information page into the 'Description' field

"€" Euro character not displaying properly

The € (euro) symbol is a three byte character, with byte values in file (UTF-8) of 0xE2, 0x82, 0xAC.

Sometimes, if the character encoding is not set consistently among all participating entities of the system, Confluence, server and the database, one may experience strange behaviour.

> ...
> I write a page with a Euro sign in it (€). All is well, the Euro sign shows up in the wiki markup text-box, and the preview, and the display of the saved page.
> One day later, the Euro sign has changed into a question mark upside down!
> ...
> What is going on? Why does the Euro sign mysteriously change? How do I prevent it?

Interestingly enough the character encoding test passes with no problems, demonstrating that Confluence and the connected Database both recognise the € symbol.

The information on this page does not apply to Confluence OnDemand.

There are two potential reasons for this behaviour:

Database and Confluence is using utf-8 encoding. The connection is not.

When data transferred to it via the connection which does not use utf-8 encoding gets encoded incorrectly. Hence, updating the connection encoding may resolve this problem from now on, yet it probably would not affect already existing data.

Database is not using utf-8. Confluence and your connection are.

If your Database encoding is not set to UTF-8, yet is using some other encoding such as *latin1*, it could be one of the potential reasons why you lose the "€" characters at some stage. It could be occurring due to **caching**. When Confluence saves data to the database, it may also keep a local cached copy. If the database encoding is set incorrectly, the Euro character may not be correctly recorded in the database, but Confluence will continue to use its cached copy of that data (which is encoded correctly). The encoding error will only be noticed when the cache expires, and the incorrectly encoded data is fetched from the database.

> For instance the *latin1* encoding would store and display all 2-byte UTF8 characters correctly except for the euro character which is replaced by '?' before being stored. As Confluence's encoding was set to UTF-8, the 2-byte UTF-8 characters were stored in *latin1* database assuming that they were two *latin1* different characters, instead of one utf8 character. Nevertheless, this is not the case for 3-byte utf8 characters, such as the Euro symbol.

Please ensure that you set the character encoding to UTF-8 for all the entities of your system as advised in this guide.

MySQL 3.x Character Encoding Problems

MySQL 3.x is known to have some problems upper- and lower-casing certain (non-ASCII) characters.

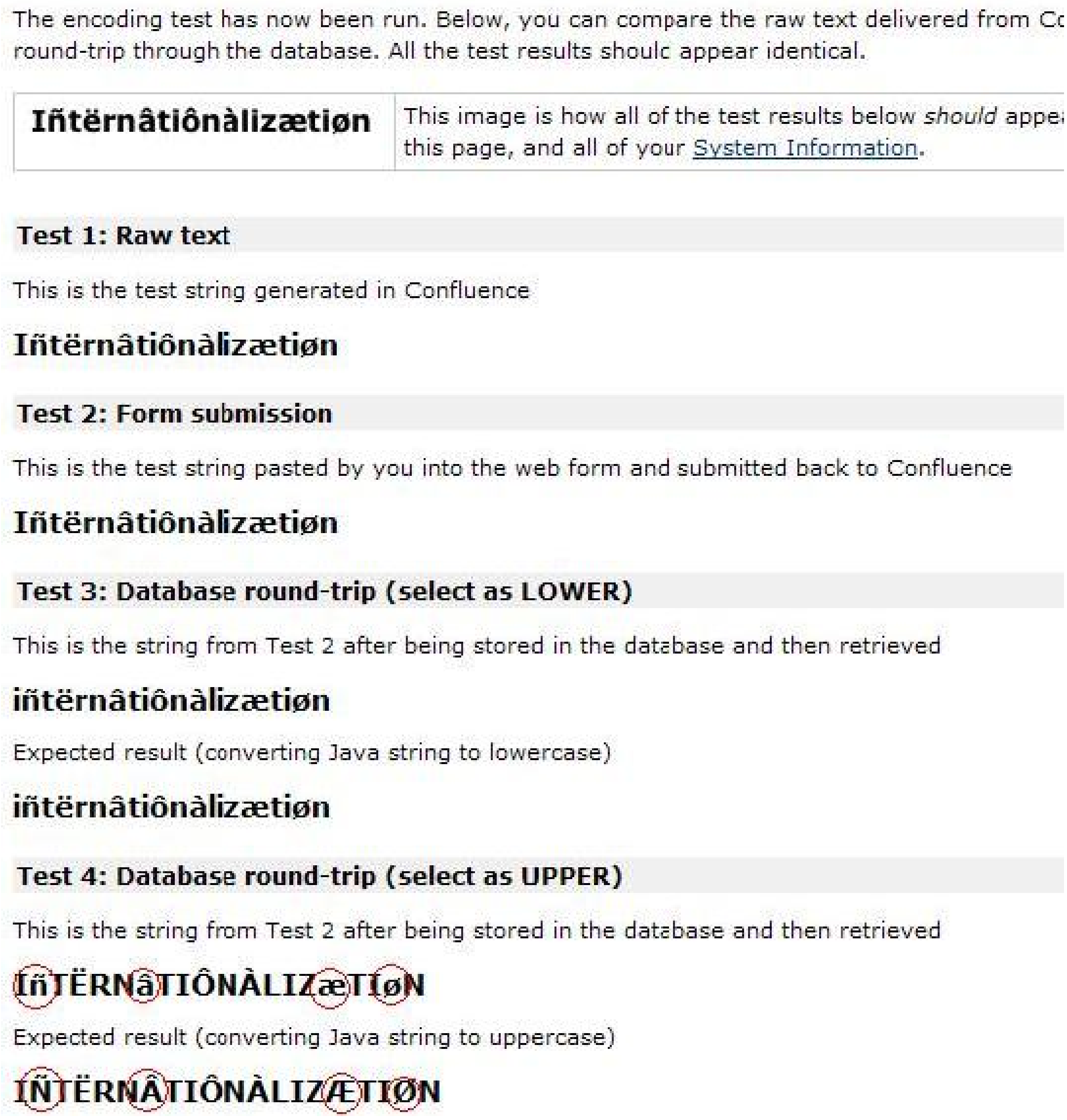
Diagnosing the problem

1. Follow the instructions for Troubleshooting Character Encodings.
2. If the upper- and lower-cased strings displayed on the Encoding Test are different, then your database is probably affected.

An example (faulty) output of the Encoding Test is shown below:

⚠ *The information on this page does not apply to Confluence OnDemand.*

Screenshot: Encoding Test Output



The encoding test has now been run. Below, you can compare the raw text delivered from Cc
round-trip through the database. All the test results shoulc appear identical.

Iñtërnâtiônàlizætiøn	This image is how all of the test results below *should* appe this page, and all of your System Information.

Test 1: Raw text

This is the test string generated in Confluence

Iñtërnâtiônàlizætiøn

Test 2: Form submission

This is the test string pasted by you into the web form and submitted back to Confluence

Iñtërnâtiônàlizætiøn

Test 3: Database round-trip (select as LOWER)

This is the string from Test 2 after being stored in the database and then retrieved

iñtërnâtiônàlizætiøn

Expected result (converting Java string to lowercase)

iñtërnâtiônàlizætiøn

Test 4: Database round-trip (select as UPPER)

This is the string from Test 2 after being stored in the database and then retrieved

IñTËRNâTIÔNÀLIZæTIøN

Expected result (converting Java string to uppercase)

IÑTËRNÂTIÔNÀLIZÆTIØN

Solution

Upgrade to a newer version of MySQL. (4.1 is confirmed to work.)

Configuring Mail

- Configuring a Server for Outgoing Mail
- Configuring the Recommended Updates Email Notification
- The Mail Queue

Customising the eMail Templates

Administrators Guide Home Confluence Documentation Home

The information on this page does not apply to Confluence OnDemand.

Configuring a Server for Outgoing Mail

Configuring your Confluence server to send email messages allows your Confluence users to:

- Receive emailed notifications and daily reports of updates.
- Send a page via email.

You can personalise email notifications by configuring the 'From' field to include the name and email address of the Confluence user who made the change.

You need System Administrator permissions in order to configure Confluence's email server settings.

On this page:

The information on this page does not apply to Confluence OnDemand.

Configuring Confluence to send email messages

To configure Confluence to send outgoing mail:

1. Choose **Browse** > **Confluence Admin**.
2. Select **Mail Servers** under **Configuration** in the left-hand panel. This will list all currently configured SMTP servers.
3. Click **Add New SMTP Server** (or **edit** an existing server).
4. Edit the following fields as required:
   - **Name**: By default, this is simply 'SMTP Server'.
   - **From Address**: Enter the email address that will be displayed in the 'from' field for email messages originating from this server.
     This field is mandatory. You will not be able to complete the Confluence mail server configuration until this field has been specified.
   - **From Name**: Enter the name that will be displayed in the 'from' field for email messages originating from this server. This is the text which appears before the user's registered email address (in angled brackets).
     This field accepts the following variables, which reference specific details defined in the relevant Confluence user's profile:

Variable	Description
${fullname}	The user's full name.
${email}	The user's email address.
${email.hostname}	The domain/host name component of the user's email address.

     The default is '`${fullname} (Confluence)`'.
     Hence, if Joe Bloggs made a change to a page he was watching and the Confluence site's 'From Address' was set to `confluence-administrator@example-company.com`, then the 'From'

field in his email notification would be: `Joe Bloggs (Confluence) <confluence-administrator@example-company.com>`.

- **Subject Prefix**: Enter a subject prefix, if required.

5. Manually enter your **Host Address**, **User Name** and **Password** details (recommended)

   OR

   Specify the **JNDI location** of a mail session configured in your application server.

Testing the email settings

A Confluence administrator can test the email server as follows:

1. Set up a mail server at **Confluence Admin** > **Mail Servers**, as described above
2. Click **Send Test Email** to check that the server is working. Check that you get the test email in your inbox.
3. You can flush the email queue to send the email message immediately. Go to **Confluence Admin** > **Mail Queue**, and click **Flush Mail Queue**. See The Mail Queue.

A user can test that notifications are working as follows:

1. Go to your user profile (using the **Settings** link) and edit your email preferences. See Subscribing to Email Notifications of Updates to Confluence Content.
2. Enable **Notify On My Actions**. (By default, Confluence does not send you notifications for your own changes.)
3. Go to a page you wish to get notifications about.
4. Choose **Tools** > **Watch**. See Watching a Page or Blog Post.
5. Edit the page, make a change, and save the page.
6. Check your email inbox. You may need to wait a while for the email message to arrive.

Troubleshooting

If you experience problems with these configurations, please check that your `<Confluence-Install>/confluence/WEB-INF/lib` contains only one copy of the following JAR files:

1. activation-x.x.x.jar
2. mail-x.x.x.jar

Ideally, these should be:

- activation-1.0.2.jar
- mail-1.3.2.jar (or later)

You will then need to move these into the proper directory:

Confluence distribution: Please move (not copy) the two jar files from the `<Confluence-Install>/confluence/WEB-INF/lib` directory to `<confluence-install>/lib` (for Confluence version 2.10 onwards) or `<Confluence-Install>/common/lib` (for earlier product versions) and restart Confluence.

Related Topics

No content found for label(s) mail-configuration.

Configuring the Recommended Updates Email Notification

Confluence sends a regular email report to subscribers, containing the top content that is relevant to the person receiving the message. This is called the 'Recommended Updates' notification.

If you have Confluence Administrator or System Administrator permissions, you can configure the default settings that determine how often the Recommended Updates notification is sent. When new users are added to Confluence, the default settings will be applied to their user profiles.

Confluence users can choose their personal settings, which will override the defaults. See Subscribing to Email Notifications of Updates to Confluence Content.

Initial settings of the defaults

When you install Confluence, the initial values of the default settings are as follows:

- The default frequency is weekly.
- If your Confluence site has public signup enabled, the Recommended Updates notification is disabled by default. If public signup is not enabled, the notification is enabled by default.

You can change the above settings, specifying a different default value for the site.

Notes:

- The Recommended Updates notification is sent only to people who have a user profile in Confluence. If your Confluence site uses external user management, such as LDAP, then people will receive the report only after they have logged in for the first time. (The first login creates their user profile.)
- The daily email message is sent at 1 p.m. in the user's configured time zone.
- The weekly email message is sent at 1 p.m. on Thursdays in the user's configured time zone.

On this page:

Related pages:

- Subscribing to Email Notifications of Updates to Confluence Content
- Confluence Administrator's Guide

Configuring the Recommended Updates notification

You can set the the default send option (send / do not send) and the default schedule (daily or weekly).

To configure the Recommended Updates email notification:

1. Choose **Browse** > **Confluence Admin**.
2. Click **Recommended Updates Email** in the left-hand panel.

Disabling the Recommended Updates notification for the entire site

You can also turn off the **recommended updates** notification for the entire site, by disabling the 'Confluence recommended updates email' plugin. See Disabling or Enabling a Plugin.

The Mail Queue

Email messages waiting to be sent out are queued in a mail queue and periodically flushed from Confluence once a minute. A Confluence administrator can also manually flush emails from the mail queue.

If there is an error sending messages, the failed emails are sent to an error queue from which you can either try to resend them or delete them.

⚠ *The information on this page does not apply to Confluence OnDemand.*

To view the mail queue,

1. Choose **Browse** > **Confluence Admin**.
2. Select '**Mail Queue**' in the left-hand panel. This will display the emails currently in the queue.
3. Click '**Flush Mail Queue**' to send all emails immediately.
4. Click '**Error Queue**' to view failed email messages. You can try to '**Resend**' the messages, which will flush the mails back to the '**Mail Queue**' or '**Delete**' them from here.

RELATED TOPICS

No content found for label(s) mail-configuration.

Optional Settings

- Attachment Storage Configuration
- Configuring a WebDAV client for Confluence
- Configuring Quick Navigation
- Enabling OpenSearch
- Enabling the Did You Mean Feature
- Enabling the Remote API
- Enabling Threaded Comments
- Enabling Trackback

Attachment Storage Configuration

Confluence allows you to store attachments in one of three places:

- Filesystem - locally in the Confluence home directory
- Database - in Confluence's configured database
- WebDAV - remotely on a WebDAV server (***deprecated***)

A System Administrator can configure Confluence's attachment storage via the '**Attachment Storage**' option on the '**Administration Console**'.

ℹ You need to have System Administrator permissions in order to perform this function.

⚠ *The information on this page does not apply to Confluence OnDemand.*

Attachment Storage Options

Local File System

By default, Confluence stores attachments in the `attachments` directory within the configured Confluence home folder. If you are looking to run Confluence Clustered, attachments must be stored in the database.

Database

Confluence gives administrators the option to store attachments in the database that Confluence is configured to use.

Here are some reasons why, as an administrator, you may want to choose this storage system:

- Ease of backup.
- Avoiding issues with certain characters in attachment file names.

> While storing attachments in the database can offer some advantages, please be aware that the amount of space used by the database will increase because of the greater storage requirements.

WebDAV

Confluence also allows administrators to set an external WebDAV repository as the location for attachment storage.

> **WebDAV attachment manager deprecated**
>
> The option to store Confluence attachments on a WebDAV server has never worked in a useful fashion, and has not been maintained for many versions.
>
> - The WebDAV attachment manager will be **deprecated** from Confluence 2.7, and will be removed from a later version of Confluence.
> - If you store attachments on external WebDAV servers, we recommend that you migrate to file-system or database-backed attachment storage as soon as possible. Refer to CONF-9313 and CONF-2887.
> - This DOES NOT affect the operation of the WebDAV plugin.

Migration between Attachment Storage Systems

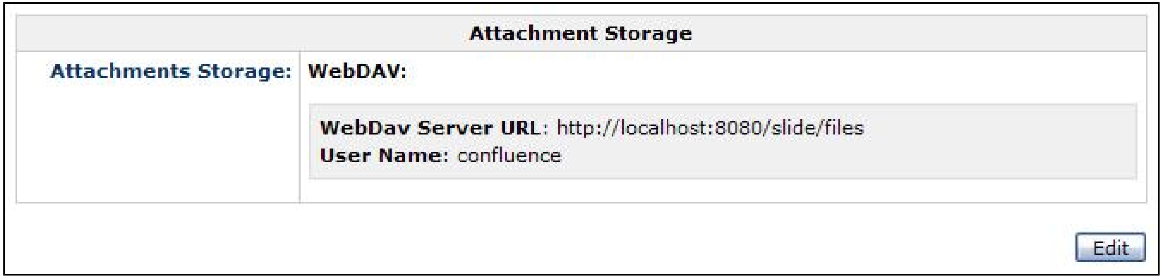
You can 'migrate' your attachments from one storage system to another. All existing attachments will be moved over to the new attachment storage system.

> When the migration occurs, all other users will be locked out of the Confluence instance. This is to prevent modification of attachments while the migration occurs. Access will be restored as soon as the migration is complete.

> When migrating attachments from your database to a filesystem, the attachments are removed from the database after migration. However, when migrating attachments from a filesystem to your database, the attachments remain on the filesystem after migration. If you wish to change this function's behaviour from 'copy' to 'move', please see CONF-14802 and cast your vote.

To perform a migration, follow the steps below:

1. Choose **Browse** > **Confluence Admin**.
2. Click '**Attachment Storage**' in the left-hand panel. The current configuration will be displayed.



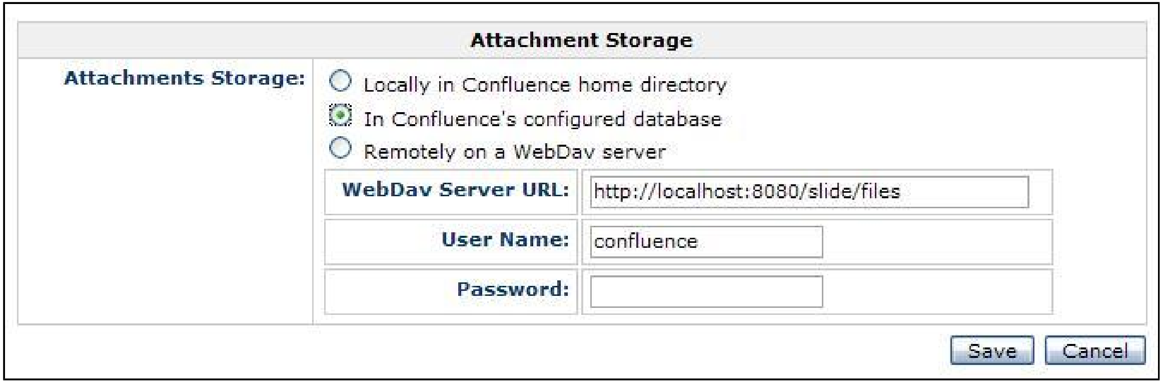
Attachment Storage

Attachments Storage: WebDAV:

WebDav Server URL: http://localhost:8080/slide/files
User Name: confluence

Attachment storage configuration

3. Click the '**Edit**' button to modify the configuration.
4. Select the storage system you desire.



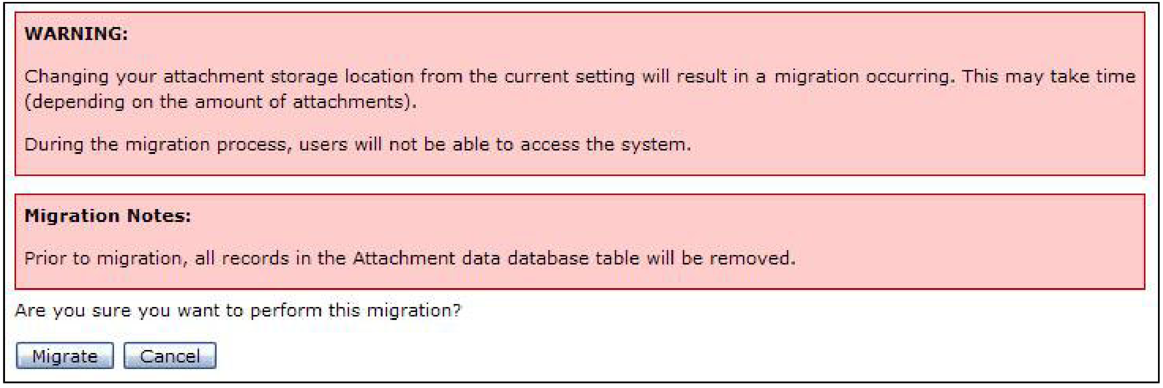
Attachment Storage

Attachments Storage:
○ Locally in Confluence home directory
● In Confluence's configured database
○ Remotely on a WebDav server

WebDav Server URL:	http://localhost:8080/slide/files
User Name:	confluence
Password:	

Edit attachment storage

5. Click the '**Save**' button to save the changes.
6. A screen will appear, asking you to confirm your changes. Clicking 'Migrate' will take you to a screen that displays the progress of the migration.



WARNING:

Changing your attachment storage location from the current setting will result in a migration occurring. This may take time (depending on the amount of attachments).

During the migration process, users will not be able to access the system.

Migration Notes:

Prior to migration, all records in the Attachment data database table will be removed.

Are you sure you want to perform this migration?

Migration warning

Troubleshooting

To enable debug logging for WebDAV attachment storage, add the following to the bottom of `WEB-INF/classes/log4j.properties` and restart Confluence:

```
log4j.logger.com.atlassian.confluence.pages.persistence.dao=DEBUG,confluencelog
log4j.additivity.com.atlassian.confluence.pages.persistence.dao=false

log4j.logger.org.apache.webdav=DEBUG,confluencelog
log4j.additivity.org.apache.webdav=false
```

RELATED TOPICS

No content found for label(s) data-storage.

Hierarchical File System Attachment Storage

For Confluence version 3.0, the structure of attachments stored on the filesystem was changed. In versions of Confluence prior to 3.0, attachments were stored in directories corresponding to the id of the content to which they belong. The more content in Confluence with attachments, the more directories you would have immediately beneath your configured attachments directory. This directory structure has been changed in Confluence 3.0 and since the default configuration of Confluence is to store attachments in the filesystem, this change is likely to have relevance to administrators of most existing Confluence installations.

If you are installing Confluence for the first time, there will be no consequences as a result of this change. If you are upgrading from a previous version of Confluence, the migration to this new filesystem structure should happen automatically during the upgrade.

The reason for introducing this change was to address the issue CONF-13004. Certain file systems have a limit on the number of files that can be stored in a directory and large Confluence installations were reaching this limit. In addition, storing too many files at a single directory level can cause performance degradation in some circumstances. This new attachment storage strategy ensures this will no longer be the case.

> ⚠ *The information on this page does not apply to Confluence OnDemand.*

> **Backup Confluence Home**
>
> Before upgrading to Confluence 3.0, as with any upgrade you must ensure you have a backup of your Confluence home directory before you proceed.

The New Directory Layout

The attachment storage layout was chosen to fulfil the following main requirements:

1. Limit the number of entries at any single level in a directory structure.
2. Partition attachments per space making it possible for a system admin to selectively back up attachments from particular spaces (see the JIRA issue for more details).

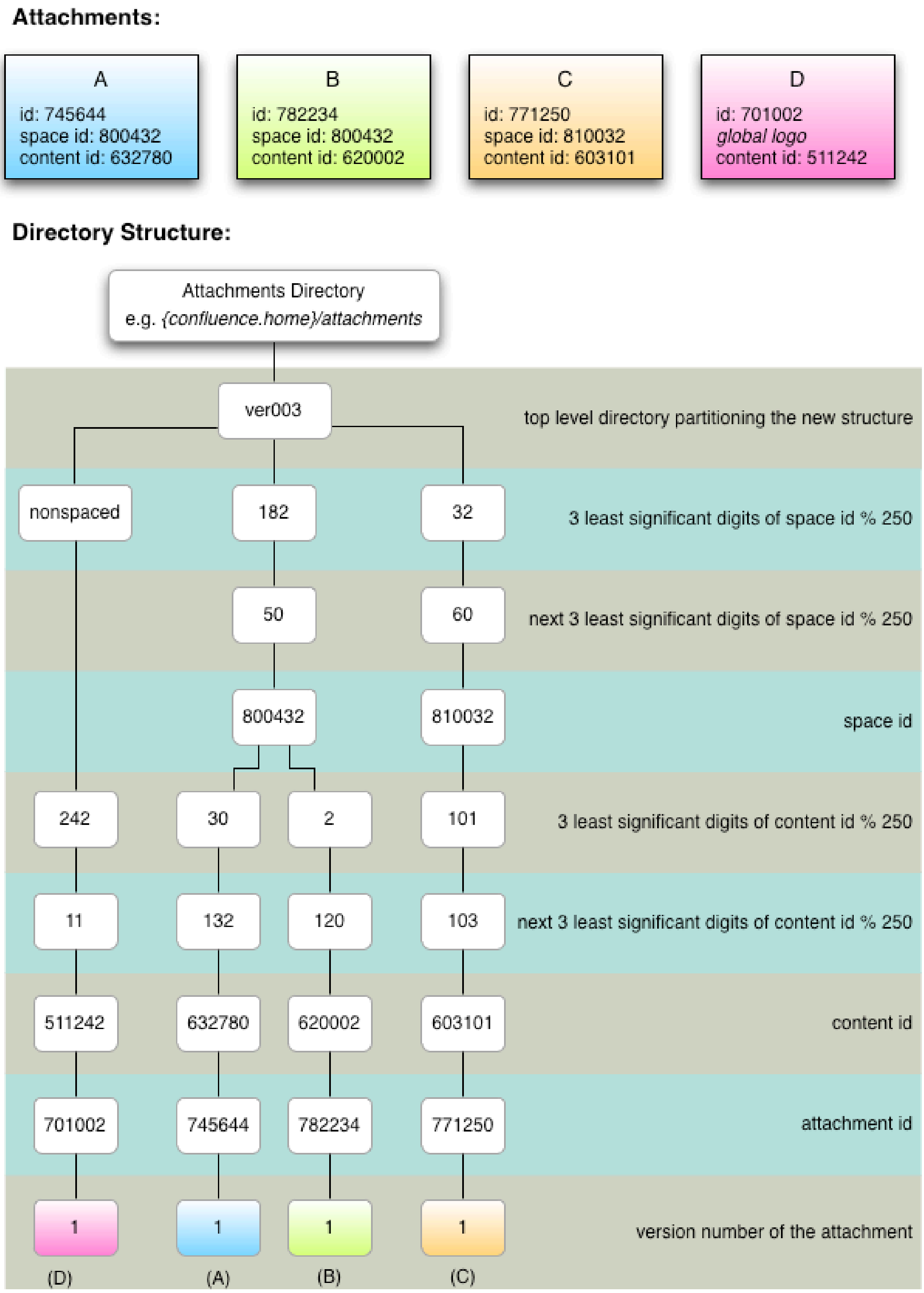
An attachment in Confluence can be thought of as having a number of identifying attributes: *id*, *space id* and *content id*. That is to say, the attachment logically belongs to a piece of content which logically belongs in a space (not all content belongs to a space). For attachments within a space in Confluence, the directory structure is typically 8 levels, with the name of each directory level based on the following algorithm:

level	Derived From
1 (top)	Always 'ver003' indicating the Confluence version 3 storage format
2	The least significant 3 digits of the *space id*, modulo 250
3	The next 3 least significant digits of the *space id*, modulo 250
4	The full *space id*

5	The least significant 3 digits of the *content id*, modulo 250
6	The next 3 least significant digits of the *content id*, modulo 250
7	The full *content id*
8	The full *attachment id*

Within the 8th level will be a file for each version of that attachment, named to match the version number e.g. 1

An example:



To find the directory where attachments for a particular space are stored, you can use the JSP findspaceattachments.jsp at the location `<confluence url>/admin/findspaceattachments.jsp`. This JSP requires a space key and returns the directory on the file system where attachments for that space are stored.

Attachment D in the above diagram is stored in a slightly different structure. Attachments that are not conceptually within a space replace the level 2 - 4 directories with a single directory called 'nonspaced'. Examples of such attachments are the global site logo and also attachments on draft content.

Upgrading to the new attachment storage structure

As mentioned previously, this upgrade is only necessary if you have Confluence configured to store attachments on the file system.

If migration is not necessary due to a different storage configuration (for example, because attachments are stored in the database), then no migration will occur during upgrade and the Confluence log will simply show the following messages -

```
INFO [main] [AbstractUpgradeManager]
upgradeStarted Starting automatic upgrade
of Confluence
INFO [main] [UpgradeTask] isUpgradeNeeded
The configured attachmentDataDao does not
store
    attachment data on the file system so
the
HierarchicalFileSystemAttachmentUpgradeTas
k is not necessary.
INFO [main] [AbstractUpgradeManager]
upgradeFinished Upgrade completed
successfully
```

Should migration be required, it will occur automatically during upgrade and the log will show output similar to this -

```
INFO [main] [UpgradeTask] doUpgrade
Beginning
HierarchicalFileSystemAttachmentUpgradeTas
k. Depending on the size of the
    attachment data this may take some
time.
INFO [main] [UpgradeTask] run 4023 pages
may have attachments to be moved to a new
hierarchical structure.
INFO [main] [UpgradeTask] run 0 of 4023
pages have had their attachments moved to
the new structure
```

```
INFO [main] [UpgradeTask] run 500 of 4023
pages have had their attachments moved to
the new structure
INFO [main] [UpgradeTask] run 1000 of 4023
pages have had their attachments moved to
the new structure
INFO [main] [UpgradeTask] run 1500 of 4023
pages have had their attachments moved to
the new structure
INFO [main] [UpgradeTask] run 2000 of 4023
pages have had their attachments moved to
the new structure
INFO [main] [UpgradeTask] run 2500 of 4023
pages have had their attachments moved to
the new structure
INFO [main] [UpgradeTask] run 3000 of 4023
pages have had their attachments moved to
the new structure
INFO [main] [UpgradeTask] run 3500 of 4023
pages have had their attachments moved to
the new structure
INFO [main] [UpgradeTask] run 4000 of 4023
pages have had their attachments moved to
the new structure
INFO [main] [UpgradeTask] run Successfully
moved the attachments for all 4023 pages
to the new hierarchical structure.
INFO [main] [UpgradeTask] doUpgrade
Completed
HierarchicalFileSystemAttachmentUpgradeTas
k.
INFO [main] [AbstractUpgradeManager]
```

```
upgradeFinished Upgrade completed
successfully
```

> It should be noted that for most implementations of Java, the migration to the new data structure involves moving the files (not copying them). Hence, there should not be a need to have additional disk space available. It also means that the migration should be relatively fast.

Have you previously applied the CONF-8298 patch?

The patch or workaround on the CONF-8298 issue changed the structure of attachment storage but not to the most efficient possible structure. So during the Confluence 3.0 upgrade process this intermediate (CONF-8298) structure will be detected and automatically upgraded.

Troubleshooting the upgrade

⚠ It should be noted that in the event of a failure, your attachment directory may be in an inconsistent state and your first step in troubleshooting should be to restore the backup of your home directory.

There are a number of reasons the migration could fail. This will be shown in the log with a message similar to "`Failed to move the attachments for all pages to the new hierarchical structure.`".

Immediately preceding this message in the log will be entries for each page whose attachments could not be moved. The following table shows examples of these messages and offers some possible explanations.

Example Message	Description
The configured attachment directory `<directory name>` could not be found or was not a directory.	The configured Confluence attachment directory is not accessible. Check confluence home for the attachment directory and ensure the permissions are correct to allow reading and writing for this directory.
It is not possible to migrate the attachments to the new structure since files already exist which the attachment process may need to create.	Your attachments directory contains files or directories which the upgrade task wants to create. That is, a top level directory called ver003 containing directories or files with names containing up to 3 digits (e.g. 1, 213). This could be due to a previous failed attempt to migrate the attachments. You should restore a previous good copy of your attachments directory and remove any files or directories with this naming pattern before retrying.
Couldn't find current Confluence content for the id `<content Id>`. The attachment is a non-spaced attachment (e.g. global logo, draft attachment, etc) and will be migrated to the nonspaced directory.	This is a normal message indicating that the attachment being migrated does not belong to a space e.g. global logo.
Problem while accessing the database for content id `content Id` so its attachments will not be migrated.	It was not possible to access the database at this point during the migration. You will need restore your Confluence attachment directory from the backup and attempt the upgrade again, once the database is accessible again.

Could not create the new attachment directory `directory`.	The upgrade task could not create the new directory to contain the attachment being moved. Does the server user have sufficient permission to perform this operation in the indicated directory? Is there sufficient disk space?
Failed to move the current attachment directory `<some path>` to the new location of `<some other path>`.	The upgrade task could not move the directory. Does the server user have sufficient permission to perform this operation in the indicated directory?

Configuring a WebDAV client for Confluence

WebDAV allows users to access Confluence content via a WebDAV client, such as 'My Network Places' in Microsoft Windows. Provided that the user has permission, they will be able to read and write to spaces, pages and attachments in Confluence. Users will be asked to log in and the standard Confluence content access permissions will apply to the equivalent content available through the WebDAV client.

Introduction to Confluence's WebDAV Client Integration

By default, all WebDAV clients have permission to write to Confluence. Write permissions include the ability for a WebDAV client to create, edit, move or delete content associated with spaces, pages and attachments in a Confluence installation.

On the '**WebDAV Configuration**' screen in the Confluence Administration Console, you can:

- Deny a WebDAV client write permissions to a Confluence installation using a regular expression (regex).
- Disable or enable strict path checking.
- Enable or disable access to specific virtual files/folders.

Note:

- The 'WebDav Configuration' page is only be available if the WebDAV plugin has been enabled. Refer to Installing Plugins and Macros for more information on enabling Confluence plugins. Note that this plugin is bundled with Confluence, and can be enabled or disabled by the System Administrator.
- The settings on the 'WebDav Configuration' page do **not** apply to external attachment storage configuration.

On this page:

⚠ *The information on this page does not apply to Atlassian OnDemand sites with multiple apps. If you are using Confluence-only OnDemand, the information does apply.*

Restricting WebDAV Client Write Access to Confluence

In earlier versions of the WebDAV plugin, separate options for restricting a WebDAV client's write permissions (that is, create/move, edit and delete actions), were available. However, in the current version of this plugin, they have been simplified and combined into a general write permission restriction that covers all of these actions.

WebDAV clients are now denied write permission to your Confluence installation by setting a regex that matches specific content within the WebDAV client's user agent header. Upon setting a regex, it will be added to a list of restricted WebDAV clients. Any WebDAV clients whose user agent header matches a regex in this list will be denied write permission to your Confluence installation.

Example: A PROPFIND method header generated by a Microsoft Web Folder WebDAV client, showing the user agent header field:

```
PROPFIND
/plugins/servlet/confluence/default
HTTP/1.1
Content-Language: en-us
Accept-Language: en-us
Content-Type: text/xml
Translate: f
Depth: 1
Content-Length: 489
User-Agent: Microsoft Data Access Internet
Publishing Provider DAV
Host: 127.0.0.1:8082
Connection: Keep-Alive
```

> ℹ Unlike earlier versions of the WebDAV plugin which could only restrict write permissions for **all** WebDAV clients, the current version of this plugin allows you to restrict write permissions to specific WebDAV clients selectively.

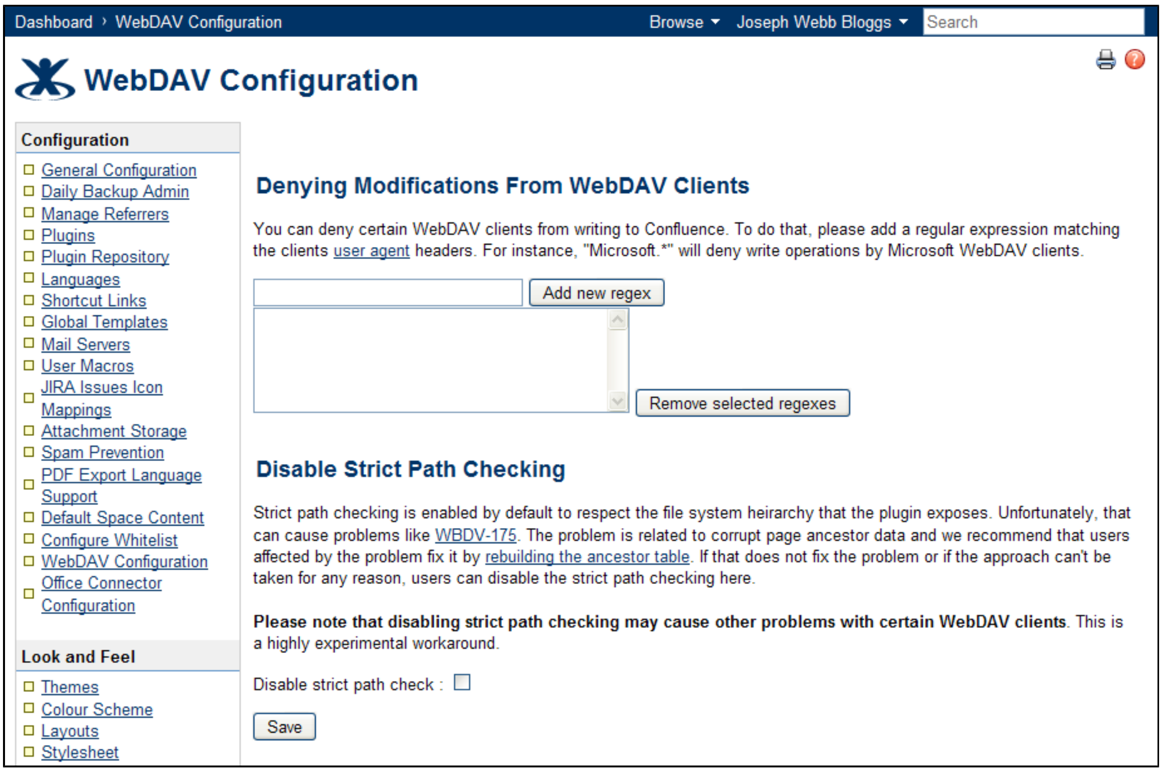
To restrict a WebDAV client's write access permissions to your Confluence installation,

1. Choose **Browse** > **Confluence Admin**.
2. Click '**WebDav Configuration**' under 'Configuration' in the left panel. The 'WebDAV Configuration' page is displayed.
3. Enter a regex that matches a specific component of the user agent header sent by the WebDAV client you want to restrict.
4. Click the '**Add new regex**' button. The regex is added to the list of restricted WebDAV clients. ℹ You can repeat steps 3 and 4 to add a regex for each additional WebDAV client you want to restrict.
5. Click the '**Save**' button to save the configuration changes.

To restore one or more restricted WebDAV client's write access permissions to your Confluence installation,

1. Choose **Browse** > **Confluence Admin**.
2. Click '**WebDav Configuration**' under 'Configuration' in the left panel. The 'WebDAV Configuration' page is displayed.
3. Select the regex(es) from the list that match(es) the user agent header sent by the restricted WebDAV client(s) you want to restore.
4. Click the '**Remove selected regexes**' button. The regexes you had selected are removed from the list of restricted WebDAV clients.
5. Click the '**Save**' button to save the configuration changes.

Screenshot: WebDAV configuration



Dashboard › WebDAV Configuration   Browse ▾ Joseph Webb Bloggs ▾ Search

WebDAV Configuration

Configuration

- □ General Configuration
- □ Daily Backup Admin
- □ Manage Referrers
- □ Plugins
- □ Plugin Repository
- □ Languages
- □ Shortcut Links
- □ Global Templates
- □ Mail Servers
- □ User Macros
- □ JIRA Issues Icon Mappings
- □ Attachment Storage
- □ Spam Prevention
- □ PDF Export Language Support
- □ Default Space Content
- □ Configure Whitelist
- □ WebDAV Configuration
- □ Office Connector Configuration

Look and Feel

- □ Themes
- □ Colour Scheme
- □ Layouts
- □ Stylesheet

Denying Modifications From WebDAV Clients

You can deny certain WebDAV clients from writing to Confluence. To do that, please add a regular expression matching the clients user agent headers. For instance, "Microsoft.*" will deny write operations by Microsoft WebDAV clients.

Add new regex

Remove selected regexes

Disable Strict Path Checking

Strict path checking is enabled by default to respect the file system heirarchy that the plugin exposes. Unfortunately, that can cause problems like WBDV-175. The problem is related to corrupt page ancestor data and we recommend that users affected by the problem fix it by rebuilding the ancestor table. If that does not fix the problem or if the approach can't be taken for any reason, users can disable the strict path checking here.

Please note that disabling strict path checking may cause other problems with certain WebDAV clients. This is a highly experimental workaround.

Disable strict path check : □

Save

Disabling Strict Path Checking

If you observe any idiosyncrasies with your WebDAV client, such as a folder that does exist on your Confluence site but is missing from the client, you can disable the WebDAV plugin's strict path checking option, which may minimise these problems.

To disable the WebDAV plugin's strict path checking option,

1. Choose **Browse** > **Confluence Admin**.
2. Click '**WebDav Configuration**' under 'Configuration' in the left panel. The 'WebDAV Configuration' page is displayed.
3. Clear the 'Disable strict path check' check box.
   ℹ You can re-enable this option at a later point in time by simply selecting this check box.
4. Click the '**Save**' button to save this configuration change.

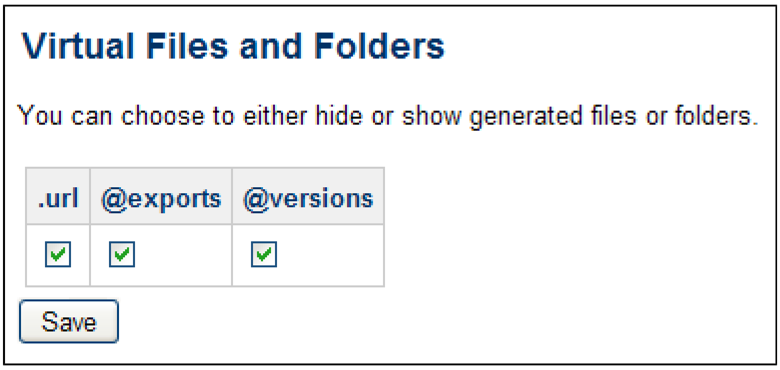
Virtual Files and Folders

In the unlikely event that you observe any problems with the WebDAV client's performance or stability, you can enable access to automatically generated (that is, virtual) files and folders.

By default, these options are hidden on the 'WebDAV Configuration' page. To make them visible, you must append the parameter `?hiddenOptionsEnabled=true` to the end of your URL and reload the page. For example:

```
<Confluence base
URL>/admin/plugins/webdav/config.action?hiddenOptionsEnabled=
true
```

Screenshot: The Hidden Virtual Files and Folders Option



Virtual Files and Folders

You can choose to either hide or show generated files or folders.

.url	@exports	@versions
☑	☑	☑

To enable or disable access to virtual files and folders,

1. Choose **Browse** > **Confluence Admin**.
2. Click '**WebDav Configuration**' under 'Configuration' in the left panel. The 'WebDAV Configuration' page is displayed.
3. Amend your URL as described in the note above and reload the 'WebDav Configuration' page.
4. Select or clear the check box options in the 'Virtual Files and Folders' section as required.
5. Click the '**Save**' button to save the configuration changes.

Using a WebDAV Client to Work with Pages

The following sections tell you how to set up a WebDAV client natively for a range of different operating systems. WebDAV clients typically appear as drives in your operating system's file browser application, such as Windows Explorer in Microsoft Windows, or Konqueror in Linux.

Setting Up a WebDAV Client in Microsoft Windows

This section covers the two methods for configuring a WebDAV client natively in Microsoft Windows:

- As a network drive
- As a web folder

If possible, use the network drive method as this will enable more comprehensive WebDAV client interaction with Confluence than that provided by a web folder. However, your Confluence instance must meet several environmental constraints if you use this method. If you cannot configure your instance to meet these requirements, then use the web folder method or third-party WebDAV client software.

✓ If you run into any problems with the procedures in this section, please refer to the Troubleshooting WebDAV page.

Windows Network Drive

To map a Confluence WebDAV client network drive, your Confluence instance must be configured so that *all* of the following criteria is met:

- Uses HTTP (not HTTPS)
- Listens on port 80 (not 8080, which is the default port value used by the popular application server Apache Tomcat that runs many Confluence EAR / WAR installations, or 8090, the default for Confluence distributions)
- Has no context root
- There is an issue (WBDV-208) that can prevent Network Drives from being mapped. Please use the Network Folders steps below as a workaround.

ℹ The reason for these restrictions results from limitations in Microsoft's Mini-Redirector component. For more information, please refer to Microsoft's server discovery issue.

To map a Confluence WebDAV client network drive in Microsoft Windows,

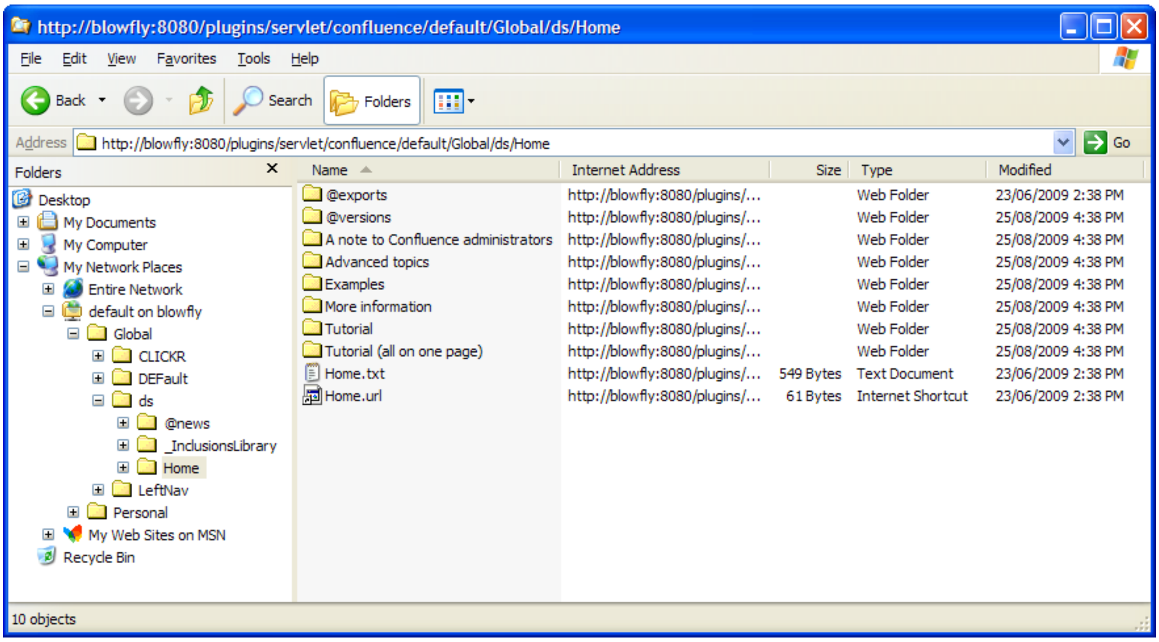
1. In Windows XP, go to **My Computer -> Tools menu -> Map Network Drive**.
   In Windows Vista, go to **Computer -> Map Network Drive**.
   The 'Map Network Drive' dialog box opens.
2. Specify the following input to map the WebDAV client as a network drive:
   - **Drive:** `<Any drive letter>` (for example, `Z:`)
   - **Folder:** `\\<hostname>\webdav` (for example, `\\localhost\webdav`)
3. Click '**Finish**'.
   ℹ When prompted for login credentials, specify your Confluence username and password.

Windows Web Folder

To map a Confluence WebDAV client web folder in Windows XP,

1. Go to **My Network Places** and choose '**Add a network place**'. The 'Add Network Place Wizard' opens.
2. Click '**Next**', ensure that '**Choose another network location**' is selected and then click '**Next**' again.
3. In the 'Internet or network address' field, enter the URL for the Confluence WebDAV location (for example, `http://<confluence server url>/confluence/plugins/servlet/confluence/default` or `http://<confluence server url>/plugins/servlet/confluence/default`) and then click '**Next**'.
   ℹ When prompted for login credentials, specify your Confluence username and password.
4. Provide a meaningful name for your web folder and proceed with the remainder of the wizard.
5. Click '**Finish**'.

Screenshot: A Confluence WebDAV Client Web Folder in Windows XP



Name	Internet Address	Size	Type	Modified
@exports	http://blowfly:8080/plugins/...		Web Folder	23/06/2009 2:38 PM
@versions	http://blowfly:8080/plugins/...		Web Folder	25/08/2009 4:38 PM
A note to Confluence administrators	http://blowfly:8080/plugins/...		Web Folder	25/08/2009 4:38 PM
Advanced topics	http://blowfly:8080/plugins/...		Web Folder	25/08/2009 4:38 PM
Examples	http://blowfly:8080/plugins/...		Web Folder	25/08/2009 4:38 PM
More information	http://blowfly:8080/plugins/...		Web Folder	25/08/2009 4:38 PM
Tutorial	http://blowfly:8080/plugins/...		Web Folder	25/08/2009 4:38 PM
Tutorial (all on one page)	http://blowfly:8080/plugins/...		Web Folder	25/08/2009 4:38 PM
Home.txt	http://blowfly:8080/plugins/...	549 Bytes	Text Document	23/06/2009 2:38 PM
Home.url	http://blowfly:8080/plugins/...	61 Bytes	Internet Shortcut	23/06/2009 2:38 PM

To map a Confluence WebDAV client web folder in Windows Vista,

ℹ This procedure is very similar to the one for Windows XP. However, the following procedure includes the slight interface differences that are specific to Windows Vista.

1. Open the 'Map Network Drive' dialog box (refer to first step of the procedure above for mapping a network drive) and choose '**Connect to a Web site that you can use to store your documents and pictures**'. The 'Add Network Location' wizard opens.
2. Click '**Next**', ensure that '**Choose a custom network location**' is selected and then click '**Next**' again.
3. In the 'Internet or network address' field, enter the URL for the Confluence WebDAV location (for example, `http://<confluence server url>/confluence/plugins/servlet/confluence/default` or `http://<confluence server url>/plugins/servlet/confluence/default`) and then click '**Next**'.
   ℹ When prompted for login credentials, specify your Confluence username and password.
4. Provide a meaningful name for your network location/web folder and proceed with the remainder of the wizard.
5. Click '**Finish**'.

Setting up a WebDAV client in Linux or Solaris

There are many tools and mechanisms available for configuring WebDAV clients in these operating systems. Therefore, we have chosen to demonstrate this using the file manager Konqueror, which is part of the Linux K Desktop Environment.

To set up a Confluence WebDAV client in Konqueror,

1. Open Konqueror.
2. In the 'Location' field, enter the URL for the Confluence WebDAV location using the 'protocol' `webdavs` (for example, `webdavs://<confluence server url>/confluence/plugins/servlet/confluence/default` or `webdavs://<confluence server url>/plugins/servlet/confluence/default`) and press `Enter`.
   ℹ If prompted for login credentials, specify your Confluence username and password.
   You should be able to click to load many, but not all files. In practice, you would normally save a modified file locally, then drag it to the Konqueror window to upload it to Confluence.

Known Issues

Please refer to the WebDAV plugin documentation for a description of the known issues and suggested workarounds.

RELATED TOPICS

No content found for label(s) data-storage,webdav.

Administrators Guide Home Confluence Documentation Home

Configuring Quick Navigation

When a user is searching Confluence (see Using the Quick Navigation Aid) the quick navigation aid automatically offers a dropdown list of pages and other items, matched by title to the search query. By default, this feature is enabled, with the maximum number of simultaneous quick navigation requests set to 40. However, these options can be modified as described below.

> The maximum number of simultaneous quick navigation requests defines the maximum number of individuals who can use this feature simultaneously on the same Confluence server. If your Confluence server serves a large number of individuals who use this feature regularly, some of whom are being denied access to it, you may wish to increase this value.

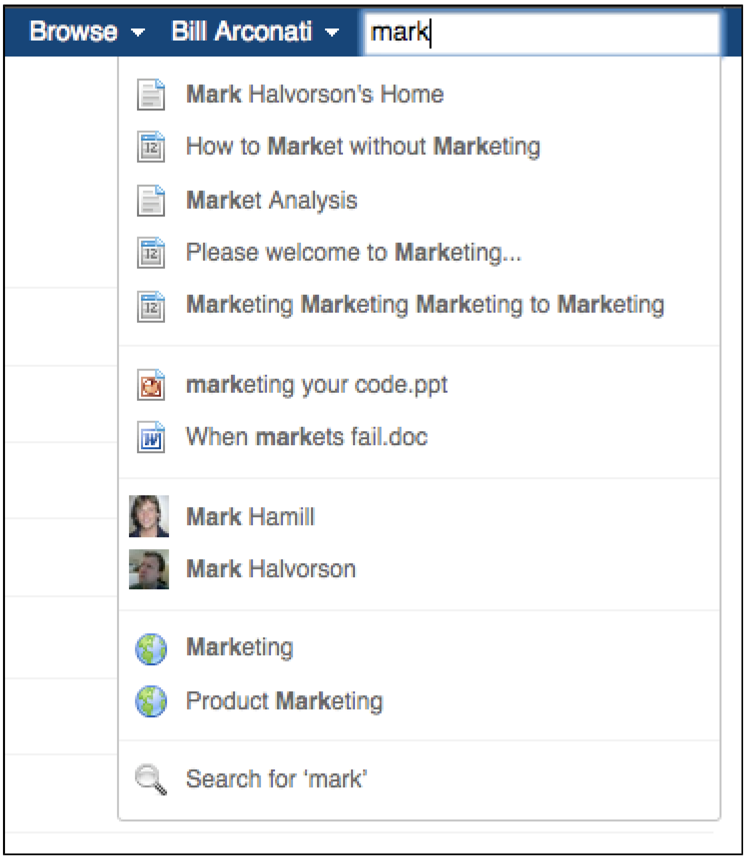
> *The information on this page does not apply to Confluence OnDemand.*

To modify the quick navigation feature's options,

1. Choose **Browse** > **Confluence Admin**.
2. Select '**General Configuration**' in the left-hand panel.
3. In the '**General Configuration**' screen, click '**Edit**'.
4. To disable this feature, select '**Off**' beside '**Quick Navigation**'.
5. To modify the maximum number of simultaneous quick navigation requests, enter the appropriate number in the field beside '**Max Simultaneous Requests**'.
6. Click '**Save**'.

The following screenshot demonstrates the user interface of the quick navigation aid.

Screenshot: The quick navigation aid showing titles matching the query 'mark'



RELATED TOPICS

Searching Confluence

Administrators Guide Home Confluence Documentation Home

Enabling OpenSearch

With OpenSearch autodiscovery, you can add Confluence search to your Firefox or IE7 search box (see Searching Confluence from your Browser's Search Box). By default, OpenSearch autodiscovery is enabled. This feature can be enabled or disabled as described below.

To enable or disable OpenSearch autodiscovery,

1. Choose **Browse** > **Confluence Admin**.
2. Select '**General Configuration**' in the left-hand panel.
3. In the '**General Configuration**' screen, click '**Edit**'.
4. Select '**On**' beside '**Open Search**' to enable this feature, or '**Off**' to disable it.
5. Click '**Save**'.

RELATED TOPICS

Searching Confluence

Administrators Guide Home Confluence Documentation Home

Enabling the Did You Mean Feature

When you perform a full Confluence search, Confluence may offer you an alternative spelling of your search query. The alternative spelling will appear next to the words 'Did you mean'. By default, this feature is disabled. You can enable it as described below.

To enable the 'Did You Mean' feature,

1. Choose **Browse** > **Confluence Admin**.
2. Select '**General Configuration**' in the left-hand panel.
3. In the '**General Configuration**' screen, click '**Edit**'.
4. Select '**On**' beside '**Did You Mean**'.
   ℹ If you have no 'Did you mean' feature index or you have not yet created it, this option will not be available. To create this index, click '**build the did-you-mean index**' and on the subsequent page, click '**Build**' in the '**Did You Mean Index**' section. Then return to the '**General Configuration**' screen in Edit mode.
5. Click '**Save**'.

Languages and Locales

The 'Did You Mean' feature supports only the English language. In addition, the 'Did You Mean' index requires the built-in UK-English locale (**en_UK**). If your Confluence site uses a different language pack, such as English (US), the 'Did You Mean' feature will not work. You will see an error message like this:

> *For Did You Mean both the indexing language and the global default language must be set to English.*

For more information about how the 'Did You Mean' feature works, please refer to the user guide.

You can track the request to support other languages by watching issue CONF-14768.

RELATED TOPICS

Searching Confluence

Administrators Guide Home Confluence Documentation Home

Enabling the Remote API

Confluence provides XML-RPC and SOAP remote APIs. You need to enable the APIs from the **Administration Console** before you can access Confluence remotely.

ℹ You need to have System Administrator permissions in order to perform this function.

To enable the remote API,

1. Choose **Browse** > **Confluence Admin**.
2. Select '**General Configuration**' in the left-hand panel.
3. Click '**Edit**' next to '**Site Configuration**'.
4. Select '**On**' next to '**Remote API (XML-RPC & SOAP)**'.
5. Click '**Save**' to retain your changes.

⚠ *Some functionality described on this page is restricted in **Confluence OnDemand**.*

RELATED TOPICS

- Confluence Remote API Reference

Enabling Threaded Comments

Comments on pages or blog posts are displayed in one of two views:

- **Threaded**: Shows the comments in a hierarchy of responses. Each reply to a comment is indented to indicate the relationships between the comments.
- **Flat**: Displays all the comments in one single list and does not indicate the relationships between comments.

By default, comments are displayed in **threaded** mode. A Confluence Administrator (see Global Permissions Overview) can enable or disable the threaded view for the entire Confluence site.

To enable or disable the threaded view:

1. Choose **Browse** > **Confluence Admin**.
2. Select **General Configuration** in the left-hand panel.
3. Click **Edit**.
4. Check **Threaded Comments** to enable threaded mode. Clear the check box to disable threaded mode and display all comments in flat mode.
5. Click **Save**.

Related pages:

- Commenting on pages and blog posts
- Confluence Administrator's Guide

Enabling Trackback

When Trackback is enabled, any time you link to an external webpage that supports Trackback Autodiscovery, Confluence will send a trackback ping to that page to inform it that it has been linked to.

Confluence pages also support Trackback Autodiscovery and when Trackback is enabled, can receive trackback pings sent by other sites.

To enable trackback,

1. Choose **Browse** > **Confluence Admin**.
2. Select '**General Configuration**' in the left panel.
3. In the '**Feature Settings**' screen, click '**Edit**'.
4. Select "**On**' beside '**Trackback**' and click '**Save**'.

RELATED TOPICS

No content found for label(s) security-options.

Administrators Guide Home Confluence Documentation Home

Other Settings

- Configuring Attachment Size
- Configuring Character Encoding
- Configuring HTTP Timeout Settings
- Configuring Indexing Language
- Configuring Number Formats
- Configuring Shortcut Links
- Configuring Time and Date Formats

Configuring Attachment Size

Confluence gives you the option of limiting the maximum size of a single file attachment. Confluence administrators should keep in mind that the amount of disk space used by Confluence is directly proportional to the number and size of attachments put into the system.

To configure the maximum size allowed for an attachment:

1. Go to the '**Administration Console**' and click '**General Configuration**' in the left-hand panel.
2. Click '**Edit**' on the '**General Configuration**' screen.
3. Enter the maximum size next to '**Attachment Maximum Size**'. The default is 10 MB.
4. '**Save**' your changes.

To configure the maximum 'index-able size of attachments':

By default, large attachment is defined as greater than 1 MB.
The threshold for attachments that won't get excerpts can be modified using the system property `atlassian.indexing.contentbody.maxsize`, which takes a size in bytes.

Example

To specify 250 kb you would use the following JVM parameter:
`-Datlassian.indexing.contentbody.maxsize=256000`

Outcomes of Limiting Attachment Indexing Size

Limiting the size of attachment indexing has the following effects:

- Decreases the size of the index when large attachments are present.
- Decreases the memory used in indexing large attachments.
- Prevent excerpts of large attachments being displayed in search results.

For more details, please refer to the following JIRA issue.

Related Topics

No content found for label(s) other-settings.

Administrators Guide Home Confluence Documentation Home

Configuring Character Encoding

Confluence uses UTF-8 character encoding to deliver its pages.

⚠ While it is possible to change the character encoding, unless you are certain of what you are doing, we recommend that you leave this as it is.

To change the character encoding:

1. Go to the '**Administration Console**' and click on '**General Configuration**' in the left panel.
2. Click '**Edit**' at the bottom of the '**Formatting and International Settings**' screen. For Confluence version earlier than 2.6.2, look for the '**Options and Settings**' screen.
3. Beside '**Encoding**', enter the new character encoding of your choice.
4. '**Save**' your changes.

Related Links

Joel Spolsky: The Absolute Minimum Every Software Developer Absolutely, Positively Must Know About Unicode and Character Sets (No Excuses!)

Related Topics

No content found for label(s) other-settings.

Administrators Guide Home Confluence Documentation Home

Configuring HTTP Timeout Settings

When macros such as the RSS Macro make HTTP requests to servers which are down, a long timeout value is used. You can set this timeout value through a system parameter to avoid this.

To configure the HTTP Timeout Settings:

1. Choose **Browse** > **Confluence Admin**.
2. Select '**General Configuration**' under the 'Configuration' heading in the left-hand panel.
3. Find the '**Connection Timeouts**' section in the lower portion of the screen.
4. Click '**Edit**' to adjust the settings:
    - **Adjust External connections enabled**: This setting allows system administrators to disable external connections so macros like the RSS Macro wont be allowed to make connections to an external server. It's provides protection against external servers providing insecure HTML, timing out or causing performance problems. The default setting is 'true'.
    - **Connection Timeout (milliseconds)**: Sets the maximum time for a connection to be established. A value of zero means the timeout is not used. The default setting is ten seconds (10000).
    - **Socket Timeout (milliseconds)**: Sets the default socket timeout (SO_TIMEOUT) in milliseconds, which is the maximum time Confluence will wait for data. A timeout value of zero is interpreted as an infinite timeout. The default setting is ten seconds (10000).

Configuring Indexing Language

Changing the indexing language defined in Confluence may improve the accuracy of Confluence search results, if the majority of the content of your site is in some language other than English. Confluence supports content indexing in English (default), German, Russian, Chinese, CJK, Custom Japanese, French, Brazilian, Czech and Greek.

To configure a different indexing language:

1. Go to the '**Administration Console**' and click '**General Configuration**' in the left-hand panel.
2. Click any of the '**Edit**' links..
3. Select the '**Indexing Language**' from the dropdown list in the '**Formatting and International Settings**' section.
4. Click '**Save**'.

Related Topics

Choosing a Default Language
Installing a Language Pack
Content Index Administration
Rebuild the Content Indices from scratch
Creating a Lowercase Page Title Index

Configuring Number Formats

To change the number formats:

1. Go to the '**Administration Console**' and click on '**General Configuration**' in the left panel.

2. Click '**Edit**' at the bottom of the '**Options and Settings**' screen.

- There are two number format settings:
  - Long Number Format
  - Decimal Number Format

3. Change the formats using the guidelines in this document.

4. '**Save**' your changes.

Related Topics

No content found for label(s) other-settings.

Administrators Guide Home Confluence Documentation Home

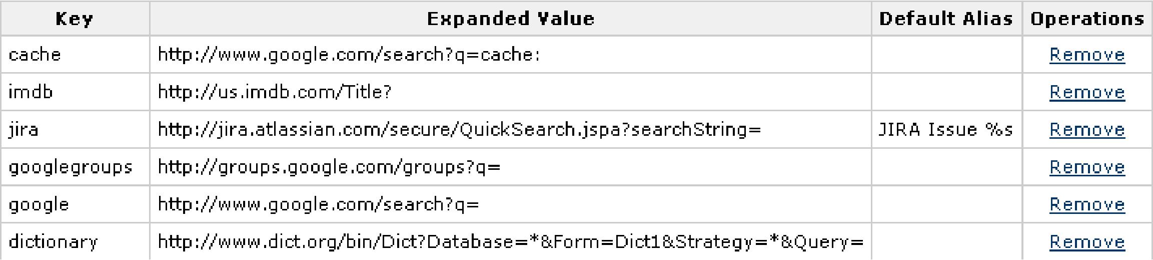
Configuring Shortcut Links

Shortcut links provide a quick way of linking to resources that are frequently referenced from Confluence. When you create a shortcut link, you assign a key to an URL so that, when editing, a user can type just the key instead of the complete URL.

Here is an example:

Most Google searches look like this: `http://www.google.com/search?q=`. If you create a shortcut for this search with the key 'google', every time a user needs to use `http://www.google.com/search?q=`**`searchterms`**, they can just type `[`**`searchterms`**`@google]` instead.

Here is a screenshot showing the shortcuts currently defined on http://confluence.atlassian.com:



Key	Expanded Value	Default Alias	Operations
cache	http://www.google.com/search?q=cache:		Remove
imdb	http://us.imdb.com/Title?		Remove
jira	http://jira.atlassian.com/secure/QuickSearch.jspa?searchString=	JIRA Issue %s	Remove
googlegroups	http://groups.google.com/groups?q=		Remove
google	http://www.google.com/search?q=		Remove
dictionary	http://www.dict.org/bin/Dict?Database=*&Form=Dict1&Strategy=*&Query=		Remove

Shortcut links are added and maintained by Confluence administrators from the **Administration Console**.

Creating Shortcut Links

To create a shortcut link:

1. Go to the Administration Console and click **Shortcut Links** in the left panel.
2. Enter a **Key** for your shortcut. This is the shortcut name a user will use to reference the URL.
3. Enter the **Expanded Value**. This is the URL for the link. You can use '%s' in the URL to specify where the user's input is inserted. If there is no '%s' in the URL, the user's input will be put at the end.
4. *(Optional. Available in Confluence version 2.3 and later.)* Enter a **Default Alias**. This is the text of the link which will be displayed on the page where the shortcut is used, with the user's text being substituted for '%s'.
5. Click **Save**.

Using Shortcut Links

Enter a shortcut link on the **Advanced** tab of the Insert Link dialog. See Linking to Pages for details.

Specify in the link what should be appended to the end of the shortcut URL, followed by an at-sign (@) and the key of the shortcut. Shortcut names are case-insensitive. So, for example, using the keys shown in the above screenshot:

To link to...	Type this	Resulting URL	Demonstration
a JIRA issue	CONF-1000@JIRA	http://jira.atlassian.com/secure/QuickSearch.jspa?searchString=CONF-1000	CONF-1000
a Google search	Atlassian Confluence@Google	http://www.google.com/search?q=Atlassian+Confluence	Atlassian Confluence@Google

Deleting Shortcut Links

Shortcut links are listed on the **Shortcut Links** tab of the Administration Console. Click **Remove** to delete the shortcut.

Related Topics

Administrators Guide Home Confluence Documentation Home

Configuring Time and Date Formats

Confluence allows you to localise the formats used to display dates and times within the web interface. The settings use the syntax of Java's SimpleDateFormat class (described below).

To change the time and date formats:

1. Go to the '**Administration Console**' and click on '**General Configuration**' in the left panel.

2. Click '**Edit**' at the bottom of the '**Options and Settings**' screen.

    - There are three time and date format settings:
        - Time Format : displaying only the time of day (for example, when each news item is posted)
        - Date Time Format : displaying both the date and the time of day (for example, in historical versions of pages)
        - Date Format : displaying only the date (for example, the creation and most recent modification dates of pages)

3. Change the formats using the guidelines in this document.

4. '**Save**' your changes.

Related Links

- Java 1.4.2 SimpleDateFormat API

Related Topics

No content found for label(s) other-settings.

Administrators Guide Home Confluence Documentation Home

Configuring System Properties

This page describes how to set Java properties and options on startup for Confluence Stand-alone and EAR/WAR versions.

✓ See Fix Out of Memory Errors by Increasing Available Memory for specific instructions for OutOfMemory Errors.

On this page:

⚠ *The information on this page does not apply to Confluence OnDemand.*

Linux

To Configure System Properties in Linux Installations,

1. From `<confluence-install>/bin` (Stand-alone) or `<Tomcat-home>/bin` (EAR-WAR installation), open **setenv.sh**.
2. Find the section **JAVA_OPTS=**
3. Refer to the list of parameters below.

ℹ Add all parameters in a space-separated list, inside the quotations.

Windows (starting from .bat file)

To Configure System Properties in Windows Installations When Starting from the .bat File,

1. From `<confluence-install>/bin` (Stand-alone) or `<Tomcat-home>/bin` (EAR-WAR installation), open **setenv.bat**.
2. Find the section **set JAVA_OPTS=%JAVA_OPTS%**
3. Refer to the list of parameters below.

ℹ Add all parameters in a space-separated list. Make sure to keep the string %JAVA_OPTS% in place.

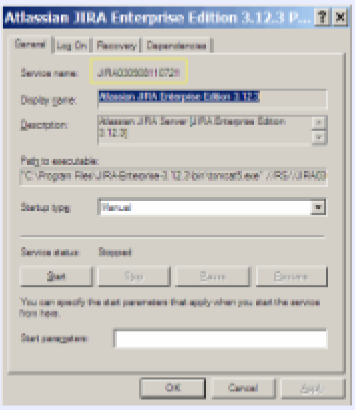
Windows Service

There are two ways to configure system properties when you Start Confluence Automatically on Windows as a Service, either via command line or in the Windows Registry

Setting Properties for Windows Services via Command Line

Setting Properties for Windows Services via Command Line

1. Identify the name of the service that Confluence is installed as in Windows (`Control Panel > Administrative Tools > Services`):

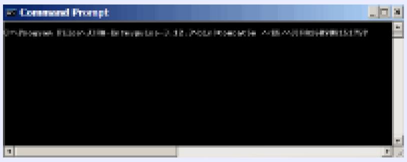


Service name: JIRA030908110721
Display name: Atlassian JIRA Enterprise Edition 3.12.3
Description: Atlassian JIRA Server (JIRA Enterprise Edition 3.12.3)
Path to executable: "C:\Program Files\JIRA-Enterprise-3.12.3\bin\tomcat5.exe" //RS//JIRA03
Startup type: Manual
Service status: Stopped
You can specify the start parameters that apply when you start the service from here.
Start parameters:

   ⓘ In the above example, the **SERVICENAME** is: `JIRA030908110721`. Find the Confluence equivalent.
2. Open the command window from `Start >> Run >> type in 'cmd' >> Enter`
3. `cd` to the `bin` directory of your Confluence instance, or the `bin` directory of your Tomcat installation if your are running Confluence EAR/WAR.
4. Run:

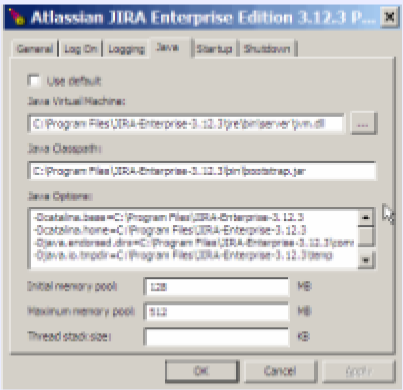
```
tomcat6w //ES//%SERVICENAME%
```

   .
   ⓘ In the above example, it would be `tomcat6w //ES//JIRA030908110721`



```
C:\Program Files\JIRA-Enterprise-3.12.3\bin>tomcat5w //ES//JIRA030908110721
```

5. Click on the `Java` tab to see the list of current start-up options:



□ Use default
Java Virtual Machine: C:\Program Files\JIRA-Enterprise-3.12.3\jre\bin\server\jvm.dll
Java Classpath: C:\Program Files\JIRA-Enterprise-3.12.3\bin\bootstrap.jar
Java Options:

```
-Dcatalina.base=C:\Program Files\JIRA-Enterprise-3.12.3
-Dcatalina.home=C:\Program Files\JIRA-Enterprise-3.12.3
-Djava.endorsed.dirs=C:\Program Files\JIRA-Enterprise-3.12.3\com
-Djava.io.tmpdir=C:\Program Files\JIRA-Enterprise-3.12.3\temp
```

Initial memory pool: 128 MB
Maximum memory pool: 512 MB
Thread stack size: KB

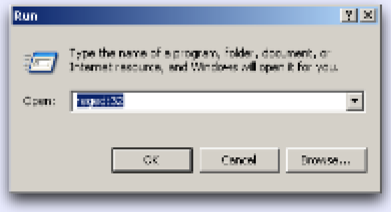
6. Append any new option on its own new line by adding to the end of the existing Java Options. Refer to the list of parameters below.

Setting Properties for Windows Services via the Windows Registry

In some versions of Windows, there is no option to add Java variables to the service. In these cases, you must add the properties by viewing the option list in the registry.

To Set Properties for Windows Services via the Windows Registry,

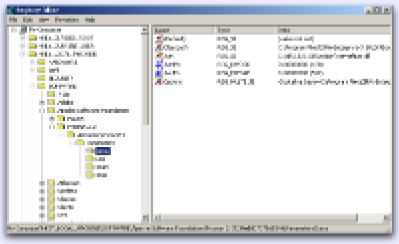
1. Go to {{Start >> Run, and run "regedit32.exe".



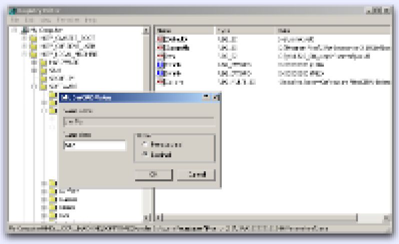
Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: regedit32

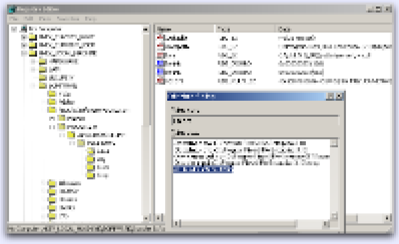
2. Find the Services entry:
32-bit: `HKEY_LOCAL_MACHINE >> SOFTWARE >> Apache Software Foundation >> Procrun 2.0 >> Confluence`
64-bit: `HKEY_LOCAL_MACHINE >> SOFTWARE >> Wow6432Node >> Apache Software Foundation >> Procrun 2.0 >> Confluence`



3. To change existing properties, especially increasing Xmx memory, double-click the appropriate value.



4. To change additional properties, double-click options.



5. Refer to the list of parameters below. Enter each on a separate line.

Verifying Your Settings

To see what Confluence is using, check Viewing System Properties.

Recognised System Properties

Property	Since	Default Value	Module...	Effect
`atlassian.forceSchemaUpdate`	1.0	`false`	atlassian-config	By default, Confluence will only run its database schema update when it detects that it has been upgraded. This flag will force Confluence to perform the schema update on system startup.
`confluence.home`	1.0	Any filesystem path	Confluence and atlassian-config	If this system property is set, Confluence will ignore the contents of the `confluence-init.properties` file, and use this property as the setting for the Confluence Home directory.
`confluence.devmode`	1.0	`false`	Confluence	Enables additional debugging options that may be of use to Confluence developers (additionally it changes spring bean creation to use lazy initialization by default to decrease startup time). Do not enable this flag on a production system.
`confluence.disable.mailpolling`	2.4	`false`	Confluence	If set to "true", will prevent Confluence from retrieving mail for archiving within spaces. Manually triggering "check for new mail" via the web UI will still work. This property has no effect on outgoing mail

`confluence.i18n.reloadbundles`	1.0	`true`	Confluence	Setting this property will cause Confluence to reload its i18n resource bundles every time an internationalised string is looked up. This can be useful when testing translations, but will make Confluence run *insanely slowly*.
`confluence.ignore.debug.logging`	1.0	`true`	Confluence	Confluence will normally log a severe error message if it detects that DEBUG level logging is enabled (as DEBUG logging generally causes a significant degradation in system performance). Setting this property will suppress the error message.
`confluence.jmx.disabled`	3.0	`false`	Confluence	If set to "true", will disable Confluence's JMX monitoring. This has the same effect as setting the "enabled" property to false in `WEB-INF/classes/jmxContext.xml`
`confluence.optimize.index.modulo`	2.2	`20`	Confluence	Number of index queue flushes before the index is optimised.

`confluence.plugins.bundled.disable`	2.9	`false`	Confluence	Starts confluence without bundled plugins. May be useful in a development environment to make Confluence start quicker, but since bundled plugins are necessary for some of Confluence's core functionality, this property should not be set on a production system.
`atlassian.mail.fetchdisabled`	3.5	`false`	Confluence	Disables mail fetching services for IMAP and POP
`atlassian.mail.senddisabled`	3.5	`false`	Confluence and atlassian-mail	Disables sending of mail
`atlassian.disable.caches`	2.4	`true`	atlassian-plugins, atlassian-cache-servlet	Setting this property will disable conditional get and expires: headers on some web resources. This will significantly slow down the user experience, but is useful in devlopment if you are frequently changing static resources and don't want to continually flush your browser cache.
`confluence.html.encode.automatic`	2.9		Confluence	Setting this property forces the antixss encoding on or off, overriding the behaviour dictated by settings. The default behaviour differs between Confluence versions.

`org.osgi.framework.bootdelegation`	2.10	empty	atlassian-plugins	Comma-separated list of package names to provide from application for OSGi plugins. Typically required when profiling Confluence. For example: "com.jprofiler.**,com.yourkit.**".
`confluence.diff.pool.size`	3.1	`20`	Confluence	Maximum number of concurrent diffs. When that number is exceeded, additional attempts by RSS feeds to create diffs are ignored and logged. (The RSS requests succeed, they are just missing diffs).
`confluence.diff.timeout`	3.1	`1000`	Confluence	Number of milliseconds to wait for a diff operation (comparing two page versions) to complete before aborting with an error message.

`atlassian.user.experimentalMapping`	2.10	`false`	Confluence	Setting this property changes the relationship between local users and local groups to reduce performance degradation when adding a local user to a local group with a large number of users. Please note, setting this property can slow down other user management functions. We recommend that you set it only if you are experiencing performance problems when adding local users to large local groups. Please refer to CONF-12319, fixed in Confluence 3.1.1.
`confluence.import.use-experimental-importer`	3.2	`false`	Confluence	Setting this property changes Confluence to use the Experimental XML Importer. It is designed to be a more stable implementation but, at the time of the release of 3.2, the importer is largely untested and thus not supported.
`atlassian.webresource.disable.minification`	3.3	`false`	atlassian-plugins	Disables automatic minification of JavaScript and CSS resources served by Confluence.

`index.queue.thread.count`	3.3	*See "Effect"*	Confluence	Sets the number of threads to be used for the reindex job. The value has to be in the range of 1 to 10 (inclusive), i.e. at least one thread but no more than 10 threads will be used. There is no default value, i.e. • If you don't set `index.queue.thread.count`, the number of threads to be used are calculated based on the number of objects that need to be reindexed and the number of processors available (a maximum of 10 threads will be used). • If you set `index.queue.thread.count=2`, then two threads will be used to reindex the content (regardless of the number of objects to be reindexed or the number of processors available) • If you set `index.queue.thread.count=200`, then ten threads (the maximum allowed) will be used to reindex the content.

`index.queue.batch.size`	3.3	1500	Confluence	Size of batches used by the indexer. Reducing this value will reduce the load that the indexer puts on the system, but indexing takes longer. Increasing this value will cause indexing to be completed faster, but puts a higher load on the system. Normally this setting does not need tuning.
`password.confirmation.disabled`	3.4	`false`	Confluence	This property disables the password confirmation functionality that Confluence uses as an additional security measure. With this property set, Confluence will *not* require password confirmation for the following actions: administrative actions, change of email address and Captcha for failed logins. Disabling password confirmations is useful if you are using a custom authenticator.

`confluence.browser.language.enabled`	3.5	`true`	Confluence	Setting this property to "false" disables the detection of browser language headers, effectively restoring Confluence behaviour to that of earlier releases. Setting this property to "true" enables the detection of the language headers sent by the browser. Confluenc will change the UI language based on the browser headers. See documentation on how users can choose a language preference.
`upm.pac.disable`	Universal Plugin Manager 1.5	`false`	Universal Plugin Manager (UPM)	When this property is set to true, then UPM will not try to access the Atlassian Plugin Exchange. This is useful for application servers that do not have access to the Internet. See the UPM documentation.
`confluence.reindex.documents.to.pop`	3.5.9	`20`	Confluence	Indicates how many objects each indexing thread should process at a time during a full re-index. Please note that this number does not include attachments
`confluence.reindex.attachments.to.pop`	3.5.9	`10`	Confluence	Indicates how many attachments each indexing thread should process at a time during a full re-index.

`confluence.upgrade.active.directory`	3.5.11	`false`	Confluence	Forces Confluence to treat any LDAP directories it migrates as Active Directory, rather than relying on looking for sAMAccountName in the username attribute. This is necessary if you are upgrading from before Confluence 3.5, and need to use an attribute other than sAMAccountName to identify your users and are seeing `LDAP: error code 4 - Sizelimit Exceeded` exceptions in your logs. For more details, see Unable to Log In with Confluence 3.5 or Later Due to 'LDAP error code 4 - Sizelimit Exceeded'
`com.atlassian.logout.disable.session.invalidation`	4.0	`false`	Confluence	Disables the session invalidation on log out. As of 4.0 the default behaviour is to invalidate the JSession assigned to a client when they log out. If this is set to true the session is kept active (but the user logged out). This may be valuable when using external authentication systems, but should generally not be needed.

`officeconnector.spreadsheet.xlsxmaxsize`	4.0.5	2^{21}	Office Connector	Indicates the maximum size in bytes of an Excel file that can be viewed using the `viewxls` macro. If empty, the maximum size defaults to 2Mb. See CONF-21043 for more details.

RELATED TOPICS

Recognised System Properties
Fix Out of Memory Errors by Increasing Available Memory

Recognised System Properties

Confluence supports some configuration and debugging settings that can be enabled through Java system properties. System properties are usually set by passing the `-D` flag to the Java virtual machine in which Confluence is running. See the full instructions.

> ⚠ *The information on this page does not apply to Confluence OnDemand.*

Property	Since	Default Value	Module...	Effect
`atlassian.forceSchemaUpdate`	1.0	`false`	atlassian-config	By default, Confluence will only run its database schema update when it detects that it has been upgraded. This flag will force Confluence to perform the schema update on system startup.
`confluence.home`	1.0	Any filesystem path	Confluence and atlassian-config	If this system property is set, Confluence will ignore the contents of the `confluence-init.properties` file, and use this property as the setting for the Confluence Home directory.

`confluence.devmode`	1.0	`false`	Confluence	Enables additional debugging options that may be of use to Confluence developers (additionally it changes spring bean creation to use lazy initialization by default to decrease startup time). Do not enable this flag on a production system.
`confluence.disable.mailpolling`	2.4	`false`	Confluence	If set to "true", will prevent Confluence from retrieving mail for archiving within spaces. Manually triggering "check for new mail" via the web UI will still work. This property has no effect on outgoing mail
`confluence.i18n.reloadbundles`	1.0	`true`	Confluence	Setting this property will cause Confluence to reload its i18n resource bundles every time an internationalised string is looked up. This can be useful when testing translations, but will make Confluence run *insanely slowly*.

`confluence.ignore.debug.logging`	1.0	`true`	Confluence	Confluence will normally log a severe error message if it detects that DEBUG level logging is enabled (as DEBUG logging generally causes a significant degradation in system performance). Setting this property will suppress the error message.
`confluence.jmx.disabled`	3.0	`false`	Confluence	If set to "true", will disable Confluence's JMX monitoring. This has the same effect as setting the "enabled" property to false in `WEB-INF/classes/jmxContext.xml`
`confluence.optimize.index.modulo`	2.2	`20`	Confluence	Number of index queue flushes before the index is optimised.
`confluence.plugins.bundled.disable`	2.9	`false`	Confluence	Starts confluence without bundled plugins. May be useful in a development environment to make Confluence start quicker, but since bundled plugins are necessary for some of Confluence's core functionality, this property should not be set on a production system.
`atlassian.mail.fetchdisabled`	3.5	`false`	Confluence	Disables mail fetching services for IMAP and POP

`atlassian.mail.senddisabled`	3.5	`false`	Confluence and atlassian-mail	Disables sending of mail
`atlassian.disable.caches`	2.4	`true`	atlassian-plugins, atlassian-cache-servlet	Setting this property will disable conditional get and expires: headers on some web resources. This will significantly slow down the user experience, but is useful in devlopment if you are frequently changing static resources and don't want to continually flush your browser cache.
`confluence.html.encode.automatic`	2.9		Confluence	Setting this property forces the antixss encoding on or off, overriding the behaviour dictated by settings. The default behaviour differs between Confluence versions.
`org.osgi.framework.bootdelegation`	2.10	empty	atlassian-plugins	Comma-separated list of package names to provide from application for OSGi plugins. Typically required when profiling Confluence. For example: "com.jprofiler.**,com.yourkit.**".

`confluence.diff.pool.size`	3.1	`20`	Confluence	Maximum number of concurrent diffs. When that number is exceeded, additional attempts by RSS feeds to create diffs are ignored and logged. (The RSS requests succeed, they are just missing diffs).
`confluence.diff.timeout`	3.1	`1000`	Confluence	Number of milliseconds to wait for a diff operation (comparing two page versions) to complete before aborting with an error message.
`atlassian.user.experimentalMapping`	2.10	`false`	Confluence	Setting this property changes the relationship between local users and local groups to reduce performance degradation when adding a local user to a local group with a large number of users. Please note, setting this property can slow down other user management functions. We recommend that you set it only if you are experiencing performance problems when adding local users to large local groups. Please refer to CONF-12319, fixed in Confluence 3.1.1.

`confluence.import.use-experimental-importer`	3.2	`false`	Confluence	Setting this property changes Confluence to use the Experimental XML Importer. It is designed to be a more stable implementation but, at the time of the release of 3.2, the importer is largely untested and thus not supported.
`atlassian.webresource.disable.minification`	3.3	`false`	atlassian-plugins	Disables automatic minification of JavaScript and CSS resources served by Confluence.

`index.queue.thread.count`	3.3	*See "Effect"*	Confluence	Sets the number of threads to be used for the reindex job. The value has to be in the range of 1 to 10 (inclusive), i.e. at least one thread but no more than 10 threads will be used. There is no default value, i.e. • If you don't set `index.queue.thread.count`, the number of threads to be used are calculated based on the number of objects that need to be reindexed and the number of processors available (a maximum of 10 threads will be used). • If you set `index.queue.thread.count=2`, then two threads will be used to reindex the content (regardless of the number of objects to be reindexed or the number of processors available) • If you set `index.queue.thread.count=200`, then ten threads (the maximum allowed) will be used to reindex the content.

`index.queue.batch.size`	3.3	1500	Confluence	Size of batches used by the indexer. Reducing this value will reduce the load that the indexer puts on the system, but indexing takes longer. Increasing this value will cause indexing to be completed faster, but puts a higher load on the system. Normally this setting does not need tuning.
`password.confirmation.disabled`	3.4	`false`	Confluence	This property disables the password confirmation functionality that Confluence uses as an additional security measure. With this property set, Confluence will *not* require password confirmation for the following actions: administrative actions, change of email address and Captcha for failed logins. Disabling password confirmations is useful if you are using a custom authenticator.

`confluence.browser.language.enabled`	3.5	`true`	Confluence	Setting this property to "false" disables the detection of browser language headers, effectively restoring Confluence behaviour to that of earlier releases. Setting this property to "true" enables the detection of the language headers sent by the browser. Confluenc will change the UI language based on the browser headers. See documentation on how users can choose a language preference.
`upm.pac.disable`	Universal Plugin Manager 1.5	`false`	Universal Plugin Manager (UPM)	When this property is set to true, then UPM will not try to access the Atlassian Plugin Exchange. This is useful for application servers that do not have access to the Internet. See the UPM documentation.
`confluence.reindex.documents.to.pop`	3.5.9	`20`	Confluence	Indicates how many objects each indexing thread should process at a time during a full re-index. Please note that this number does not include attachments
`confluence.reindex.attachments.to.pop`	3.5.9	`10`	Confluence	Indicates how many attachments each indexing thread should process at a time during a full re-index.

`confluence.upgrade.active.directory`	3.5.11	`false`	Confluence	Forces Confluence to treat any LDAP directories it migrates as Active Directory, rather than relying on looking for sAMAccountName in the username attribute. This is necessary if you are upgrading from before Confluence 3.5, and need to use an attribute other than sAMAccountName to identify your users and are seeing `LDAP: error code 4 - Sizelimit Exceeded` exceptions in your logs. For more details, see Unable to Log In with Confluence 3.5 or Later Due to 'LDAP error code 4 - Sizelimit Exceeded'
`com.atlassian.logout.disable.session.invalidation`	4.0	`false`	Confluence	Disables the session invalidation on log out. As of 4.0 the default behaviour is to invalidate the JSession assigned to a client when they log out. If this is set to true the session is kept active (but the user logged out). This may be valuable when using external authentication systems, but should generally not be needed.

`officeconnector.spreadsheet.xlsxmaxsize`	4.0.5	2^{21}	Office Connector	Indicates the maximum size in bytes of an Excel file that can be viewed using the `viewxls` macro. If empty, the maximum size defaults to 2Mb. See CONF-21043 for more details.

RELATED TOPICS

Configuring System Properties

Configuring a Large Confluence Installation

Deploying *any* application to several thousand users requires care and planning, especially if those users are going to be relying on the application to get their work done.

> ⚠ *The information on this page does not apply to Confluence OnDemand.*

General Advice

Staged Rollout

Do not try to deploy Confluence immediately to your whole organisation. Instead, roll it out department by department, or project by project.

How Confluence will scale given a particular software and hardware configuration depends very much on how Confluence is likely to be used in your organisation. Launching Confluence to everybody at once may seem like a neat idea, but it also means that any problems you might experience scaling the system up to your entire organisation will hit you *all at once*, annoy everyone and possibly hurt adoption.

Rolling Confluence out gradually will give you the chance to tune it as you go, resulting in a much more painless experience. There will also be organisational advantages: you can identify those teams or projects who are most likely to be successful 'early adopters', and those teams can experiment with how best a wiki might suit your organisation, and pass on their 'best wiki practices' as usage of Confluence expands.

Plugin Governance

Confluence plugins can add tremendous value. Before adding one, visit the plugin's page and explore its issues (available from the issue management link). Try the plugin in a test environment and make sure to note any adverse effects after adding it to a production environment. Test plugins independently when upgrading.

Backup strategy

Disable the XML backup and use the Production Backup Strategy.

New Spaces Governance

For both performance and good practice, put some modest governance in place around the creation of new spaces, such as a simple request that includes a check for duplicates and some strategy around how to best use a space. Duplicates and unused spaces should be purged by a wiki gardener. Try to keep it to one space per group.

Choosing User Management and Single Sign-On

We recommend that you choose and configure your user management solution as soon as possible, rather than adding it to your Confluence installation at a later date.

It is possible to integrate with an LDAP repository, such as Microsoft Active Directory, or add a single sign-on solution later (especially with the addition of Crowd). But if possible it is best to configure your user management system up front. You can configure access for only a specific group or set of groups, thereby keeping the gradual rollout.

Please refer to our detailed guide to Configuring User Directories and examine the User Management Limitations and Recommendations.

Configuring your Application Server, Web Server and Database

Because Confluence can be deployed in so many server combinations, we do not currently have guides on the best tuning parameters for each individual server. We will be happy to provide support, however. If you have any tuning parameters that you find particularly useful for Confluence instances, feel free to share them with other Confluence users in the Confluence Community space.

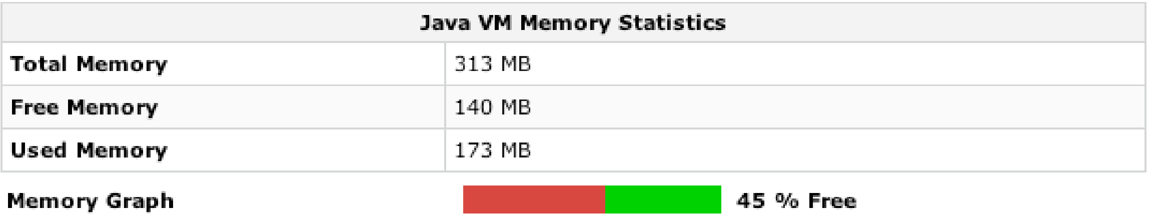
Best Practices

Troubleshooting possible memory leaks

The Troubleshooting Confluence Hanging or Crashing guide is a good place to start. Some of the known causes listed there could result in performance issues short of a crash or hang. Many of the issues reported there are exacerbated with a large installation.

Memory Usage

The Java virtual machine is configured with a "maximum heap size" that limits the amount of memory it will consume. If Confluence fills up this maximum heap size it will run out of memory, and start behaving unpredictably. You can keep track of Confluence's memory usage from the System Information screen of the administration console:



Java VM Memory Statistics	
Total Memory	313 MB
Free Memory	140 MB
Used Memory	173 MB
Memory Graph	🟥🟩 **45 % Free**

This example shows that, at the time of writing, confluence.atlassian.com is using 173MB of an allocated 313MB of heap. (The JVM was configured with a maximum heap size of 450MB, but this information is not available in the graph. The 313MB figure shows that the full 450MB of heap has not yet been needed)

Database Connection Pool

Confluence will need a database connection for each simultaneous user connection to the server. It is also a good idea to have 5-10 connections spare for Confluence internal processes such as backups, re-indexing or daily notification jobs.

Running out of pooled connections will cause the server to slow down as more users are waiting for a connection to be freed before starting their own request, and will eventually cause visible system errors as Confluence times out waiting for a database connection.

If you are using Confluence's internal connection pool, you can increase the number of available connections by modifying the `hibernate.c3p0.max_size` property in `{confluence_home}/confluence-cfg.xml`, and restarting Confluence. **Make sure** you have also configured your database to be able to support that many simultaneous connections.

Cache Sizes

The Performance Tuning page includes some useful rules of thumb for configuring the sizes of Confluence's internal caches.

RELATED TOPICS

Operating Large or Mission-Critical Confluence Installations
Performance Tuning
Confluence Clustering Overview
Requesting Performance Support
User Management
Confluence Administrator's Guide
Confluence Configuration Guide

Configuring Logging

We recommend that you configure Confluence's logging to your own requirements. You can change the log settings in two ways:

- Configure logging in Confluence Administration – Your changes will be in effect only until you next restart Confluence.
- Edit the properties file – Your changes will take effect next time you start Confluence, and for all subsequent sessions.

Both methods are described below. In some rare circumstances you may *also* need to configure Configuring Logging.

Terminology: In log4j, a 'logger' is a named entity. Logger names are case-sensitive and they follow a hierarchical naming standard. For example, the logger named `com.foo` is a parent of the logger named `com.foo.Bar`.

⚠ *The information on this page does not apply to Confluence OnDemand.*

Configure logging in Confluence Administration

You can change some of Confluence's logging behaviour via the **Administration Console** while Confluence is running. Any changes made in this way will apply only to the currently-running Confluence lifetime. The changes are not written to the `log4j.properties` file and are therefore discarded when you next stop Confluence.

Not all logging behaviour can be changed via the Administration Console. For logging configuration not mentioned below, you will need to stop Confluence and then edit the logging properties file instead.

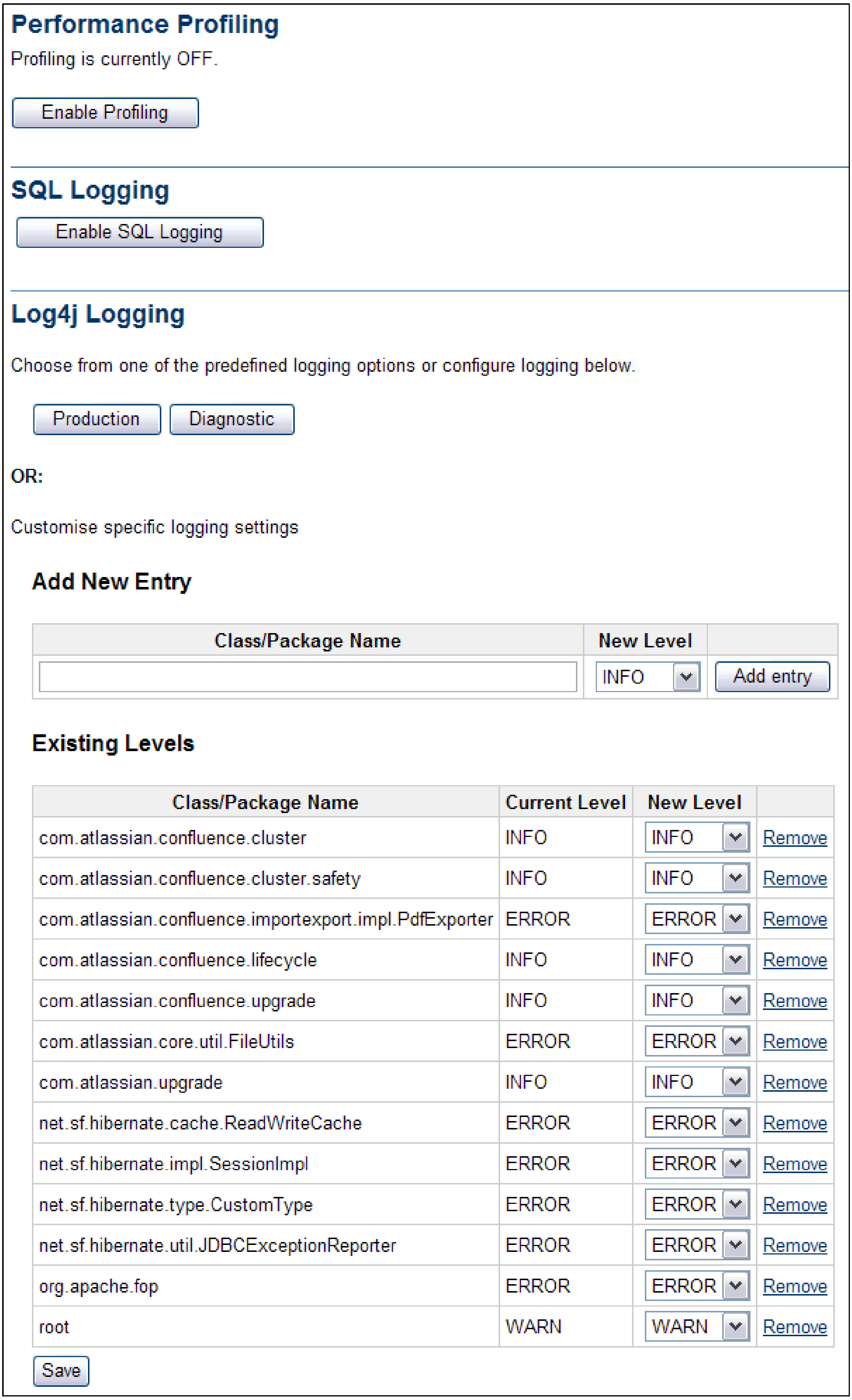
The '**Logging and Profiling**' screen shows a list of all currently defined loggers. On this screen you can:

- Turn page profiling on or off.
- Turn detailed SQL logging on or off.
- Add a new logger for a class/package name.
- Remove a logger for a class/package name.
- Set the logging level (INFO, WARN, FATAL, ERROR or DEBUG) for each class or package name.
- Reset all logging levels to a predefined profile.

Changing the logging configuration

1. Choose **Browse** > **Confluence Admin**.
2. Select '**Logging and Profiling**' in the '**Administration**' section of the left-hand panel.
   You need to have System Administrator permissions in order to perform this function.
3. The '**Logging and Profiling**' screen appears, as shown below. Use the following guidelines to change the logging behaviour while Confluence is running:
   - '**Performance Profiling**' — See Page Request Profiling.
   - '**SQL Logging**' — Click the '**Enable SQL Logging**' button to log the details of SQL requests made to the database.
     If you need to enable logging of SQL parameter values, you will need to change the setting in the properties file. This option is not available via the Administration Console.
   - '**Log4j Logging**' — Click one of the profile buttons to reset all your loggers to the predefined profiles:
     - The '**Production**' profile is a fairly standard profile, recommended for normal production conditions.
     - The '**Diagnostic**' profile gives more information, useful for troubleshooting and debugging. It results in slower performance and fills the log files more quickly.
   - '**Add New Entry**' — Type a class or package name into the text box and click the '**Add Entry**' button. The new logger will appear in the list of '**Existing Levels**' in the lower part of the screen.
   - '**Existing Levels**' - These are the loggers currently in action for your Confluence instance.
     - You can change the logging level by selecting a value from the '**New Level**' dropdown list. Read the Apache documentation for a definition of each level.
     - Click the '**Remove**' link to stop logging for the selected class/package name.
4. Click the '**Save**' button to save any changes you have made in the '**Existing Levels**' section.

Screenshot: Changing Log Levels and Profiling



Performance Profiling

Profiling is currently OFF.

SQL Logging

Log4j Logging

Choose from one of the predefined logging options or configure logging below.

OR:

Customise specific logging settings

Add New Entry

Class/Package Name	New Level	
	INFO	Add entry

Existing Levels

Class/Package Name	Current Level	New Level	
com.atlassian.confluence.cluster	INFO	INFO	Remove
com.atlassian.confluence.cluster.safety	INFO	INFO	Remove
com.atlassian.confluence.importexport.impl.PdfExporter	ERROR	ERROR	Remove
com.atlassian.confluence.lifecycle	INFO	INFO	Remove
com.atlassian.confluence.upgrade	INFO	INFO	Remove
com.atlassian.core.util.FileUtils	ERROR	ERROR	Remove
com.atlassian.upgrade	INFO	INFO	Remove
net.sf.hibernate.cache.ReadWriteCache	ERROR	ERROR	Remove
net.sf.hibernate.impl.SessionImpl	ERROR	ERROR	Remove
net.sf.hibernate.type.CustomType	ERROR	ERROR	Remove
net.sf.hibernate.util.JDBCExceptionReporter	ERROR	ERROR	Remove
org.apache.fop	ERROR	ERROR	Remove
root	WARN	WARN	Remove

Editing the Properties File

To configure the logging levels and other settings on a permanent basis, you need to stop Confluence and then change the settings in the `log4j.properties` file, described above.

The properties file contains a number of entries for different loggers that can be uncommented if you are interested in logging from particular components. Read more in the Apache log4j documentation.

See Working with Confluence Logs for some guidelines on specific configuration options you may find useful.

Configuring Levels for java.util.logging in logging.properties

A few libraries used by Confluence use java.util.logging rather than log4j or slf4j. These libraries include:

- com.sun.jersey
- org.apache.shindig
- net.sf.ehcache

Confluence's `logging.properties` file is set to redirect java.util.logging at specific levels to log4j via slf4j.

To increase logging levels for these libraries you must first configure the `logging.properties` file in `<CONFLUENCE-INSTALL>/confluence/WEB-INF/classes/`. The logging levels are different from log4j and are listed here.
For example, to increase logging for shindig change the following line in the `logging.properties` file:

```
org.apache.shindig.level = INFO
```

to

```
org.apache.shindig.level = FINE
```

And then use one of the methods above **as well** to configure the log4j level.

Registering External Gadgets

You can register gadgets from external web sites (such as JIRA, iGoogle or Gmail) with your Confluence installation, so that the gadgets appear in the macro browser and people can add them to Confluence pages via a gadget macro.

Choose one of the following ways to register the external gadgets on Confluence:

- **Subscribe to all of the external application's gadgets:** You can add all the gadgets from your JIRA, Bamboo, FishEye or Crucible site – or from another Confluence site – to your Confluence gadget directory. People can then pick and choose the gadgets to add to their Confluence pages.
- **Register the external gadgets one by one:** If you cannot subscribe to an application's gadgets, you will need to add the gadgets one by one. This is necessary for applications and websites that do not support gadget subscription, and for applications where you cannot establish a trusted relationship via Application Links.

Both methods are described below. First, consider whether you need to set up a trust relationship between Confluence and the other application.

Setting up a trust relationship with the other application

In addition to registering the external gadgets, we recommend that you set up an OAuth or Trusted Application relationship between the application that serves the gadget (the service provider) and Confluence (the consumer). The trust relationship is required for gadgets that access restricted data from the external web application.

See how to configure OAuth or Trusted Applications Authentication, using Application Links.

If the external web application provides anonymous access to all the data you need in the gadgets, then you do not need a trust relationship.

For example, if your gadgets will retrieve data from JIRA and your JIRA server includes projects and issues that are restricted to logged-in users, then you will need a trust relationship between Confluence and JIRA. If you do not set up the trust relationship, then the gadgets will show only the information that JIRA makes visible to anonymous users.

Subscribing to all of the application's gadgets

You can add all the gadgets from your JIRA, Bamboo, FishEye or Crucible site – or from another Confluence site – to your Confluence gadget directory. People can then pick and choose the gadgets to add to their Confluence pages.

To subscribe to another site's gadgets:

1. Choose **Browse** > **Confluence Admin**.
2. Click **External Gadgets** in the left-hand panel.
3. Click the **Gadget Feeds** tab.
4. Enter the base URL of the application you want to subscribe to, in the text box labelled **Gadget Feed URL**. For example, `http://example.com/jira` or `http://example.com/confluence`.
5. Click **Add**. Confluence will convert the URL to a gadget feed and place it in the list of 'Added Gadget Feeds'.

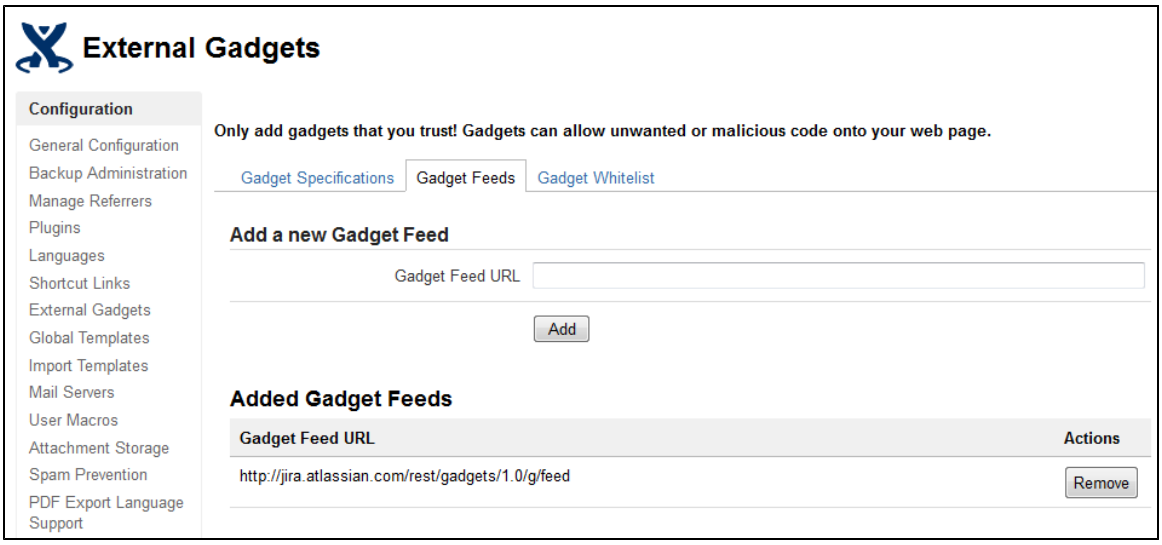
On this page:

Related pages:

- Configuring a URL Whitelist for Gadgets
- The big list of Atlassian gadgets
- Adding JIRA Gadgets to a Confluence Page
- Configuring Application Links

The information on this page does not apply to Confluence OnDemand.

Screenshot 1: Subscribing to a gadget feed



Only add gadgets that you trust! Gadgets can allow unwanted or malicious code onto your web page.

Add a new Gadget Feed

Gadget Feed URL

Added Gadget Feeds

Gadget Feed URL	Actions
http://jira.atlassian.com/rest/gadgets/1.0/g/feed	Remove

Registering individual gadgets

If you cannot subscribe to an application's gadgets, you will need to register the gadgets one by one. This is necessary for applications and websites that do not support gadget subscription, and for applications where you cannot establish a trusted relationship via Application Links.

First you will need to obtain that gadget's URL and copy it to your clipboard.

Getting a gadget's URL from an Atlassian application

If your web application is another Atlassian application such as Confluence or JIRA:

A gadget's URL points to the gadget's XML specification file. In general, a gadget's URL looks something like this:

```
http://example.com/my-gadget-location/my-gadget.xml
```

If the gadget is supplied by a plugin, the URL will have this format:
`http://my-app.my-server.com:port/rest/gadgets/1.0/g/my-plugin.key:my-gadget/my-path/my-gadget.xml`
For example:
`http://mycompany.com/jira/rest/gadgets/1.0/g/com.atlassian.streams.streams-jira-plugin:activitystream-gadget/gadgets/activitystream-gadget.xml`

To find a gadget's URL in JIRA:

- Go to your dashboard by clicking the **Dashboards** link at the top left of the screen.
- Click **Add Gadget** to see the list of gadgets in the directory.
- Find the gadget you want, using one or more of the following tools:
  - Use the scroll bar on the right to move up and down the list of gadgets.
  - Select a category in the left-hand panel to display only gadgets in that category.
  - Start typing a key word for your gadget in the **Search** textbox. The list of gadgets will change as you type, showing only gadgets that match your search term.
- Right-click the **Gadget URL** link for that gadget and copy the gadget's URL into your clipboard.

To find a gadget's URL in Confluence:

- Choose **Browse** > **Confluence Gadgets** to see the list of available Confluence gadgets.
- Find the gadget you want.
- Right-click the **Gadget URL** link for that gadget and copy the gadget's URL into your clipboard.

Getting a gadget's URL from another application

If the gadget comes from a non-Atlassian web application or web site, please consult the relevant documentation for that application to obtain the gadget's URL.

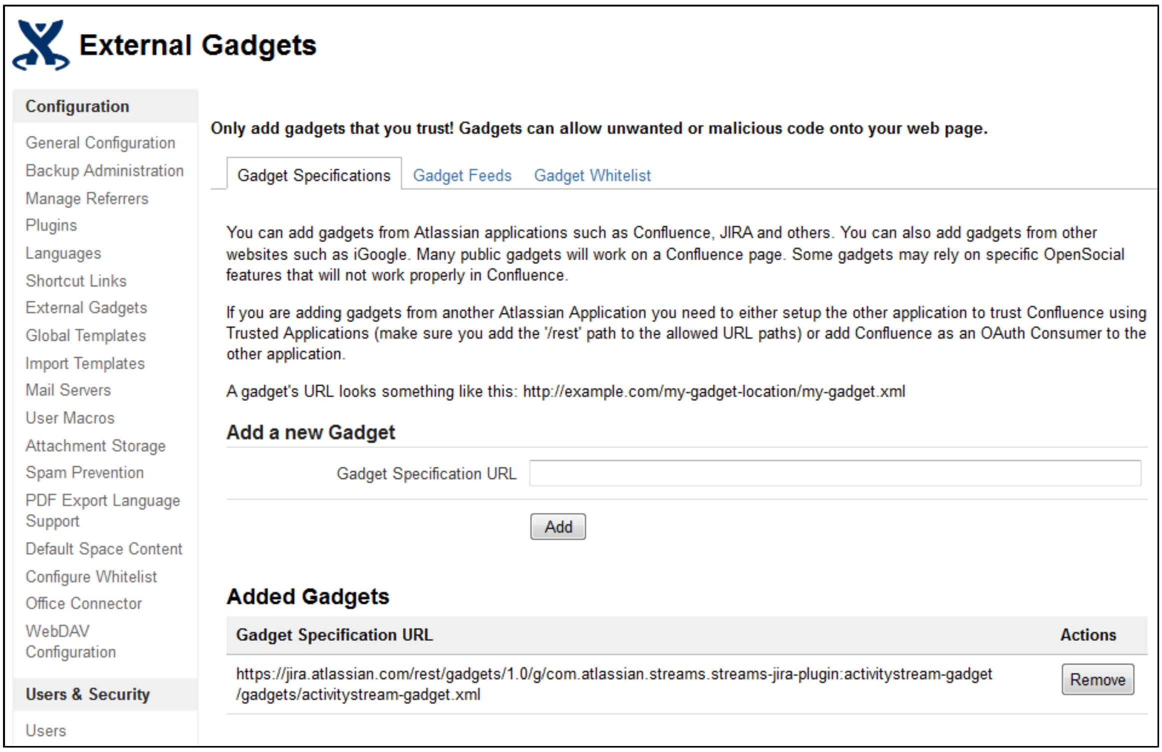
Registering the gadget for use in Confluence

Now that you have the gadget's URL, you can register it in Confluence, so that people can add it to their pages.

To register the gadget in Confluence:

1. Choose **Browse** > **Confluence Admin**.
2. Click **External Gadgets** under 'Configuration' in the left panel. The 'External Gadgets' page is displayed.
3. In the 'Add a new Gadget' section, paste your gadget's URL into the **Gadget Specification URL** field.
4. Click **Add**. Your gadget will be shown in the list of registered gadgets below and it will also become available in the macro browser.

Screenshot 2: Registering external gadgets one by one



Only add gadgets that you trust! Gadgets can allow unwanted or malicious code onto your web page.

You can add gadgets from Atlassian applications such as Confluence, JIRA and others. You can also add gadgets from other websites such as iGoogle. Many public gadgets will work on a Confluence page. Some gadgets may rely on specific OpenSocial features that will not work properly in Confluence.

If you are adding gadgets from another Atlassian Application you need to either setup the other application to trust Confluence using Trusted Applications (make sure you add the '/rest' path to the allowed URL paths) or add Confluence as an OAuth Consumer to the other application.

A gadget's URL looks something like this: http://example.com/my-gadget-location/my-gadget.xml

Add a new Gadget

Gadget Specification URL

Added Gadgets

Gadget Specification URL	Actions
https://jira.atlassian.com/rest/gadgets/1.0/g/com.atlassian.streams.streams-jira-plugin:activitystream-gadget/gadgets/activitystream-gadget.xml	Remove

Removing access to external gadgets

To remove a single gadget from Confluence, click the **Remove** button next to the gadget URL.

If you have subscribed to an application's gadgets, you will need to remove the entire subscription. You cannot unregister a single gadget. Click the **Remove** button next to the gadget feed URL.

The gadget(s) will no longer be available in the macro browser, and people will not be able to add them using the Gadget macro. Any pages that already use the gadget will show a broken gadget link.

Configuring a URL Whitelist for Gadgets

For security reasons, you may wish to limit the URLs from which users can get content that is displayed on your Confluence site, such as the content displayed in a gadget. A whitelist is a list of URLs whose content you wish to make available to users of your site.

Adding whitelist URLs for external gadgets

By default, Confluence will block a gadget's access to third-party data sources. When you are using a gadget that draws content from a third-party data source, you will need to add the URL of that data source to the gadget whitelist.

To add a URL to the whitelist for gadgets:

1. Choose **Browse** > **Confluence Admin**.
2. Click **External Gadgets** in the left-hand panel.
3. Click the **Gadget Whitelist** tab.
4. Enter a URL for the **Host to Whitelist**. For example, `http://jira.atlassian.com`. You can also enter a URL pattern, as described below.
5. Click **Add**.

On this page:

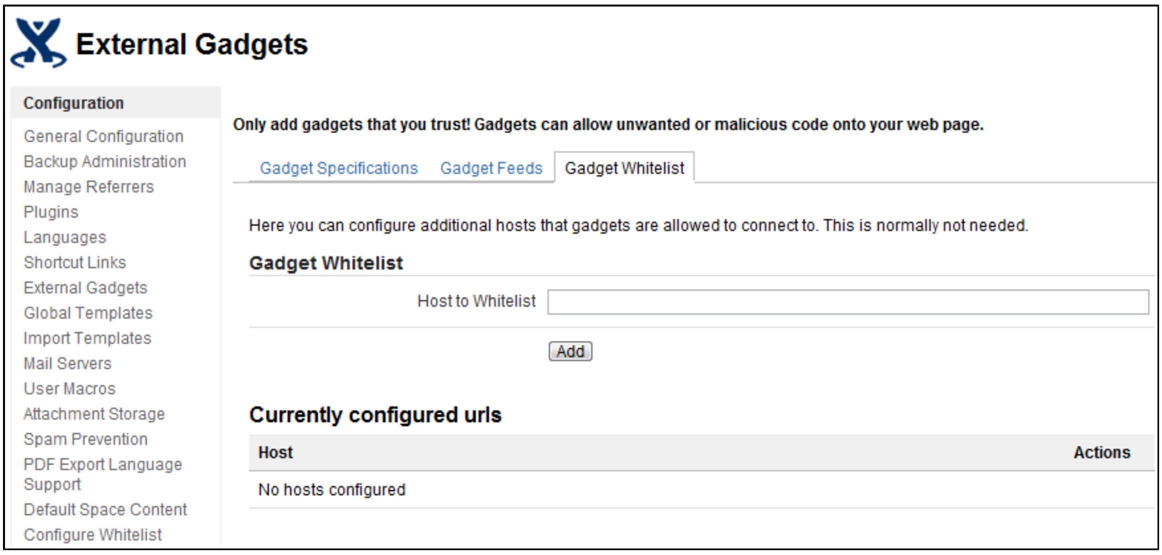
- Adding whitelist URLs for external gadgets
- Rules for URL pattern-matching
- Notes

Related pages:

- Registering External Gadgets
- Configuring a URL Whitelist for Macros
- Confluence Administrator's Guide

⚠ *The information on this page does not apply to Confluence OnDemand.*

Screenshot: Configuring a URL whitelist for external gadgets



External Gadgets

Only add gadgets that you trust! Gadgets can allow unwanted or malicious code onto your web page.

Here you can configure additional hosts that gadgets are allowed to connect to. This is normally not needed.

Gadget Whitelist

Host to Whitelist

Currently configured urls

Host	Actions
No hosts configured	

Rules for URL pattern-matching

Enter one URL or URL pattern per line. You can enter a full URL or use pattern-matching as described below:

- If the rule starts with an equals sign (=), only the exact URL following the '=' will be allowed.
- If the rule starts with a slash (/) then the whole rule will be treated as a regular expression.
- Otherwise, any asterisk (*) will be treated as a wildcard to match one or more characters.

Notes

- URLs for which Application Links are configured are automatically whitelisted, so you do not need to add them to this list.
- When a gadget or subscription is removed from your site, the whitelist entry is **not** automatically removed.

Confluence Clustering Overview

It is possible to run Confluence in a clustered environment instead of on a single server. This means that you can run multiple copies of Confluence in a cluster, so that clients (such as a browser) can connect to any copy and see the same information.

> ⚠ **Consider your options carefully before deciding on a clustered installation**
>
> While we have tried to make clustering Confluence as easy and administrator-friendly as possible, it is a major architectural change and requires extra planning for deployment and upgrades. Please consider the information on the Cluster Checklist and then consult Atlassian support before making your final decision.

This page gives an overview and links to further pages with information on installing, configuring and administering a Confluence cluster.

> ⚠ *The information on this page does not apply to Confluence OnDemand.*

Before Deciding to Run a Confluence Cluster

1. Read and consider the details on the Cluster Checklist.
2. Consider the difference between clustering for scalability and clustering for high availability (HA).
3. Contact Atlassian support for further information and advice.

Technical Overview

> ℹ **Confluence on Virtualised Environments**
>
> Atlassian officially supports non-clustered installations of Confluence 3.0 and later on VMware. Although possible, we do not recommend (nor support) running versions of Confluence prior to 3.0 on VMware, since Confluence 3.0 resolved many performance issues that were present in earlier versions. Be aware that we also do not support clustered installations of Confluence on VMware. Please comment or vote on the feature request at CONF-19559.

Read a technical overview of clustering in Confluence.

Server and Network Requirements

- Server hardware requirements
- Technical overview of Confluence clustering
- Diagram of recommended network topology

Installation and Upgrading

There are two methods of installing Confluence in a cluster, depending on whether you have existing data:

- Fresh installation
- Existing data

If you are upgrading an existing Confluence cluster to a new version of Confluence, refer to the cluster upgrade guide.

Configuration and Administration

- Cluster Administration page in the **Administration Console**
- Changing datasources in clusters

Troubleshooting

- Cluster troubleshooting

RELATED TOPICS

Operating Large or Mission-Critical Confluence Installations
Performance Tuning
Requesting Performance Support
Confluence Administrator's Guide
Confluence Configuration Guide

Technical Overview of Clustering in Confluence

Overview of clustering documentation

Refer to the overview of Confluence clustering in the *Administrators' Guide*.

The information on this page does not apply to Confluence OnDemand.

Introduction

From version 2.3, Confluence has had the ability to configure and run multiple copies of itself in a cluster, so that clients can connect to any copy and see the same information. In effect, a Confluence cluster behaves as a single, powerful Confluence installation. While we have tried to make clustering Confluence as easy and administrator-friendly as possible, it is a major architectural change from earlier versions (or non-clustered installations) and consequently, requires extra planning for deployment and upgrades.

This document will give a technical overview of clustering in Confluence, primarily for those users and developers who will be installing and configuring Confluence in a cluster. A separate overview is available for Confluence plugin developers.

Cluster topology

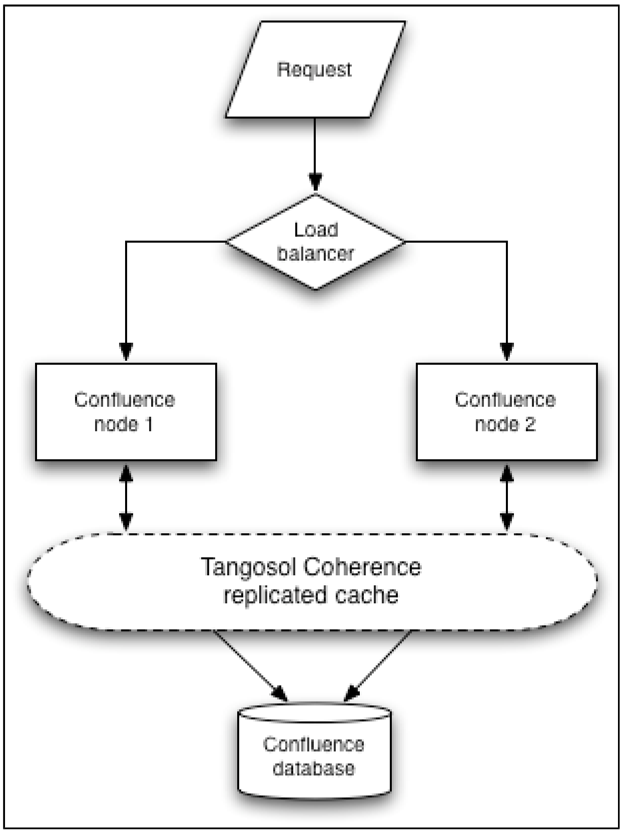
A simple description of the cluster topology for Confluence would be **multiple applications, shared data source**. A cluster of Confluence consists of:

- multiple homogeneous installations of Confluence (called *nodes*below)
  - a Confluence home directory for each installation.
- a distributed Oracle Coherence cache (formerly known as

Tangosol Coherence), which all nodes use via a multicast group - see networking summary below
- a single database, which all nodes connect to

The user is responsible for configuring an appropriate HTTP load balancer in front of the clustered installations. Typically this means using mod_jk or another application server load-balancing technology. The load balancer must be configured to support **session affinity**.

Communication between clustered nodes is minimised by using a distributed cache which propagates updates to all other nodes automatically. Where necessary, Coherence provides a locking mechanism for synchronising jobs and a RMI interface for more complex communication.



Confluence cluster topology (simplified)

LAN Clustering Only

Atlassian **only supports clustering over a local area network**. While it is theoretically possible to configure Confluence to cluster across a WAN, the latency involved is likely to kill performance of the cluster. We can't stop you trying, of course, but you're going to have to work out how to configure Coherence yourself, and we're not going to support the resulting mess.

Homogeneous Confluence installations

All the Confluence installations must be running exactly the same application, down to the lowest level. Items that must be the same include:

- Confluence version
- Application server version
- JDK version
- Libraries and plugins in the Confluence classpath, WEB-INF/lib
- Libraries in the application server classpath

The installation section has more information how to ensure homogeneous node installations.

Creating a Confluence cluster

When installing Confluence in a clustered setup, you will be responsible for configuring your web server and load balancer to distribute traffic between each node. No additional software is required as Coherence is bundled with Confluence.

Here is an overview of the process:

1. Obtain a clustered licence key from Atlassian for each node
2. Upgrade a single node to the clustered licence

3. Start the cluster from that node's administration menu, specifying a name and optionally a preferred network interface
4. Restart the single node and test it
5. Copy the Confluence application and Confluence home directory to the second node
6. Bring up the second node and it will automatically join the cluster.

Copying the Confluence application and home directory helps ensure that the installations are homogeneous.

An alternative to this method is to copy the Confluence web application, but not the Confluence home directory. In this case, the installation wizard will require your cluster name to connect to the other nodes, and it will automatically configure itself. You will need to rebuild the index manually after this installation, however.

There is now full documentation for a Confluence Cluster Installation.

Upgrade process

Another consequence of the homogeneous requirement is that upgrades must be done by following a strict process.

1. All cluster nodes are brought down
2. Upgrade a single node to the latest Confluence version
3. Start the single node so it can upgrade the database
4. Upgrade subsequent nodes and start them one-by-one.

This is the only safe method of upgrading a Confluence cluster.

Single database

The Confluence database in a cluster is shared by all nodes. This means that the database must be able to scale to service *all* the Confluence nodes, which will probably mean implementing some kind of database cluster and JDBC-level load balancing. We can not offer support with scaling or tuning your database, you will need to talk to your DBA or database vendor.

For obvious reasons, you must have an external database to run Massive - you can not cluster Confluence when using the embedded HSQL database.

The most important requirement for the cluster database is that it have sufficient connections available to support the expected number of application nodes. For example, if each Confluence instance has a connection pool of 20 connections and you expect to run a cluster with four nodes, your database server must allow at least 80 connections to the Confluence database. In practice, you may require more than the minimum for debugging or administrative purposes.

In a cluster, attachments must be stored in the database. Configuring a cluster in an existing installation will automatically migrate your attachments to the database. Non-clustered installations still have the option of using the Confluence home directory for storing attachments.

While attachments are stored in the database, they are temporarily written to the cluster node's local filesystem, designated `<confluence-home>/temp` folder, when being streamed to users (so Confluence doesn't have to hold open database connections unnecessarily). For this reason, Confluence will still need enough temporary disk space to hold any attachments currently in transit.

Distributed cache

In a normal configuration, Confluence uses many caches to reduce the number of database queries required for common operations. Viewing a page might require dozens of permissions checks, and it would be very slow if Confluence queried the database for this information with every page view. However, caches must be carefully maintained so they are consistent with the application data. If the page permissions change, the old invalid data needs to be removed from the cache so it can be replaced with a fresh correct copy.

To preserve consistent caches across a cluster, Confluence uses a distributed cache called Oracle Coherence, which manages replicating cache updates transparently across all nodes. The network requirements of the distributed cache are quite simple, but must be preserved if the cluster is to work properly.

To discover other nodes in the cluster, Confluence broadcasts a join request on a multicast network address. Confluence must be able to open a UDP port on this multicast address, or it will not be able to find the other cluster nodes.

Once the nodes are discovered, each responds with a unicast (normal) IP address and port where it can be contacted for cache updates. Confluence must be able to open a UDP port for regular communication with the other nodes.

Because the Coherence network requirements are different to those required by the Confluence database connection, the situation can arise where Confluence can use the database but not talk to the other nodes in the cluster via Coherence. When Confluence detects this, it will shut itself down in a cluster panic.

For more details on the network configuration of the distributed cache, see the networking summary

Home directory

Confluence's home directory has a much-reduced role in a cluster. Because the application data must be shared between all nodes for consistency, the only information stored in the Confluence home directory is either node-specific, or needed to start Confluence. This includes information related to:

- database connection
- license
- cluster connection

The only application data stored in the Confluence home directory is the **Lucene search index**. Confluence synchronises this data itself by keeping track of indexing tasks in the database.

This is also why we recommend copying the Confluence home directory from the first node when setting up subsequent nodes. If you did not copy the Confluence home directory, you would need to rebuild the search index from scratch on the subsequent nodes after installation.

Event handling

Broadcasting events to all nodes in a cluster is supported in Confluence, but not recommended. The cluster topology uses a shared data store so that application state does not need to be synchronised by events.

The event broadcasting is done only for certain events, like installing a plugin. When a plugin is installed in one node, Confluence puts the plugin data in the database, and notifies the other nodes that they need to load the plugin into memory.

Indexing

Confluence maintains a copy of its Lucene search index on each node of the cluster. This index is used for many things beside full-text searches, including RSS feeds and lists of recently updated content. Indexing in a cluster works like this:

1. Node 1 gets a request to save some page update
2. After saving the page in the database, Node 1 adds a "page-updated" index entry to the queue, which is in the database
3. Periodically, each node picks up the "latest entries" from the queue, where what is latest is determined from a timestamp on a file in the Confluence home directory which indicates when the queue was last inspected. This process is called "flushing the index queue".
4. Each node independently updates its local Lucene index. The "page-updated" index entry is internally changed into a delete-document task and an add-document task to apply the changes to Lucene.
5. Each node updates the timestamp on its index-queue-timestamp file to reflect the most recent processing

or "flushing" of the index queue.

Because of step #3, if the timing of the nodes is not synchronised or changes sporadically (due to a virtualisation environment, typically), index changes will not be correctly synchronised in the cluster. This is the most common cause of index sync problems in clusters.

If a node is disconnected from the cluster for a short amount of time (less than three hours), it will be able to bring its copy of the index up-to-date when it rejoins the cluster. If a node is down for a long amount of time and its lucene index has become stale as a result, you may want to avoid the expensive operation of rebuilding the index. To do that, you must copy a "live" version of the Lucene index from an active node. Simply replace the contents of the `Confluence Home]/index` directory with those from an active node before bringing the stale node back up.

Job synchronisation

For tasks such as sending the daily report emails, it is important that only one node in the cluster does this. Otherwise you would get multiple emails from Confluence every day.

Confluence uses locks in the Coherence distributed cache to ensure only one node can be running certain jobs at a time. This ensures email notifications will only be sent once.

Activity tracking

Activity tracking does not work in a cluster, and will be disabled for clustered deployments. We're working on making the activity tracker clusterable in a future release. You can follow this issue. You can try some other options for tracking usage.

Cluster panic

In some situations, there can be a network issue or firewall that prevents the distributed cache from communicating but still allows Confluence to update the database. This is a dangerous situation because when the caches on the detached nodes become inconsistent, users on different nodes will see different information and updates can be lost.

Confluence can detect this problem by checking a database value against a cached value, and if they differ, all the clustered nodes will be shut down with a 'Cluster panic' message. This is considered a fatal error because the consequences can cause damage to your data. For those administrators that like to live on the edge, there is a system property to prevent cluster panic and allow data corruption. For more information, see Cluster safety mechanism.

If a cluster panic does occur, you need to ensure proper network connectivity between the clustered nodes. Most likely multicast traffic is being blocked or not routed correctly. See the networking summary below.

Summary of network requirements

In addition to normal connectivity with its database, all clustered Confluence instances require access to a multicast group and the ability to open a UDP unicast port.

By default, the multicast address is automatically generated from the cluster name you provide when starting the cluster and the multicast port is fixed. During cluster setup, Confluence will prompt for the unicast IP address to use if the server has multiple network interfaces, and by default the unicast port is fixed. The cluster multicast group will be joined on the same network interface as the bound unicast IP address.

For any settings which are not configurable through the Confluence web interface, they can be configured via an XML file in the Confluence home directory for more exotic networking requirements.

Scaling Confluence On A Single Server

Since the maximum addressable memory on a 32 bit JVM is 4GB, some large servers may scale Java applications by running JVM instances concurrently. This would be implemented as separate, clustered Confluence nodes running on a single server and communicating internally. Because each JVM replicates the cache entirely, it may be useful to test a single, massive instance running a 64 bit JVM as an alternative. This configuration may result in superior performance than an internal cluster.

Geographically Distributed Clusters

Collocating nodes is strongly recommended as high latency will almost certainly degrade performance due to the overhead of cache replication. Cluster nodes will provide the best performance if servers are physically adjacent. However, as long as all nodes share a LAN, users may wish to test alternative configurations to see how performance is affected.

RELATED TOPICS

Server Hardware Requirements Guide
Overview of Confluence Clusters
Developers' Guide to Clustering

Cluster safety mechanism

Introduction

A mechanism was added in Confluence 2.3 and above to ensure database consistency when running multiple cluster nodes against the same database. This is called the *cluster safety mechanism*, and is designed to ensure that your wiki cannot become inconsistent because updates by one user are not visible to another. A failure of this mechanism is a fatal error in Confluence and is called *cluster panic*.

Because the cluster safety mechanism helps prevents data inconsistency whenever any two copies of Confluence running against the same database, it is enabled in *all* instances of Confluence, not just clusters.

> ⚠ *The information on this page does not apply to Confluence OnDemand.*

How cluster safety works

A scheduled task, ClusterSafetyJob, runs every 30 seconds in Confluence. In a cluster, this job is run only on one of the nodes. The scheduled task operates on a *safety number* – a randomly generated number that is stored both in the database and in the distributed cache used across a cluster. It does the following:

1. **Generate** a new random number
2. **Compare the existing safety numbers**, if there is already a safety number in both the database and the cache.
3. **If the numbers differ, publish a ClusterPanicEvent**. Currently in Confluence, this causes the following to happen:
    - disable all access to the application
    - disable all scheduled tasks
    - update the database safety number to a new value, which will cause all nodes accessing the database to fail.
4. If the numbers are the same or aren't set yet, **update the safety numbers**:
    - set the safety number in the database to the new random number
    - set the safety number in the cache to the new random number.

How to fix it

See 'Database is being updated by an instance which is not part of the current cluster' Error Message

Technical details

The cluster safety number in the database is stored in the `CLUSTERSAFETY` table. This table has just one row: the current safety number.

Changing Datasources Manually in a Cluster

> The recommended way of changing database connections is to shut down the whole cluster, install Confluence into new and empty directories and use the Setup Wizard to configure all new database connection settings.

However, if you wish to manually change your settings, you may proceed as described below.

It is **strongly recommended** that you test all of the following in a staging or test instance of Confluence before performing these steps in your production environment.

> *The information on this page does not apply to Confluence OnDemand.*

Step 1: Prepare

- Locate the `confluence-cfg.xml` file in the Confluence home directory.
- Make a backup copy of that file.
- Prepare the necessary changes to that file.

Step 2: Shut Down Confluence

You need to shut down all the nodes in the cluster, not just one.

Step 3: Apply your Changes

Apply your configuration changes to the required node.

Step 4: Restart the Changed Node

It is crucial that you bring up the node on which you applied the changes **first**. Otherwise you will get an error message, and have to shut down all instances again.

Step 5: Restart all Other Nodes

Done.

RELATED PAGES

Overview of Confluence Clusters

Cluster Troubleshooting

Confluence on Virtualised Environments

Atlassian officially supports non-clustered installations of Confluence 3.0 and later on VMware. Although possible, we do not recommend (nor support) running versions of Confluence prior to 3.0 on VMware, since Confluence 3.0 resolved many performance issues that were present in earlier versions. Be aware that we also do not support clustered installations of Confluence on VMware. Please comment or vote on the feature request at CONF-19559.

Overview of clustering documentation

Refer to the overview of Confluence clustering.

This page covers troubleshooting for the Clustered Edition. If you're experiencing Cluster Panic messages in a Standard Edition, visit the Knowledge Base article 'Database is being updated by an instance which is not part of the current cluster' Error Message.

On this page:

⚠ *The information on this page does not apply to Confluence OnDemand.*

Symptoms

Below is a list of potential problems with a Confluence cluster, and their likely solutions. The solutions are listed below.

Problem	Likely solutions
`Database is being updated by an instance which is not part of the current cluster` errors on a stand-alone	'Database is being updated by an instance which is not part of the current cluster' Error Message
`Database is being updated by an instance which is not part of the current cluster` errors on a cluster	Add multicast route, Check firewall
`Cannot assign requested address` on startup, featuring an IPv6 address	Prefer IPv4
Error in log: `The interface is not suitable for multicast communication`	Change multicast interface, Add multicast route
Multicast being sent, but not received (detectable with Multicast Test)	Check firewall, Check intermediate routers, Increase multicast TTL

Any issue not covered here	Contact support

Confluence cluster debugging tools

There is an umbrella issue opened for all cluster debugging tools here

It includes the tools listed below.

Multicast

- Which multicast address?

The multicast address and port used by Confluence can be found on the Cluster Administration page, or in `confluence.cfg.xml` in the Confluence home directory.

- Multicast address generation.

Confluence uses a hashing algorithm to take the inputted name during setup and it is then turned into a multicast address stored in the config file. Thus, once the initial setup is completed, Confluence will use the address this is the reason why user can change the address if needed, without actually changing the name. Consequently the additional nodes using the same multicast address specified in the config file are able to join the cluster.

Each node has a multicast address configured in the `confluence-cfg.xml` file

```
name="confluence.cluster.address">xxx.xx.xxx.xxx</property>
```

A warning message is displayed when an user changes the address from the one that Confluence has generated by the hashing of the name. There is no way of eliminating the message any other way other than by returning the address to the one that matches the cluster name. Purpose of the warning message is to remind the user that the address has been changed - as it is not the hashed version any longer - consequently the node can not join the cluster just by using the name. It is also necessary to provide the correct address as well.

Mapping interface to IP address.

To ensure that the interface name is mapped correctly, the following tool can be used. It shows the mapping of the interface name to the IP address.

```
C:\>java -jar list-interfaces.jar
interfaces.size() = 4
networkInterface[0] = name:lo (MS TCP
Loopback interface) index: 1 addresses:
/127.0.0.1;

networkInterface[1] = name:eth0 (VMware
Virtual Ethernet Adapter for VMnet8)
index: 2 addresses:
/192.168.133.1;

networkInterface[2] = name:eth1 (VMware
Virtual Ethernet Adapter for VMnet1)
index: 3 addresses:
/192.168.68.1;

networkInterface[3] = name:eth2 (Broadcom
NetXtreme 57xx Gigabit Controller - Packet
Scheduler Miniport) index: 4 addresses:
/192.168.0.101;
```

Debugging tools

Listed below are some debugging tools that help determine what the status of the multicast traffic is:

Tool	Information provided
`netstat -gn`	Lists multicast groups. Does not work on Mac OS X.
`netstat -rn`	Lists system routing table.
Multicast Test	Coherence tool for testing multicast traffic from one node to another.
`tcpdump -i` *`interface`*	Captures network traffic on the given interface. Most useful on an interface that only receives cluster traffic.

Add multicast route

Multicast networking requirements vary across operating systems. Some operating systems require little configuration, while some require the multicast address to be explicitly added to a network interface before Confluence can use it.

If the Multicast Test tool shows that multicast traffic can't be sent or received correctly, adding a route for multicast traffic on the correct interface will often fix the problem. The example below is for a Ubuntu Linux system:

```
route add -net 224.0.0.0 netmask 240.0.0.0
dev eth0
```

To support multiple applications using multicast on different interfaces, you may need to specify a route specific to the Confluence multicast address.

Check firewall

Ensure your firewall allows UDP traffic on the multicast address and port used by Confluence.

Prefer IPv4

> ⛔ There's a known issue with IPv6, especially on Linux.

The fix is to add `-Djava.net.preferIPv4Stack=true` to `JAVA_OPTS`. This tells the JVM to try binding an IPv4 address first, and resort to IPv6 only if that fails.
Note: *A more radical approach is to add NETWORKING_IPV6=no to /etc/sysconfig/network, yet probably should be left for a later consideration on a production machine.*

Change multicast interface

Confluence might have selected the incorrect interface for multicast traffic, which means it cannot connect to other nodes in the cluster. To override the interface used for multicast traffic after initial setup, edit `confluence.cfg.xml` in the Confluence home directory and add a property (or change the existing one) to select your desired network interface. For example to tell Confluence to use `eth1`:

```
<property
name="confluence.cluster.interface">eth1</
property>
```

Increase multicast TTL

The multicast time-to-live (TTL) specifies how many *hops* a multicast packet should be allowed to travel before it is discarded by a router. It should be set to the number of routers in between your clustered nodes: 0 if both are on the same machine, 1 if on two different machines linked by a switch or cable, 2 if on two different machines with one intermediate router, and so on.

Create a file in the Confluence home directory called `tangosol-coherence-override.xml`. Add the following to it, setting the TTL value appropriately (1 is the default):

```
<?xml version='1.0'?>
<coherence>
<cluster-config>
  <multicast-listener>
    <time-to-live
system-property='tangosol.coherence.ttl'>1
</time-to-live>
  </multicast-listener>
</cluster-config>
</coherence>
```

Alternatively, simply start Confluence with the system property: `-Dtangosol.coherence.ttl=1`. Again, 1 is the default value, and you should change it to something appropriate to your network topology.

Check intermediate routers

Advanced switches and routers have the ability to understand multicast traffic, and route it appropriately. Unfortunately sometimes this functionality doesn't work correctly with the multicast management information (IGMP) published by the operating system running Confluence.

If multicast traffic is problematic, try disabling advanced multicast features on switches and routers in between the clustered nodes. These features can prevent multicast traffic being transmitted by certain operating systems.

For best results, use the simplest network topology possible for the cluster traffic between the nodes. For two nodes, that means a single network cable. For larger numbers, try using a single high-quality switch.

Advanced Tangosol configuration

If the solution to your problem involves changes to the Tangosol configuration, these changes should **not** be made to the Confluence configuration in `confluence/WEB-INF/classes/`. Instead, to ensure your configuration survives upgrades, make your changes via:

- Tangosol system properties
- creating a `tangosol-coherence-override.xml` file in the Confluence home directory.

Examples of making these changes are shown in the increasing the TTL section.

Didn't find a solution?

Check Related Articles from the Confluence Knowledge Base

No content found for label(s) cluster.

Open JIRA Features and Bug Reports

JIRA Issues (50 issues)

Type	Key	Summary	Assignee	Reporter	Priority	Status	Resolution	Created	Updated	Due
↗	CONF-14338	Specify an arbitrary multicast port for a cluster	Unassigned	James Fleming [Atlassian]		Open	Unresolved	Jan 30, 2009	Jan 30, 2009	
↗	CONF-9712	Plugins which don't work in a cluster shouldn't look like an error	Unassigned	Gary Weaver		Open	Unresolved	Oct 15, 2007	Oct 16, 2007	
↗	CONF-11206	Confluence Clustered and JIRA trust delegation	Unassigned	Ivan Benko [Atlassian]		Open	Unresolved	Mar 25, 2008	May 12, 2010	
✚	CONF-10977	Generate new Multicast address from a "new" cluster name	Unassigned	Ivan Benko [Atlassian]		Open	Unresolved	Mar 06, 2008	Sep 11, 2008	
↗	CONF-20501	Consider upgrading coherence	Unassigned	Partha Kamal [Atlassian]		Open	Unresolved	Jul 30, 2010	Jul 30, 2010	
↗	CONF-21670	Confluence should explicitly check for other confluence instances using the same	Unassigned	Don Willis [Atlassian]		Open	Unresolved	Jan 20, 2011	Jan 25, 2011	

		home directory								
＋	CONF-10979	List confluence cluster interface	Unassigned	Ivan Benko [Atlassian]		Open	Unresolved	Mar 06, 2008	Mar 06, 2008	
↗	CONF-10635	Database logging of clustersafety access	Unassigned	James Fleming [Atlassian]		Open	Unresolved	Feb 03, 2008	Feb 03, 2008	
↗	CONF-8716	Determine index mismatch in cluster and warn on cluster info page	Unassigned	Matt Ryall [Atlassian]		Open	Unresolved	Jun 17, 2007	Oct 29, 2007	
↗	CONF-10981	Check how many nodes/processes running in a cluster and their identity	Unassigned	Ivan Benko [Atlassian]		Open	Unresolved	Mar 06, 2008	Mar 06, 2008	
＋	CONF-10953	Support unicast addressing in cluster when well-known-addresses WKA are defined	Unassigned	Ivan Benko [Atlassian]		Open	Unresolved	Mar 06, 2008	Aug 25, 2009	
↗	CONF-23223	Remove the option to store attachments on	Unassigned	Carlos Alberto Feijo Schedle		Open	Unresolved	Sep 14, 2011	Sep 15, 2011	

		filesystem when using a cluster		r [Atlassian]						
↗	CONF-9297	Confluence should be able to automatically recover from cluster panics	Unassigned	Gary Weaver		Open	Unresolved	Aug 27, 2007	Mar 25, 2009	
↗	CONF-20500	A cluster panic should not bring down other nodes	Unassigned	Partha Kamal [Atlassian]		Open	Unresolved	Jul 30, 2010	Nov 08, 2010	
↗	CONF-10980	Cluster debugging/troubleshooting tools	Unassigned	Ivan Benko [Atlassian]		Open	Unresolved	Mar 06, 2008	Mar 06, 2008	
✚	CONF-14948	Support failover NICs for cluster configuration...	Unassigned	Tony Atkins [Atlassian]		Open	Unresolved	Mar 19, 2009	Mar 19, 2009	
✚	CONF-19559	Provide support for Confluence clustered in a virtualized environment...	Unassigned	Tony Atkins [Atlassian]		Open	Unresolved	May 06, 2010	Jan 31, 2012	
↗	CONF-12689	Support Confluence cluster upgrades	Unassigned	Igor Minar		Open	Unresolved	Aug 06, 2008	May 04, 2010	

		without an outage								
✚	CONF-9335	In cluster, allow attachments to be stored on file system in network-shared directory	Unassigned	Jeremy Largman [Atlassian]		Open	Unresolved	Aug 29, 2007	Apr 02, 2012	
☒	CONF-16794	Document new cluster distributions	Giles Gaskell [Atlassian]	Jeremy Largman [Atlassian]	⇧	Open	Unresolved	Sep 04, 2009	May 12, 2010	
●	CONF-12287	Coherence cache fails while retrieving profile picture metadata (dashboard or view page shows UnexpectedRollbackException)	Unassigned	Matt Ryall [Atlassian]	⇧	Open	Unresolved	Jul 01, 2008	Apr 05, 2011	
●	CONF-14120	Hibernates UpdateTimestampsCache doesn't handle concurrent writes	Unassigned	Chris Kiehl [Atlassian]	⇧	Open	Unresolved	Jan 05, 2009	May 05, 2009	
●	CONF-8959	Attachment migration does	Unassigned	Nicholas Ilacqua [Atlassian]	⇧	Open	Unresolved	Jul 19, 2007	Feb 29, 2012	

		not happen when upgrading to a clustered license								
●	CONF-17089	Reindexing in cluster only runs on one node if triggered from web UI	Unassigned	Anatoli Kazatchkov [Atlassian]	⬆	Open	Unresolved	Oct 01, 2009	May 12, 2010	
⊠	CONF-15523	Run cluster performance build on two machines	Unassigned	Matt Ryall [Atlassian]	⬆	Open	Unresolved	May 05, 2009	May 12, 2010	
●	CONF-9324	Lots of ObjectDeletedException's during cluster builds	Unassigned	Matthew Jensen [Atlassian]	⬆	Open	Unresolved	Aug 28, 2007	May 12, 2010	
●	CONF-10868	Node that can not join cluster due to license restriction causes cluster panic	Unassigned	Ivan Benko [Atlassian]	⬆	Open	Unresolved	Feb 29, 2008	Sep 03, 2008	
●	CONF-9040	Authenticator (subclass of DefaultAuthenticator) can be called twice at almost	Unassigned	Gary Weaver	⬆	Open	Unresolved	Jul 30, 2007	Nov 04, 2007	

		exactly same time by 2 or more clustered servers								
●	CONF-9813	Disable attachments migration to Filesystem in Cluster	Unassigned	Gurleen Anand [Atlassian]	⇧	Open	Unresolved	Oct 24, 2007	Sep 04, 2011	
●	CONF-12614	Intermittent ConcurrentModificationException in cluster	Unassigned	Anatoli Kazatchkov [Atlassian]	⇧	Open	Unresolved	Jul 29, 2008	Mar 31, 2009	
●	CONF-10325	Viewing the members of a group in a clustered environment works only on one node and not the other.	Unassigned	Partha Kamal [Atlassian]	⇧	Open	Unresolved	Dec 27, 2007	Jul 02, 2009	
●	CONF-9594	ConditionalPropertySet's cannot be cached breaking cluster installations that delegate user	Unassigned	Dave Loeng [Atlassian]	⇧	Open	Unresolved	Sep 28, 2007	Jul 02, 2009	

		management to JIRA								
●	CONF-14657	Retrieving the global settings in a clustered environment causes a lot of contention	Unassigned	Chris Kiehl [Atlassian]	↑	Open	Unresolved	Feb 21, 2009	Nov 08, 2009	
●	CONF-13421	Layout customisations are not propagated to other cluster nodes	Unassigned	Matt Ryall [Atlassian]	↑	Open	Unresolved	Oct 16, 2008	Dec 09, 2008	
●	CONF-10323	Coherence Lock being held when it appears no thread should have the lock. Causes ConcurrentModificationException	Unassigned	Paul Curren [Atlassian]	↑	Open	Unresolved	Dec 26, 2007	Oct 25, 2010	
●	CONF-12486	ClassNotFoundException logged on cluster node startup	Unassigned	Anatoli Kazatchkov [Atlassian]	↑	Open	Unresolved	Jul 17, 2008	Aug 25, 2009	
●	CONF-16419	Installing a font for PDF export in a cluster will not	Unassigned	Charles Miller [Atlassian]	↑	Open	Unresolved	Jul 20, 2009	Aug 05, 2009	

		carry to cluster nodes that are down or unavailable.								
⊠	CONF-12345	Park issue :)	Unassigned	Dave Loeng [Atlassian]	⬆	Open	Unresolved	Jul 07, 2008	Jan 21, 2009	
●	CONF-23033	Viewfile macro does not work in Confluence Clustered when Office Connector is configured to use Cache in Memory for temporary storage	Unassigned	Roy Hartono [Atlassian]	⬆	Open	Unresolved	Aug 09, 2011	Feb 29, 2012	
●	CONF-17040	Cannot build milestones outside Atlassian due to coherence	Unassigned	Jonathan Gilbert [Atlassian]	⬇	Open	Unresolved	Sep 25, 2009	Dec 08, 2009	
●	CONF-17577	Cluster build passed but didn't close down Confluence	Unassigned	Brian Nguyen [Atlassian]	⬇	Open	Unresolved	Nov 10, 2009	May 12, 2010	
●	CONF-13870	After a site Import into a cluster,	Unassigned	Agnes Ro [Atlassian]	⬇	Open	Unresolved	Nov 27, 2008	Sep 04, 2011	

		admin console displays attachment storage as filesystem								
●	CONF-22466	Content Permission changes are propagated between nodes one at a time, should be in bulk	Unassigned	Richard Atkins [Atlassian]	↓	Open	Unresolved	May 09, 2011	May 10, 2011	
●	CONF-13698	Changing custom html on one node of a cluster is not imideatly reflected on the other node.	Unassigned	Anatoli Kazatchkov [Atlassian]	↓	Open	Unresolved	Nov 12, 2008	Nov 13, 2008	
●	CONF-22979	Migrating to a cluster with existing data does not add cluster attributes to the confluence.cfg.xml	Unassigned	Adam Laskowski [Atlassian]	↓	Open	Unresolved	Jul 27, 2011	Jul 28, 2011	
●	CONF-7368	Confluence Cluster setup	Unassigned	Don Willis [Atlassian]	↓	Open	Unresolved	Nov 23, 2006	Jan 19, 2009	

		dies horribly when DNS fails								
●	CONF-9281	Plugin's I18n properties not loaded in other cluster nodes unless restarted	Unassigned	Roberto Dominguez	↓	Open	Unresolved	Aug 26, 2007	Apr 16, 2011	
I	CONF-9749	Coherence does not allow the disabling of all JDK shutdown hooks	Unassigned	Christopher Owen [Atlassian]	↓	Open	Unresolved	Oct 17, 2007	Jan 29, 2008	
●	CONF-14088	Locking on cache keys needs to check if the lock was actually aquired	Unassigned	Chris Kiehl [Atlassian]	↓	Open	Unresolved	Dec 30, 2008	Nov 22, 2009	
●	CONF-8300	Cannot override TTL configuration through tangosol coherence properties	Unassigned	Matthew Jensen [Atlassian]	↑	Needs Verification	Unresolved	Apr 20, 2007	Nov 10, 2009	

Contact Atlassian support

We have dedicated staff on hand to support your installation of Confluence. Please follow the instructions for raising a support request and mention that you're having trouble setting up your Confluence cluster.

Related

Cluster Safety Mechanism

Multicast Test

This page describes the **Multicast Test**, a Coherence tool for testing multicast traffic from one node to another. You may find this useful when troubleshooting a clustered installation of Confluence.

In order to run the Multicast test, you need to first download the attached Coherence zip file.

The Multicast Test comes as a script called `multicast-test`, which you will find located in the `bin` folder in the above zip file.

Instructions on how to run this script file can be found in the Coherence documentation. You may like to go straight to the subheading called '**Example**' in the guide, where there is an example on how to use the `multicast-test` script.

> ⚠ *The information on this page does not apply to Confluence OnDemand.*

RELATED TOPICS

Cluster Troubleshooting
Confluence Clustering Overview

Clustering for Scalability vs Clustering for High Availability (HA)

People occasionally enquire about setting up High-Availability (HA) Confluence clusters. Confluence's clustering is designed to solve a different problem, that of scaling under high load. This page explains the difference.

What is High Availability (HA)?

HA means that your application *will be* available, without interruption. It's a very difficult thing to achieve, and is typically what people are talking about when they refer to five-nines availability.

In the context of application clustering, it means that any given node (or combination of nodes) can be shut down, blown up, or simply disconnected from the network unexpectedly, and the rest of the cluster will continue operating cleanly as long as at least one node remains. It requires that nodes can be upgraded individually while the rest of the cluster operates, and that no disruption will result when a node rejoins the cluster. It typically also requires that nodes be installed in geographically separate locations.

What does Confluence's clustering do, then?

Confluence's clustering system allows a single installation to serve a much greater number of concurrent requests than a single server. This is what we refer to as 'scaling under load'.

It does provide a certain amount of resilience, as the death of one node won't bring the other(s) down. However, it requires very low network latency, which rules out geographic separation of the servers, and upgrading can only be performed while the entire cluster is shut down. This doesn't mean that Confluence's clustering is buggy or broken. It simply reflects the difference between the two design aims.

On this page:

The information on this page does not apply to Confluence OnDemand.

So what kind of resilience can I build into a Confluence installation?

It's still entirely possible to build a resilient Confluence installation, using a 'cold-failover' approach in which two (or more) servers share a database and (normally) a network-mounted file system, where no more than one server is actually running at any given time.

Several different approaches are feasible, but the common elements are:

- a well-configured load balancer (session affinity is irrelevant in this case)
- a reliable monitoring system which can detect and shut down a misbehaving Confluence instance before starting the spare server
- startup scripts with added smarts to check for the presence of another running node before deciding whether to start up a server
- servers with the same view of both the database and the home directory.

It's vital to ensure that only one server is running at any one time, in this kind of setup. If a server starts while another is already running against the same database, the result will be a cluster panic that shuts down both servers.

A single database becomes the single point of failure in such a system. This can be alleviated by database clustering, or by replication from the 'active' database server to the standby server(s) if you wish to separate the failover systems while keeping database latency to a minimum.

In the same vein, the home directory can be hosted on a shared network system — SAN or NAS, preferably with its own replication/rapid recovery system — though there's a known issue to consider. Alternatively, to avoid the use of networked file systems, a utility such as `rsync` can be used to periodically bring the spare servers' home directories up to date, so long as you keep the period sufficiently short — probably between one and five minutes, depending on the rate of activity. This can be avoided altogether by keeping attachments in the database; it increases the demands on the bandwidth between the application and database servers, but guarantees that the system is in a consistent state at switchover. If the data is at all sensitive or confidential, it's advisable to run `rsync` over `ssh`, to minimise the opportunity for the data to be captured on its way across the network.

What's the difference between load balancing and failover?

Load balancing means that all servers are active, and new requests are distributed among them. Several strategies are available, but the most common are:

- round-robin — the first request goes to the first server, the second request goes to the second server, and so on. When you run out of servers, the next request goes to the first server, and around it goes again.
- percentage-based — if (for example) you have two servers, and one can handle twice the load of the other, you can tell the load balancer to send two requests to the stronger server for every request that goes to the weaker one.
- availability — the load balancer sends a test query to each of the servers every second or so, and directs

each new request to the server that's currently responding the fastest.

Failover means that only one server is active at any given time, and normally involves two servers (any number of servers may be involved, depending on the system). If the active one stops responding, requests are directed to the other server — the system 'fails over' to the second one.

'Cold failover' means that the second server is only started up after the first one has been shut down. This is the case for non-clustered Confluence.

'Hot failover' or 'hot standby' means that all servers are running at all times, and that the load is directed entirely toward one server at any one time.

A load balancer can be used in both scenarios, especially if it's smart enough to keep track of which servers are currently running.

Failover can also be managed via DNS, in a sufficiently well-controlled environment.

What do you mean by 'session affinity'?

Sessions consist of several transmissions in each direction between the client (browser) and the server. Session affinity means that the load balancer keeps track of which server received the initial transmission from a given browser, and that it will then send any subsequent requests from that browser to the same server.

This is necessary with Confluence clustering, in particular, because sessions are not shared across cluster nodes. If you log into one node and then send a request to another, the other node will send you the login screen because it doesn't recognise your session cookie.

RELATED TOPICS

Confluence Clustering Overview

Recommended network topology

Atlassian recommends a network topology similar to the one shown below, to get the best results from a Confluence Clustered deployment.

The number of Confluence nodes in the deployment is adjustable — select the number which suits your own requirements.

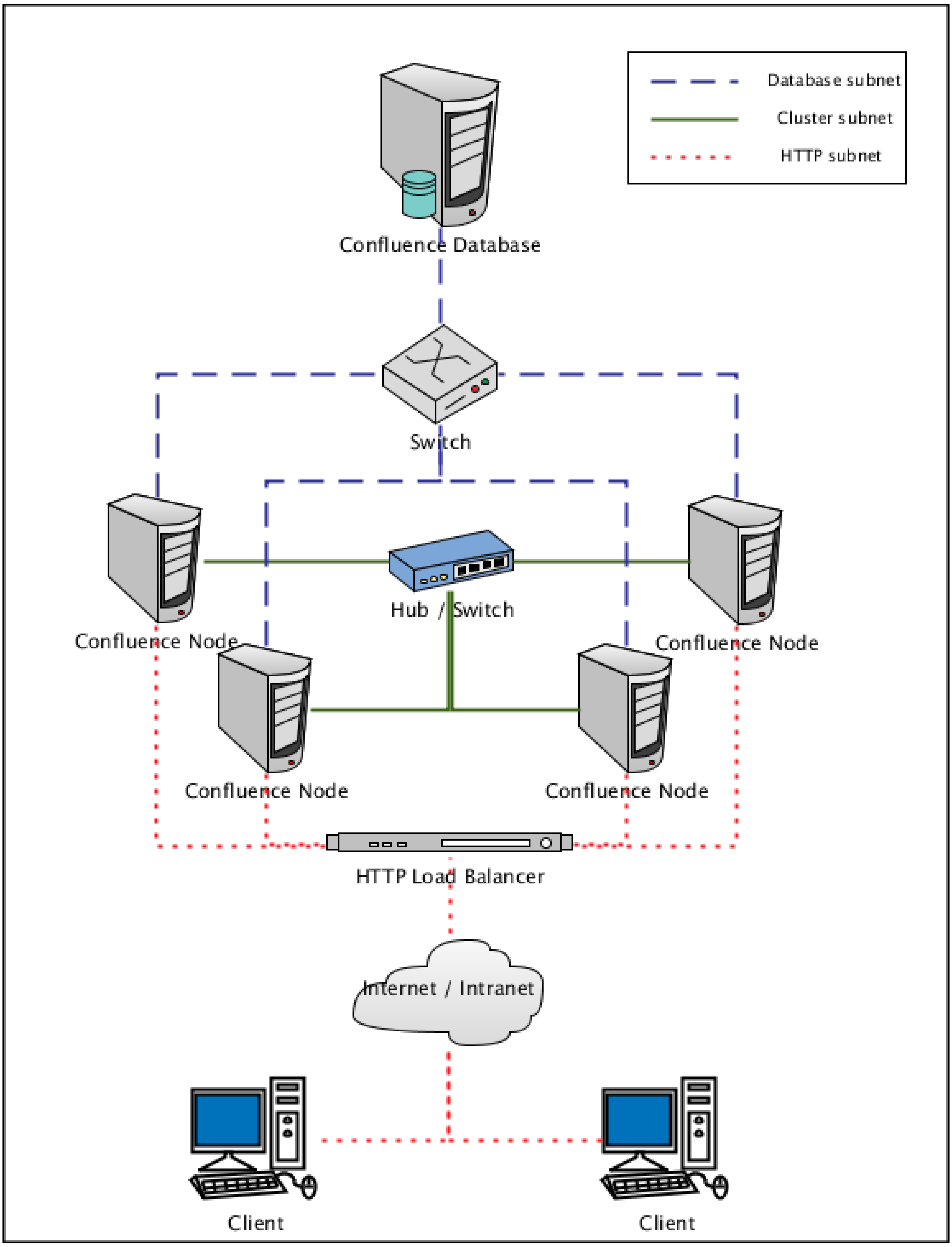
The most important aspect is that cluster, database and HTTP (client) traffic are all carried on separate subnets. It is possible, on a sufficiently fast network, to carry cluster and database traffic on the same subnet but we do strongly recommend that HTTP traffic be always confined to a separate subnet on production deployments.

Confluence Clustered does not support clustered communication over WAN, VLAN or VPN. All Confluence Clustered nodes must be on the same local subnet, ideally networked via an ethernet hub or simple switch. The cluster communication network must also support multicast IP networking.

⚠ *The information on this page does not apply to Confluence OnDemand.*

✓ **Use this example as a basis for your own network diagram**

When you are considering a Confluence Clustered deployment, you should prepare a network diagram like the one on this page. This will facilitate discussion with Atlassian Support and help with your own planning. Please refer to the cluster checklist for more guidance on planning your clustered deployment.



Cluster Administration page

Overview

Any instance of Confluence which uses a clustered license has a Cluster Configuration page which includes information about the active cluster.

To open the Cluster Administration page,

1. Choose **Browse** > **Confluence Admin**.
2. Click '**Cluster Configuration**' in the left-hand menu, in the section called 'Clustering'.

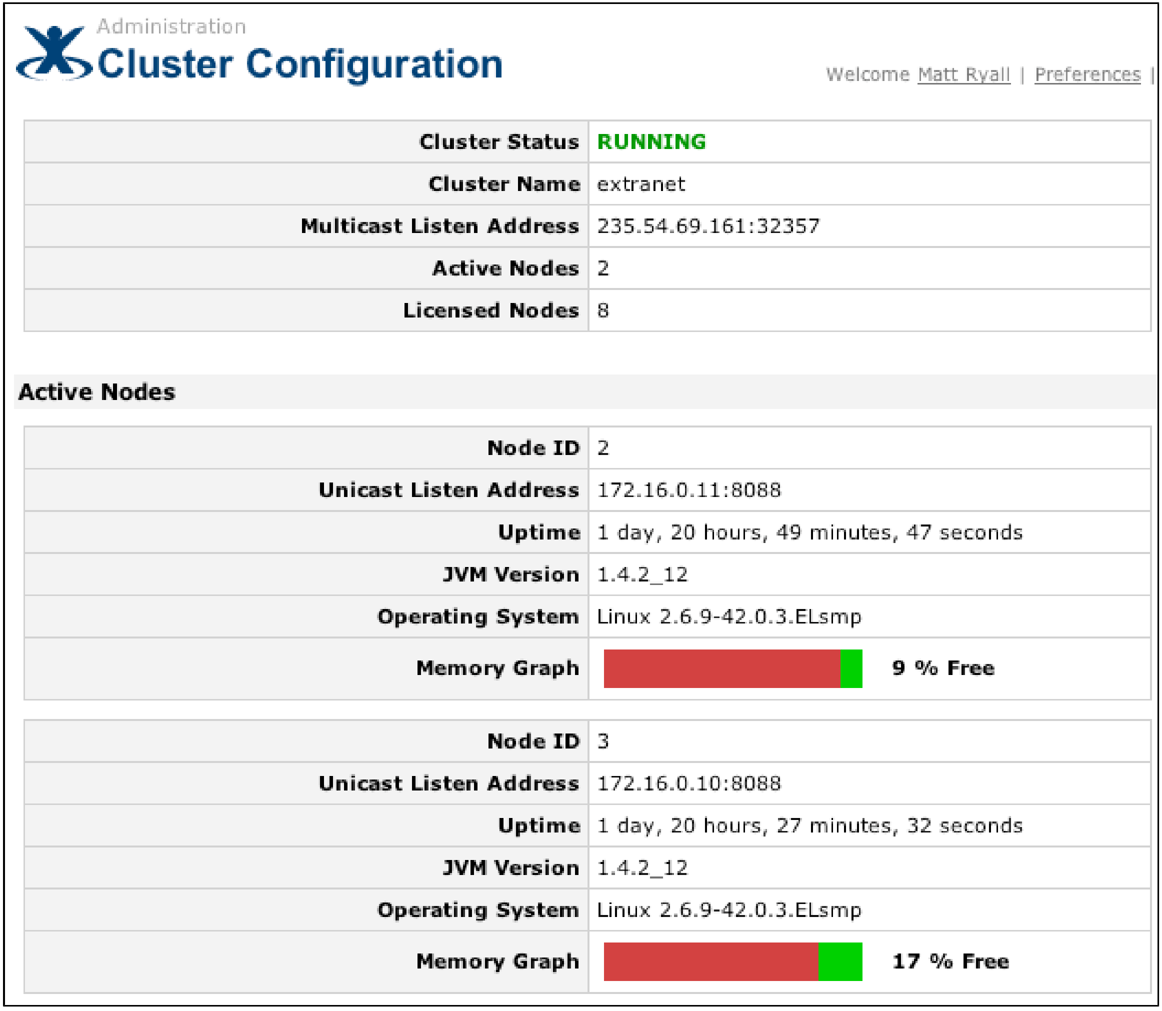
⚠ *The information on this page does not apply to Confluence OnDemand.*

Availability

To access this functionality, you must:

- Be a System Administrator (i.e. have global System Administrator permissions), and
- be using Confluence 2.3 or later, and
- be using a clustered Confluence license.

Screenshot: Cluster Administration Page



Cluster Configuration

Cluster Status	RUNNING
Cluster Name	extranet
Multicast Listen Address	235.54.69.161:32357
Active Nodes	2
Licensed Nodes	8

Active Nodes

Node ID	2
Unicast Listen Address	172.16.0.11:8088
Uptime	1 day, 20 hours, 49 minutes, 47 seconds
JVM Version	1.4.2_12
Operating System	Linux 2.6.9-42.0.3.ELsmp
Memory Graph	**9 % Free**

Node ID	3
Unicast Listen Address	172.16.0.10:8088
Uptime	1 day, 20 hours, 27 minutes, 32 seconds
JVM Version	1.4.2_12
Operating System	Linux 2.6.9-42.0.3.ELsmp
Memory Graph	**17 % Free**

This page shows your cluster configuration, and allows you to start a new Confluence cluster using data from this instance.

Cluster Status indicates whether your cluster is currently running.

Licensed nodes is the maximum number of instances of Confluence your license allows in a cluster.

Active nodes lists the instances of Confluence currently participating in the cluster.

Starting a new cluster will perform the following changes:

- enable a clustered cache
- migrate attachments from file system to the database

- publish database connection information so other nodes can join the cluster.

All access to Confluence will be locked while this takes place, and you will be forced to restart Confluence afterwards.

Cluster name is a short name for identifying your cluster. Other Confluence instances can join the cluster using this name.

To join an existing cluster, start a clean copy of Confluence on this node and select 'Join Cluster' during the setup wizard.

Related documents

Overview of Confluence Clusters
Confluence Cluster Installation
Cluster Troubleshooting

Cluster Checklist

It is possible to run Confluence in a **clustered** environment instead of on a single server. This means that you can run multiple copies of Confluence in a cluster, so that clients (such as a browser) can connect to any copy and see the same information.

Refer to the clustering overview for more information and a list of related pages about clustering Confluence.

> **Consider your options carefully before deciding on a clustered installation**
>
> While we have tried to make clustering Confluence as easy and administrator-friendly as possible, it is a major architectural change and requires extra planning for deployment and upgrades. Please consider the information below and then consult Atlassian Sales before making your final decision.

On this page:

The information on this page does not apply to Confluence OnDemand.

Purpose of this Document

The purpose of this cluster checklist is to help you:

- Decide whether Confluence Clustered is the right solution for you.
- Create a plan for your clustered deployment.

If you need to raise a support request with Atlassian during or after cluster deployment, we will need to ask you questions about your configuration. It will save crucial time if you can provide us with your deployment plan.

For more information about clustering Confluence, refer to the clustering overview.

Assumed Knowledge

In writing this document, we have assumed that our readers have an in-depth knowledge of the following technical areas:

- Database
- Networking
- Application servers
- Load balancers

Before starting a clustered deployment please read the information on this page carefully, as well as the linked documentation, to assess if you have the assumed knowledge.

General Considerations

What will Confluence Clustered do for you?

The points in this section of the page will help you evaluate your reasons for considering a clustered deployment, and then decide whether Confluence Clustered is the right solution for your environment.

Confluence Clustered is designed to scale the number of simultaneously connected users at a much better performance than what a single node can achieve

Confluence Clustered will not improve performance in systems with few users.

Clustering Confluence means that user requests can be served by independent machines. The performance gains are substantial, and have improved a lot further since Confluence 3.0. Clustering is especially great in dealing with spikes to the load, e.g. during certain hours of business. Just note that if rendering a complicated page (e.g. containing many macros or rendering many graphs) takes five seconds on an otherwise idle server, will not be faster in a clustered environment. Also, the first step when you encounter performance issues is to tune your existing system, make sure you are using the right hardware and have looked at your database.

Confluence Clustered is not a high availability solution.

Confluence Clustered is not designed specifically to provide a high availability solution.

General availability is higher in a Confluence cluster than on a single installation, you can for example take one node down for minor maintenance tasks e.g. when adding a new CPU or adding RAM. But you still have to brir down all nodes at the same time for software upgrades. Also there are certain conditions, like loss of network connectivity between nodes ('split brain'), that will result in the cluster shutting itself down. Confluence Clustere offers higher reliability, but not high availability.

Confluence Clustered is not for disaster recovery nor for transparent failover.

If one node crashes, there is no transparent failover for the connected client. Also, our network requirements (see below) make Confluence unsuitable for deployment to different cities or even to different buildings.

Server Setup

The number of supported cluster nodes is limited to four.

⚠ **Not supported.** In theory, you can connect more than four nodes — but that is not covered by Atlassian Support.

All cluster nodes must have the same version of OS, application server, etc.

Confluence requires a homogeneous environment. All Confluence cluster nodes must have the same version c the following:

- Operating system

- CPU
- Installed memory
- Java
- Application server

ℹ Note that 'same version' means '**same to the last digit**'. For example, Java v1.4.2_16 is not the same as v1.4.2_15
✅ We strongly recommend user to have the same memory configuration (both the JVM and the physical memory) because a cluster uses a replicated cache. A replicated cache requires the same amount of memory on each node in the operating cluster. The memory allocations must be equal.

Use good and up-to-date hardware.

While the details are up to you, we strongly suggest that your servers have at least 4GB of physical RAM. A hig number of concurrent users means that a lot of RAM will be consumed. You usually don't need to assign more than 4GB per JVM process, and most of the time even just 1GB or 2GB will be fine, you should just be prepare to fine tune the settings.

Confluence Clustered is not supported when run in VMware or other virtualisations.

⚠ **Not supported.** We strongly discourage you to deploy a production environment of Confluence to virtual servers, and we will not be able to support you when problems arise.

When running a Confluence cluster your goal is high capacity and performance, so you should not risk lower performance by virtualising it and sharing a computer with other processes.

Many customers who are running Confluence on VMware, or similar virtualisation solutions, experience major performance problems that are extremely hard to pinpoint. Since the problems are not related to Confluence itself, we will not be able to help you.

Confluence should be the only application on the cluster servers.

No additional applications (other than core operating system services) should be running on the same servers Confluence.

Since your goal should be increased capacity and performance, you should not risk this by running any other process on the machine with a Confluence Clustered node. While it may be fine to run JIRA, Confluence and Bamboo on a dedicated Atlassian software server for small installations, it is strongly discouraged for clustering Confluence.

Do not upgrade and switch to Confluence Clustered at the same time

If you plan to migrate to a clustered solution, make sure you are migrating within the same version of Confluence. If you plan to upgrade to a higher version of Confluence, do this **before** the migration to the clustered version.
For example, if you are currently running Confluence 2.9.2, and want to roll out the clustered version of Confluence 3.0, you must first upgrade to Confluence 3.0 and check that everything works fine (e.g. by running and monitoring your production system for a week). Then you are in a good position to migrate to the clustered version.

Database Setup

Run the database on its own physical server.

You are optimising for performance, so you don't want the database to slow down your application servers, or vice versa. In high load scenarios, the database may need to have better hardware than the application servers to be able to handle all requests. You should find out by performing loadtesting.

Attachments must be stored in a database and not the local file system

Storing attachments in the database is the only supported attachment storage configuration for clustering Confluence.

Make sure that you use a supported version of a database server to store Confluence's data.

Please check that your intended database is officially supported by Atlassian Confluence. The load on an average cluster solution is higher than on a single box installation, and it is therefore even more crucial to use the right database vendor and version.

Your database must be provisioned to store a large volume of binary data.

Note that Confluence clustered stores file attachments in the database, and you need an experienced DBA wh can monitor and manage the data growth.

You need an experienced DBA available to troubleshoot database performance issues.

Not having an experienced full-time DBA at hand at short notice when entering the realm of high load is dangerous. While small installations of Confluence basically work 'out of the box', anything that involves high load and a lot of database space requires continual monitoring, optimising and fine tuning of the Confluence database. When we ramp up the load on our loadtesting environment, we see that database usage goes up as well. Having powerful hardware in place helps, but if there are queries that become inefficient with you particula load pattern, you need an expert to tune it. As an example, we have seen PostgresSQL switch its internal caching mechanism when a particular table reached a certain size, which resulted in a drop of performance by about 200ms per request. This happened from one second to the other. Being able to troubleshoot and then fix issues like these is important in any enterprise system, but it is even more in a high load scenario.

Network Setup

We recommend hardware load balancers or putting a software loadbalancer onto its on server.

If you use a software load balancer (which is fine except for really extreme installations), it must be deployed o a machine of its own. Running a software load balancer on a cluster node is not supported. If a node unexpectedly got overwhelmed by a spike in load, a load balancer on that node would turn unresponsive. As a result, your whole cluster would be inaccessible even though the other nodes would be available. So using a different server is common practice and common sense.

Use separate network adapters for communication between servers.

The Confluence cluster nodes should have a separate physical network (i.e. separate NICs) for inter-server communication.

This is the best way of getting the cluster to run fast and reliably. Performance problems are likely to occur if yo connect cluster nodes via a network that has lots of other data streaming through it.

The switch connecting the Confluence cluster nodes must not be a 'smart switch'.

⚠ **Not supported.** Smart switches are not covered by Atlassian Support for Confluence Clustered.

Do not use smart switches between cluster nodes. Many problems have been reported and attributed to smart switches. They have a tendency to interrupt broadcast or multicast traffic, thus reliably killing a cluster after a certain amount of time has passed. This makes troubleshooting especially complex and tedious.

Cisco switches need additional configuration.

If the switch connecting the Confluence cluster nodes is a Cisco switch then it might need additional configuration to support Confluence clustering.

Please make sure you find out all the details about your switches before you start the deployment.

It is recommended that the database is on a different physical network from the Confluence server nodes.

Since you want to increase your capacity and performance for high loads, it is recommended to have your database on a different network. Please refer to the recommended topology diagram for more information.

Minimize the latency between the Confluence cluster nodes and the database.

Even though having the nodes and the database on the same physical network usually suffices, you should tak the time to explicitly measure network latency, and make sure it is as close to zero as possible.

Prepare a network diagram.

To facilitate discussion and to ease planning, you should prepare a network diagram like this example of recommended network topology.

If you request support with Confluence Clustered, we may ask for your network diagram. We recommend that you create one similar to our example before you proceed with the installation.

You need network support staff available to troubleshoot cluster communication issues.

Setting up a cluster is not trivial. Even small problems in network design will be expanded in a clustered installation. (This is true of any kind of software.)

It is absolutely vital that you have dedicated network staff available to track down problems when they arise. A cluster will usually be used by thousands of users, and you don't want to keep them waiting because a network card breaks, or because someone made an undocumented change to the network and you don't have an expe around who can figure it out.

Staging Environment

You need a staging environment that is exactly the same as your production system.

You must be able to test drive any change to the cluster (installing upgrades, installing plugins) and to perform other tests (checking connectivity, debugging problems) on a staging cluster.

The staging environment must be:

- On the same OS, database, and Java version as your production environment.
- Clustered.

If you require support, we may for example ask you to turn off certain third-party plugins. If you can't do this in your production environment and you don't have a staging environment for troubleshooting, we may not be abl to help you.

Getting a license for your staging environment
Only a **technical contact** for your commercial/academic license is able to create a Developer license.

Atlassian supplies 'developer' licenses which can be used by existing commercial license holders who wish to deploy non-production installations of our software to use in QA/staging environments. Developer licenses are free of charge to commercial license holders and, like our commercial offerings, they include 12 months of updates starting from the date of purchase of the commercial license.

If you hold a commercial license, you can obtain a free developer license by following these steps:

1. Log in to your Atlassian account.
2. Under the "Licenses" heading, all of your licenses will be displayed. Click the plus sign next to a license to view its details.
3. Click the **'View Developer License'** link in the bottom right corner of the license detail panel, below your commercial license key.

Related Topics

No content found for label(s) cluster.

Confluence Security

This document is for system administrators looking to evaluate the security of the Confluence web application. The page addresses overall application security and lists the security advisories issued for Confluence. As a public-facing web application, Confluence's application-level security is important. This document answers a number of questions that commonly arise when customers ask us about the security of our product.

Other topics:

- For information about user management, groups and permissions, please refer to the internal security overview.
- For guidelines on configuring the security of your Confluence site, see the administrator's guide to configuring Confluence security.

On this page:

⚠ *The information on this page does not apply to Confluence OnDemand.*

Application Security Overview

Password Storage

When Confluence's internal user management is used, passwords are hashed through SHA1 before being stored in the database. There is no mechanism within Confluence to retrieve a user's password – when password recovery is performed, a new random password is generated and mailed to the user's registered address.

When external user management is enabled, password storage is delegated to the external system.

Buffer Overflows

Confluence is a 100% pure Java application with no native components. As such it is highly resistant to buffer overflow vulnerabilities – possible buffer overruns are limited to those that are bugs in the Java Runtime Environment itself.

SQL Injection

Confluence interacts with the database through the Hibernate Object-Relational mapper. Database queries are generated using standard APIs for parameter replacement rather than string concatenation. As such, Confluence is highly resistant to SQL injection attacks.

Script Injection

Confluence is a self-contained Java application and does not launch external processes. As such, it is highly resistant to script injection attacks.

Cross-Site Scripting

As a content-management system that allows user-generated content to be posted on the web, precautions have been taken within the application to prevent cross-site scripting attacks:

- The wiki markup language in Confluence does not support dangerous HTML markup
- Macros allowing the insertion of raw HTML are disabled by default
- HTML uploaded as a file attachment is served with a content-type requesting the file be downloaded, rather than being displayed inline
- Only system administrators can make HTML-level customisations of the application

When cross-site scripting vulnerabilities are found in the Confluence web application, we endeavour to fix them as quickly as possible.

Transport Layer Security

Confluence does not directly support SSL/TLS. Administrators who are concerned about transport-layer security should set up SSL/TLS at the level of the Java web application server, or the HTTP proxy in front of the Confluence application.

For more information on configuring Confluence for SSL, see: Running Confluence Over SSL or HTTPS

Session Management

Confluence delegates session management to the Java application server in which it is deployed. We are not aware of any viable session-hijacking attacks against the Tomcat application server shipped with Confluence. If you are deploying Confluence in some other application server, you should ensure that it is not vulnerable to session hijacking.

Plugin Security

Administrators install third party plugins **at their own risk**. Plugins run in the same virtual machine as the Confluence server, and have access to the Java runtime environment, and the Confluence server API.

Administrators should always be aware of the source of the plugins they are installing, and whether they trust those plugins.

Administrator Trust Model

Confluence is written under the assumption that anyone given System Administrator privileges is trusted. System administrators are able, either directly or by installing plugins, to perform any operation that the Confluence application is capable of.

As with any application, you should not run Confluence as the root/Administrator user. If you want Confluence to listen on a privileged network port, you should set up port forwarding or proxying rather than run Confluence with additional privileges. The extra-careful may consider running Confluence inside a `chroot` jail.

Stack Traces

To help debug support cases and provide legendary support, Confluence provides stack traces through the web interface when an error occurs. These stack traces include information about what Confluence was doing at the time, and some information about your deployment server.

Only non-personal information is supplied such as operating system and version and Java version. With proper network security, this is not enough information to be considered dangerous. No usernames or passwords are included.

Finding and Reporting a Security Vulnerability

Atlassian's approach to reporting security vulnerabilities is detailed in How to Report a Security Issue.

Publication of Confluence Security Advisories

Atlassian's approach to releasing security advisories is detailed in Security Advisory Publishing Policy.

Severity Levels

Atlassian's approach to ranking security issues is detailed in Severity Levels for Security Issues.

Our Patch Policy

Atlassian's approach to releasing patches for security issues is detailed in Security Patch Policy.

Published Security Advisories

- Confluence Security Advisory 2011-05-31
- Confluence Security Advisory 2011-03-24
- Confluence Security Advisory 2011-01-18
- Confluence Security Advisory 2010-11-15
- Confluence Security Advisory 2010-10-12
- Confluence Security Advisory 2010-09-21
- Confluence Security Advisory 2010-08-17
- Confluence Security Advisory 2010-07-06
- Confluence Security Advisory 2010-06-02
- Confluence Security Advisory 2010-05-04
- Confluence Security Advisory 2009-12-08
- Confluence Security Advisory 2009-10-06
- Confluence Security Advisory 2009-08-20
- Confluence Security Advisory 2009-06-16
- Confluence Security Advisory 2009-06-01
- Confluence Security Advisory 2009-04-15
- Confluence Security Advisory 2009-02-18
- Confluence Security Advisory 2009-01-07
- Confluence Security Advisory 2008-12-03
- Confluence Security Advisory 2008-10-14
- Confluence Security Advisory 2008-09-08
- Confluence Security Advisory 2008-07-03
- Confluence Security Advisory 2008-05-21
- Confluence Security Advisory 2008-03-19
- Confluence Security Advisory 2008-03-06
- Confluence Security Advisory 2008-01-24
- Confluence Security Advisory 2007-12-14
- Confluence Security Advisory 2007-11-27
- Confluence Security Advisory 2007-11-19
- Confluence Security Advisory 2007-08-08
- Confluence Security Advisory 2007-07-26
- Confluence Security Advisory 2006-06-14
- Confluence Security Advisory 2006-01-23
- Confluence Security Advisory 2006-01-20
- Confluence Security Advisory 2005-12-05
- Confluence Security Advisory 2005-02-09
- Confluence Community Security Advisory 2006-01-19

Other Security Resources

No content found for label(s) security-resources.

Confluence Community Security Advisory 2006-01-19

⛔ This security advisory is not endorsed by Atlassian - this is a public service advisory from a member of the confluence community. **Please** remember to backup any modified files, and use these instructions at your own risk. While this information is based on Confluence v2.1.2, it may have uses with older affected versions of Confluence.

The official security advisory is located at Confluence Security Advisory 2006-01-20

Problem

There is a possibility of XSS exploitation of the Full Name user profile field when displayed.

Solution

The problem was unescaped outputting of the fullname - wrapping the output in $generalUtil.htmlEncode() resolve it. The vast majority of the problem can be resolved by changing `/confluence/template/includes/macros.vm` in the distribution on the following lines:

- 180
- 186
- 200
- 340
- 893

I have attached the modified macros.vm file here which you can copy into your distribution.

Scope

There are other places which are still affected which Atlassian have been made aware of, a complete resolution should be provided by Atlassian in their own offical advisory.

I hope this helps some of you!

Confluence Security Advisory 2005-02-09

A flaw has been found in Confluence by which attackers can bypass Confluence security and change content on the site. Atlassian STRONGLY recommends that all Confluence customers apply the fix described below immediately, or upgrade to Confluence 1.3.3

Vulnerability

By crafting custom URLs, any person with the ability to browse Confluence can modify content on the site, bypassing security settings. This vulnerability does not allow users to view content they would not normally be able to view, or escalate their privileges in other ways.

This flaw affects all versions of Confluence prior to 1.3.3, including the 1.4-DR development releases.

Fix

This vulnerability is fixed in Confluence 1.3.3 and later. Customers who do not wish to migrate to 1.3.3 can fix this bug using the procedure below:

1. Edit the file confluence/WEB-INF/classes/xwork.xml
2. Find the following section near the top of the file (around line 34):

```
<interceptor-stack name="defaultStack">
    <interceptor-ref name="profiling">
        <param name="location">Before defaultStack</param>
    </interceptor-ref>
    <interceptor-ref name="transaction"/>
    <interceptor-ref name="authentication"/>
    <interceptor-ref name="requestParameterHack"/>
    <interceptor-ref name="eventnotifier"/>
    <interceptor-ref name="autowire"/>
    <interceptor-ref name="params"/>
    <interceptor-ref name="servlet"/>
    <interceptor-ref name="pageAware"/>
    <interceptor-ref name="permissions"/>
    <interceptor-ref name="profiling">
        <param name="location">After defaultStack</param>
    </interceptor-ref>
</interceptor-stack>
```

3. Locate the "autowire" and "params" entries:

```
<interceptor-ref name="eventnotifier"/>
-->           <interceptor-ref name="autowire"/>      <--
-->           <interceptor-ref name="params"/>        <--
              <interceptor-ref name="servlet"/>
```

4. Swap the two lines around. The whole stack should now look like this:

```
<interceptor-stack name="defaultStack">
    <interceptor-ref name="profiling">
        <param name="location">Before defaultStack</param>
    </interceptor-ref>
    <interceptor-ref name="transaction"/>
    <interceptor-ref name="authentication"/>
    <interceptor-ref name="requestParameterHack"/>
    <interceptor-ref name="eventnotifier"/>
    <interceptor-ref name="params"/>
    <interceptor-ref name="autowire"/>
    <interceptor-ref name="servlet"/>
    <interceptor-ref name="pageAware"/>
    <interceptor-ref name="permissions"/>
    <interceptor-ref name="profiling">
        <param name="location">After defaultStack</param>
    </interceptor-ref>
</interceptor-stack>
```

5. Restart Confluence.

Confluence Security Advisory 2005-12-05

A flaw has been found in Confluence by which attackers to inject malicious HTML code into Confluence. Atlassian STRONGLY recommends that all Confluence customers apply the fix described below immediately, or upgrade to Confluence 2.0.2

Vulnerability

By entering HTML code into the Confluence search input fields, attackers can cause arbitrary scripting code to be executed by the user's browser in the security context of the Confluence instance.

This flaw affects all versions of Confluence between 1.4-DR releases and 2.0.1.

(Atlassian was not informed of the problem before it was published by third-party security researchers. You can read the third-party security advisory here: http://secunia.com/advisories/17833/. The vulnerability was originally reported here.)

Fix

This vulnerability is fixed in Confluence 2.0.2 and later. Customers who do not wish to migrate to 2.0.2 can fix this bug using the procedure below:

1. Edit the confluence/decorators/components/searchresults.vmd
2. Replace the following reference (around line 48):

   ```
   $action.getText("search.result", [$start, $end, $total, $queryString])
   ```

   with

   ```
   $action.getText("search.result", [$start, $end, $total,
   $generalUtil.escapeXml($queryString)]).
   ```

3. Edit the confluence/search/searchsite-results.vm.
4. Replace the following reference (around line 11):

   ```
   Searched for <b>$action.searchQuery.queryString</b>
   ```

   with

   ```
   Searched for
   <b>$generalUtil.escapeXml($action.searchQuery.queryString)</b>
   ```

5. Restart Confluence.

Alternatively, you can download the patched source files from CONF-4825. If you are patching a 2.0.x installation, then use the files with the .2.0 suffix. If you are patching a 1.4.x installation, then use the files with the .1.4 suffix.

Confluence Security Advisory 2006-01-20

A flaw has been found in Confluence by which attackers to inject malicious HTML code into Confluence.

Atlassian STRONGLY recommends that all Confluence customers apply the fix described below immediately, or upgrade to Confluence 2.1.3.

Vulnerability

By entering HTML/JavaScript code into the full name of a user's profile, attackers can cause arbitrary scripting code to be executed by the user's browser in the security context of the Confluence instance.

This flaw affects all versions of Confluence between 1.4-DR releases and 2.1.2.

This issue was initally reported by Ricardo Sueiras and a fix was quickly documented by Dan Hardiker at the Confluence Community Security Advisory 2006-01-19 page. Our thanks to them for bringing this to our attention.

There is an issue in JIRA at CONF-5233.

Fix

This vulnerability is fixed in Confluence 2.1.3 and later. Customers who do not wish to migrate to 2.1.3 can fix this bug using the procedure below:

Steps to fix:

1. Copy macros.vm to your confluence/template/includes folder
2. Restart Confluence

Note: If you are using version 1.4.4, please download and copy this file instead. You will need to rename it back to `macros.vm`.

If you are not using any of the above versions, you will need to replace wrap calls to display full names of users in $generalUtil.htmlEncode(). Alternatively, send us an email. We do however encourage you to use the latest stable point release regardless of the version you are using.

Confluence Security Advisory 2006-01-23

A flaw has been found in Confluence by which the unrestricted content of a space can be revealed in search results.

Vulnerability

By entering in a space key and blank query string into the Search macro, pages from the specified space will be displayed, without filtering on page and space permissions. This can allow unpermitted users to view the excerpts of pages they don't have access to.

This flaw is confirmed to affect all releases from 1.4 to 2.1.2.

More information is available at CONF-5189.

Fix

This vulnerability is fixed in Confluence 2.1.3 and later. We strongly suggest that customers upgrade to this release to fix the vulnerability.

Customers who are using 1.4.x and do not wish to upgrade can download a patched class from CONF-5198.

Confluence Security Advisory 2006-06-14

Vulnerability

By crafting a custom HTTP request, an attacker can delete or modify global permissions settings on a

Confluence site.

This flaw affects all Confluence versions between 1.4 and 2.2.2. 2.2.3 and later are not vulnerable.

Fix

This issue has been fixed in Confluence 2.2.3. Patches are also available for all versions of Confluence betwen 1.4 and 2.2.2. For more information, please see this issue report.

Atlassian STRONGLY recommends that all customers either upgrade to Confluence 2.2.3, or apply the patch.

Confluence Security Advisory 2007-07-26

In this advisory:

Users with view permission in a space can copy and save a page

Vulnerability

A user who has only view permissions in a space can copy a page and then save it in the space. In this way, users can create a page in a space where they have only view permission.

This flaw affects only Confluence version 2.5.4.

Fix

This issue has been fixed in Confluence 2.5.5. A patch is also available for Confluence 2.5.4. For more information, including instructions on applying the patch, please see this issue report.

If you are using Confluence 2.5.4, Atlassian **strongly** recommends that you upgrade to Confluence 2.5.5 or apply the patch.

Space name and key are not validated nor escaped

Vulnerability

The input for space name and key is not validated properly - any characters are allowed. This makes a Confluence instance vulnerable to an XSS attack.

Fix

This issue has been fixed in Confluence 2.5.5. For more information, please see this issue report.

Atlassian recommends that you upgrade to Confluence 2.5.5.

Confluence Security Advisory 2007-08-08

In this advisory:

Input in the RSS Feed Builder is not validated

Vulnerability

The input for the RSS Feed Builder is not required to be escaped. This can make a Confluence instance vulnerable to an XSS attack.

Fix

This issue has been fixed in Confluence 2.5.6. For more information, please see CONF-8993.

Atlassian recommends that you upgrade to Confluence 2.5.6.

Input when editing Space Permissions is not validated

Vulnerability

The 'Grant permission to' field on the 'Edit Space Permissions' screen is not validated. This can make a Confluence instance vulnerable to an XSS or DoS attack.

Fix

This issue has been fixed in Confluence 2.5.6. For more information, please see CONF-8980 and CONF-8979.

Atlassian recommends that you upgrade to Confluence 2.5.6.

Number of labels that can be added to a page is not restricted

Vulnerability

There is no restriction on the number of labels that can be added to a page at a time. This can make a Confluence instance vulnerable to a DoS attack.

Fix

This issue has been fixed in Confluence 2.5.6. For more information, please see CONF-8978.

Atlassian recommends that you upgrade to Confluence 2.5.6.

Input when editing navigation themes is not validated

Vulnerability

The 'Navigation Page' specified in the 'Left Navigation Theme' configuration is not validated. This can make a Confluence instance vulnerable to a XSS attack.

Fix

This issue has been fixed in Confluence 2.5.6. For more information, please see CONF-8956.

Atlassian recommends that you upgrade to Confluence 2.5.6.

Viewing of space content alphabetically is not validated

Vulnerability

When viewing space content by alphabetic character, the input is not validated as being alphabetic. This can make a Confluence instance vulnerable to an XSS attack.

Fix

This issue has been fixed in Confluence 2.5.6. For more information, please see CONF-8952.

Atlassian recommends that you upgrade to Confluence 2.5.6.

Input when editing Space Name is not validated

Vulnerability

The 'Name' field on the 'Edit Space Details' screen is not validated. This can make a Confluence instance vulnerable to an XSS attack.

Fix

This issue has been fixed in Confluence 2.5.6. For more information, please see CONF-8951.

Atlassian recommends that you upgrade to Confluence 2.5.6.

Input when viewing attachments by file-type is not validated

Vulnerability

The 'Filter By Extension' field on the 'List Space Attachments' screen is not validated. This can make a Confluence instance vulnerable to an XSS attack.

Fix

This issue has been fixed in Confluence 2.5.6. For more information, please see CONF-8950.

Atlassian recommends that you upgrade to Confluence 2.5.6.

Confluence Security Advisory 2007-11-19

In this advisory:

- DWR debug mode enabled

Atlassian recommends that you upgrade to Confluence 2.6.1 to fix the vulnerabilities described below.

DWR debug mode enabled

Vulnerability

Debug mode was enabled by default on Direct Web Remoting (DWR). This made it easy for a potential attacker to find information about available AJAX request handlers in Confluence.

Fix

This issue has been fixed in Confluence 2.6.1. If you do not wish to upgrade at this time, you can fix the problem by editing your `<confluence install>/confluence/WEB-INF/web.xml` file. For more information, please see CONF-9718.

XSS vulnerability in exception error page

Vulnerability

The attributes and parameters were not escaped on the Confluence exception error page. This is a potential vulnerability to a cross-site scripting attack.

Fix

This issue has been fixed in Confluence 2.6.1. For more information, please see CONF-9704 and CONF-9560.

XSS vulnerability in the URL destination for the print icon

Vulnerability

The print icon on the HTTP 404 error page uses the path of the requested URL, which potentially contains malicious JavaScript. The 404 page did not correctly escape it. This is a potential vulnerability to a cross-site scripting attack.

Fix

This issue has been fixed in Confluence 2.6.1. A patch is supplied for customers with **Confluence version 2.6** w ho do not wish to upgrade at this time. For more information, please see CONF-9456.

XSS vulnerability in wiki markup for images

Vulnerability

When using image URLs in wiki markup, quotes were not correctly escaped. This is a potential vulnerability to a cross-site scripting attack.

Fix

This issue has been fixed in Confluence 2.6.1. For customers with **Confluence 2.6** who do not with to upgrade at this time, the new `atlassian-renderer` JAR should resolve this issue. For more information, please see CONF-9209.

Confluence Security Advisory 2007-11-27

In this advisory:

XSS Type 2 Vulnerabilities in Macros and Wiki Markup

Severity

Atlassian rates this vulnerability as **high**, according to the scale published in Confluence Security. The scale allows us to rank a vulnerability as critical, high, moderate or low.

Risk Assessment

We have identified and fixed some security flaws which may affect Confluence instances in a public environment. These flaws are XSS (cross-site scripting) vulnerabilities in some of Confluence's macros and Wiki Markup, which potentially allow a malicious user (hacker) to insert their own HTML tags or script into a Confluence page.

- The hacker might take advantage of this flaw to steal other users' session cookies or other credentials, by sending the credentials back to the hacker's own web server.
- The hacker's text and script might be displayed to other people viewing the Confluence page. This is potentially damaging to your company's reputation.

Atlassian recommends that you upgrade to Confluence 2.6.2 to fix the vulnerabilities described below.

You can read more about XSS attacks at cgisecurity, CERT and other places on the web.

Risk Mitigation

If you judge it necessary, you can disable public access (e.g. anonymous access and public signon) to your wiki until you have applied the necessary patch or upgrade. For even tighter control, you could restrict access to trusted groups only.

Vulnerability

The following macros are affected:

- {color}
- {panel}
- {section}
- {column}
- {code}

The Wiki Markup for inserting images (e.g. `!myImage.png!`) is also vulnerable to XSS exploitation.

Fix

The fix is to escape all user input, so that no user input is interpreted as HTML or CSS. In some cases we also perform stricter validation on the range of values a user can supply in an attribute.

These issues have been fixed in Confluence 2.6.2. For more information, please see CONF-9350.

> Our thanks to **Igor Minar**, who reported this issue to Atlassian. We fully support the reporting of vulnerabilities and we appreciate his working with us towards identifying and solving the problem.

Please let us know what you think of the format of this security advisory and the information we have provided.

Confluence Security Advisory 2007-12-14

In this advisory:

XSS Vulnerability in Configure RSS Feed Action

Severity

Atlassian rates this vulnerability as **high**, according to the scale published in Confluence Security. The scale allows us to rank a vulnerability as critical, high, moderate or low.

Risk Assessment

We have identified and fixed a security flaw which may affect Confluence instances in a public environment. This flaw is an XSS (cross-site scripting) vulnerability in a Confluence action, which potentially allows a malicious user (hacker) to embed their own JavaScript into a Confluence page.

- The hacker might take advantage of this flaw to steal other users' session cookies or other credentials, by sending the credentials back to the hacker's own web server.
- The hacker's text and script might be displayed to other people viewing the Confluence page. This is potentially damaging to your company's reputation.

To fix the vulnerabilities described below, Atlassian recommends that you take one of the following steps:

- Upgrade to Confluence 2.7, or
- Download and install the patch for Confluence 2.5.8 or Confluence 2.6.2 from our JIRA site – see issue CONF-10164.

You can read more about XSS attacks at cgisecurity, CERT and other places on the web.

Risk Mitigation

If you judge it necessary, you can disable public access (e.g. anonymous access and public signon) to your wiki until you have applied the necessary patch or upgrade. For even tighter control, you could restrict access to trusted groups only.

Vulnerability

A hacker can inject their own JavaScript into the following Confluence action:

```
http://www.anyhost.com/confluence/dashboard/configurerssfeed.action
```

The above Confluence action is used to build an RSS feed based on your Confluence pages and news items. The action is invoked when a selects '**Feed Builder**' from your Confluence Dashboard. It can also be invoked by simply entering the URL into the browser address bar.

Fix

These issues have been fixed in **Confluence 2.7**, which you can download from the download centre.

A patch is available for **Confluence 2.5.8** and **Confluence 2.6.2**. For more information, please see CONF-10164.

> Our thanks to **jeff peichel**, who reported this issue to Atlassian. We fully support the reporting of vulnerabilities and we appreciate his working with us towards identifying and solving the problem.

Please let us know what you think of the format of this security advisory and the information we have provided.

Confluence Security Advisory 2008-01-24

In this advisory:

XSS Vulnerability in Dashboard Action

Severity

Atlassian rates this vulnerability as **high**, according to the scale published in Confluence Security. The scale allows us to rank a vulnerability as critical, high, moderate or low.

Risk Assessment

We have identified and fixed a security flaw which may affect Confluence instances in a public environment. This flaw is an XSS (cross-site scripting) vulnerability in a Confluence action, which potentially allows a malicious user (hacker) to embed their own JavaScript into a Confluence page.

- The hacker might take advantage of this flaw to steal other users' session cookies or other credentials, by sending the credentials back to the hacker's own web server.
- The hacker's text and script might be displayed to other people viewing the Confluence page. This is potentially damaging to your company's reputation.

To fix the vulnerabilities described below, Atlassian recommends that you take one of the following steps:

- Upgrade to Confluence 2.7.1, or
- Download and install the patch for Confluence 2.6.2 or Confluence 2.7.0 from our JIRA site – see issue CONF-10289.

You can read more about XSS attacks at cgisecurity, CERT and other places on the web.

Risk Mitigation

If you judge it necessary, you can disable public access (e.g. anonymous access and public signon) to your wiki until you have applied the necessary patch or upgrade. For even tighter control, you could restrict access to trusted groups only.

Vulnerability

A hacker can inject their own JavaScript into the following Confluence action:

```
http://confluence-location/dashboard.action?spacesSelectedTab
```

The above Confluence action is used to determine which spaces are listed on a user's Dashboard. For example, the following URL requests a list of team spaces only:

```
http://confluence-location/dashboard.action?spacesSelectedTab=team
```

The action is invoked when a user selects one of the 'Spaces' tabs on the Dashboard, such as the '**Team**' tab. It can also be invoked by simply entering the URL into the browser address bar.

Fix

These issues have been fixed in **Confluence 2.7.1** (see the release notes), which you can download from the download centre.

A patch is available for **Confluence 2.6.2** and **Confluence 2.7.0**. For more information, please see CONF-10289.

> Our thanks to **Mary Johnson**, who reported this issue to Atlassian. We fully support the reporting of vulnerabilities and we appreciate her working with us towards identifying and solving the problem.

Please let us know what you think of the format of this security advisory and the information we have provided.

Confluence Security Advisory 2008-03-06

In this advisory:

- Users with View-Only Permission can Delete (Purge) Pages
  - Severity
  - Risk Assessment
  - Risk Mitigation
  - Vulnerability
  - Fix

Users with View-Only Permission can Delete (Purge) Pages

Severity

Atlassian rates this vulnerability as **high**, according to the scale published in Confluence Security. The scale allows us to rank a vulnerability as critical, high, moderate or low.

More explanation of the ranking we chose:

- You might rank this vulnerability as **critical**, because in most installations the vulnerability will allow anonymous users to delete information.
- We have chosen a ranking of **high**, because the vulnerability does not allow privilege escalation i.e. it doesn't allow users to gain administration privileges.

Risk Assessment

We have identified and fixed a security flaw which allowed users who have 'View' permission (or higher) on a space to purge (delete) any page in that space.

The following Confluence versions are vulnerable: All versions from **1.3 to 2.7.1** inclusive.

To fix the vulnerabilities described below, Atlassian recommends that you take one of the following steps:

- Upgrade to Confluence 2.7.2, or
- Download and install the patch for Confluence 2.6.x or Confluence 2.7.x from our JIRA site – see issue CONF-10807.

Risk Mitigation

If you judge it necessary, you can disable public access (e.g. anonymous access and public signon) to your wiki until you have applied the necessary patch or upgrade. For even tighter control, you could restrict access to trusted groups only.

If it is not immediately feasible to upgrade to Confluence 2.7.2 or apply a patch, we recommend an alternative strategy:

- As a temporary measure, you can block the URL which allows someone to purge (delete) a page. Please ask your website administrator to block the URL described below.
- The impact is that Space Administrators will not be able to purge individual pages or news items. However, Space Administrators can still use the 'Purge All' link to clear the entire contents of Trash.

Vulnerability

Description:
A user can use the following Confluence action to permanently delete (purge) any Confluence page, provided that the user has 'View' permission (or higher) in the space to which the page belongs:

```
http://confluence-location/pages/purgetrashitem.action?key=XXX&contentId=XXX
```

The above action is invoked when a space administrator clicks the 'Purge' link on the space's 'Trash' page next to a wiki page which has already been deleted.

The action can also be invoked by simply entering the URL into the browser address bar. In this way, it is possible for a user with 'View' permission (or higher) to remove a page via the 'Purge' action, even if the page has not been deleted.

Fix

These issues have been fixed in **Confluence 2.7.2** (see the release notes), which you can download from the download centre.

A patch is available for **Confluence 2.6.x**, **Confluence 2.7.0** and **Confluence 2.7.1**. For more information, please see CONF-10807.

> Our thanks to **Neeraj Jhanji**, who reported this issue to Atlassian. We fully support the reporting of vulnerabilities and we appreciate his working with us towards identifying and solving the problem.

Confluence Security Advisory 2008-03-19

In this advisory:

- XSS Vulnerabilities in Various Confluence Actions
  - Severity
  - Risk Assessment
  - Risk Mitigation
  - Vulnerability
  - Fix

XSS Vulnerabilities in Various Confluence Actions

Severity

Atlassian rates these vulnerabilities as **high**, according to the scale published in Confluence Security. The scale allows us to rank a vulnerability as critical, high, moderate or low.

Risk Assessment

We have identified and fixed a number of security flaws which may affect Confluence instances in a public environment. The flaws are all XSS (cross-site scripting) vulnerabilities in various Confluence actions. Each vulnerability potentially allows a malicious user (hacker) to embed their own JavaScript into a Confluence page.

- The hacker might take advantage of the flaw to steal other users' session cookies or other credentials, by sending the credentials back to the hacker's own web server.
- The hacker's text and script might be displayed to other people viewing the Confluence page. This is potentially damaging to your company's reputation.

To fix the vulnerabilities described below, Atlassian recommends that you take one of the following steps:

- Upgrade to Confluence 2.7.3, or
- Download and install the patches for Confluence **2.6.x** from our JIRA site — refer to the list of issues below.

You can read more about XSS attacks at cgisecurity, CERT and other places on the web.

Risk Mitigation

If you judge it necessary, you can disable public access (e.g. anonymous access and public signon) to your wiki until you have applied the necessary patch or upgrade. For even tighter control, you could restrict access to trusted groups only.

Vulnerability

A hacker can inject their own JavaScript into the Confluence actions listed in the table below. Each of the actions is invoked when a user performs a specific function in Confluence, such as clicking a link or a button. The actions can also be invoked by simply entering the URL into the browser address bar.

For more details please refer to the related JIRA issue, also shown in the table below.

Confluence Actions	Affected Confluence Versions	More Details	Reporter (If Not Atlassian)
Create, edit or copy a page or news item	From **2.2 to 2.7.2** inclusive	CONF-11027	
Add a comment	From **2.2 to 2.7.2** inclusive	CONF-11027	
Create a space	From **2.2 to 2.7.2** inclusive	CONF-11042	Wyatt Crossin
Sign up for an account	From **2.2 to 2.7.2** inclusive	CONF-11005	
Choose a page (page picker)	From **2.2 to 2.7.2** inclusive	CONF-11137	
View a user	From **2.2 to 2.7.2** inclusive	CONF-11002	
Insert an image or link	From **2.2 to 2.7.2** inclusive	CONF-11141	
Choose a user or group (user picker and group picker)	From **2.2 to 2.7.2** inclusive	CONF-11040	Jean Marois
Add a user to favourites	From **2.0 to 2.7.2** inclusive	CONF-11026	
HTTP 500 error page	From **1.3 to 2.7.2** inclusive	CONF-11019	
Add bookmark	All Confluence instances that have the Social Bookmarking plugin. Note that the plugin is bundled with Confluence since version **2.6**, so Confluence 2.6.x and 2.7.x are vulnerable even if you don't use social bookmarking. Patches are supplied for Confluence 2.6.x and 2.7.x.	CONF-11153	

Fix

These issues have been fixed in **Confluence 2.7.3** (see the release notes), which you can download from the download centre.

Patches are available for **Confluence 2.6.x**. For more information, please refer to the specific JIRA issues shown in the table of vulnerabilities above.

> Our thanks to the people who reported some of the vulnerabilities listed above. We fully support the reporting of vulnerabilities and we appreciate their working with us towards identifying and solving the problem.

Confluence Security Advisory 2008-05-21

In this advisory:

- Users can Move Attachments to Any Page Regardless of Permissions
  - Severity
  - Risk Assessment
  - Risk Mitigation
  - Vulnerability
  - Fix
- XSS Vulnerability in Page Information View
  - Severity
  - Risk Assessment
  - Risk Mitigation
  - Vulnerability
  - Fix

Users can Move Attachments to Any Page Regardless of Permissions

Severity

Atlassian rates this vulnerability as **high**, according to the scale published in Confluence Security. The scale allows us to rank a vulnerability as critical, high, moderate or low.

Risk Assessment

We have identified and fixed a security flaw which allows users who have 'Create Page' permission in a space to move an attachment from a page in that space to any other page in the Confluence site, regardless of the user's permissions in the destination space.

The following Confluence versions are vulnerable: All versions from **1.0 to 2.8.0**.

Risk Mitigation

This security flaw grants extra powers only to users who already have 'Create Page' permissions in one of the spaces on the Confluence site. In most installations, this will be a trusted group of users.

If your Confluence instance allows a less trusted group of users to create and edit pages in one space, while restricting access to other spaces, you may judge it necessary to disable public access (e.g. anonymous access and public signon) to your wiki until you have applied the necessary patch or upgrade. For even tighter control, you could restrict access to trusted groups only.

Vulnerability

Any user who has 'Create Page' permission in a Confluence space can move an attachment from a page in that space to any other page in the Confluence site, regardless of the user's permissions in the destination space.

Note: If a user has permission to create a space, they will also have 'Create Page' permission in any space they create, including a personal space. Such users could upload an attachment onto the space they have created and then move the attachment to any page in the Confluence site.

Fix

This issue has been fixed in Confluence 2.8.1 (see the release notes), which you can download from the download centre.

Alternatively, you can download and install the patch for Confluence 2.7.x or Confluence 2.8.0 from our JIRA site – see issue CONF-11452.

> Our thanks to **Stafford Vaughan** from CustomWare, who reported this issue to Atlassian. We fully support the reporting of vulnerabilities and we appreciate it when people work with us towards identifying and solving a problem.

XSS Vulnerability in Page Information View

Severity

Atlassian rates this vulnerability as **high**, according to the scale published in Confluence Security. The scale allows us to rank a vulnerability as critical, high, moderate or low.

Risk Assessment

We have identified and fixed a security flaw which may affect Confluence instances in a public environment. This flaw is an XSS (cross-site scripting) vulnerability in a Confluence action, which potentially allows a malicious user (hacker) to embed their own JavaScript into a Confluence page.

- The hacker might take advantage of this flaw to steal other users' session cookies or other credentials, by sending the credentials back to the hacker's own web server.
- The hacker's text and script might be displayed to other people viewing the Confluence page. This is potentially damaging to your company's reputation.

You can read more about XSS attacks at cgisecurity, CERT and other places on the web.

The following Confluence versions are vulnerable: All versions from **1.3 to 2.8.0** inclusive.

Risk Mitigation

If you judge it necessary, you can hide referrers on page information views by disabling this functionality.

Vulnerability

A hacker can inject their own JavaScript into the referrer URLs which are displayed on the 'Info' view of a wiki page. The rogue JavaScript will be executed when a user opens the 'Info' view.

Fix

This issue has been fixed in Confluence 2.8.1 (see the release notes), which you can download from the download centre.

Alternatively, you can download and install the patch for Confluence 2.7.x or Confluence 2.8.0 from our JIRA site – see issue CONF-11524.

Confluence Security Advisory 2008-07-03

In this advisory:

- Fix

XSS Vulnerability in Various Confluence Actions

Severity

Atlassian rates these vulnerabilities as **high**, according to the scale published in Confluence Security. The scale allows us to rank a vulnerability as critical, high, moderate or low.

Risk Assessment

We have identified and fixed a number of security flaws which may affect Confluence instances in a public environment. The flaws are all XSS (cross-site scripting) vulnerabilities in various Confluence actions. Each vulnerability potentially allows a malicious user (hacker) to embed their own JavaScript into a Confluence page.

- The hacker might take advantage of the flaw to steal other users' session cookies or other credentials, by sending the credentials back to the hacker's own web server.
- The hacker's text and script might be displayed to other people viewing the Confluence page. This is potentially damaging to your company's reputation.

You can read more about XSS attacks at cgisecurity, CERT and other places on the web.

Risk Mitigation

If you judge it necessary, you can disable public access (e.g. anonymous access and public signon) to your wiki until you have applied the necessary patch or upgrade. For even tighter control, you could restrict access to trusted groups only.

Vulnerability

A hacker can inject their own JavaScript into the Confluence actions listed in the table below. Each of the actions is invoked when a user performs a specific function in Confluence, such as clicking a link or a button. The actions can also be invoked by simply entering the URL into the browser address bar. The rogue JavaScript will be executed when a user invokes the URL.

For more details please refer to the related JIRA issue, also shown in the table below.

Confluence Actions	Affected Confluence Versions	More Details	Reporter (If Not Atlassian)
Create, edit or copy a page or news item	2.8.0 and 2.8.1	CONF-11985	James Rinker
Page picker and space picker	2.2.0 to 2.8.1 inclusive	CONF-11137	

Fix

These issues have been fixed in Confluence 2.8.2 (see the release notes), which you can download from the download centre.

Alternatively, you can download and install the patches provided on our JIRA site. For more information, please refer to the specific JIRA issues shown in the table of vulnerabilities above.

Our thanks to **James Rinker** who reported some of the vulnerabilities listed above. We fully support the reporting of vulnerabilities and we appreciate his working with us towards identifying and solving the problem.

Confluence Security Advisory 2008-09-08

In this advisory:

XSS Bug: Usernames Not HTML-Encoded in All Places

Severity

Atlassian rates this vulnerability as **HIGH**, according to the scale published in Confluence Security. The scale allows us to rank a vulnerability as critical, high, moderate or low.

Risk Assessment

We have identified and fixed a security flaw which allowed certain users to circumvent Confluence's security measures, by including HTML markup in their own username. This could allow a malicious user to execute Javascript on another user's authenticated session.

The following Confluence versions are vulnerable: All versions from **1.0 to 2.9**.

Risk Mitigation

If the user specified a username that included HTML markup (which could include Javascript), in some places Confluence would not correctly escape this source before displaying it. This could result in Javascript being executed in another user's authenticated session. To address the issue, you should update your Confluence instance as soon as possible (or follow the patch instructions on the issue).

Vulnerability

This is a classic Cross-Site Scripting issue where usernames could include malicious Javascript.

Fix

This issue has been fixed in Confluence 2.9.1 (see the release notes), which you can download from the download centre.

For more information, see issue CONF-7615 which has instructions on how to patch the affected velocity template.

Inherited Page Restrictions Are Not Applied After 2.9 Upgrade

Severity

Atlassian rates this vulnerability as **HIGH**, according to the scale published in Confluence Security. The scale allows us to rank a vulnerability as critical, high, moderate or low.

Risk Assessment

We have identified and fixed a security flaw that caused any content permission inherited by a page to be lost during the upgrade process to Confluence 2.9.

The following Confluence versions are vulnerable: Version **2.9**; specifically instances of Confluence that were *upgraded to version 2.9* (from an earlier version) only.

Risk Mitigation

This issue can be resolved by following the steps under **Fix**, or upgrading to Confluence 2.9.1. If this cannot be done immediately, it may be prudent to manually apply restrictions to each page that is normally protected by inherited restrictions (that is, all child pages residing under a restricted page). Enacting the fix is trivial and should take around ten minutes for a typical Confluence instance.

Vulnerability

If you had given a parent page restrictions prior to the 2.9 upgrade, then any child pages that should be inheriting these restrictions are no longer restricted. This potentially renders these child pages viewable and editable by Confluence users who should not have these rights. However you should note that any space level restrictions are still respected so these affected pages are only opened as far as the space level security allows for your site. Note for individual pages where you have manually set the permissions, those pages are not at risk — just the pages underneath them using inherited permissions.

Fix

This issue has been fixed in Confluence 2.9.1 (see the release notes), which you can download from the download centre.

Alternatively, you can apply the manual fix, which involves a simple series of actions in the Confluence administration screens.

For more information see issue CONF-12911.

Access Vulnerability in View Wiki Markup Function

Severity

Atlassian rates this vulnerability as **HIGH**, according to the scale published in Confluence Security. The scale allows us to rank a vulnerability as critical, high, moderate or low.

Risk Assessment

We have identified and fixed a security flaw which allows users who don't have the correct '**View Page**' permission in a space to view the Wiki Markup source of the page content.

The following Confluence versions are vulnerable: Version **2.9** only.

Risk Mitigation

If a user knows the URL to view the source of a page they will be able to bypass Confluence's security checks. This will allow the user to view the contents of a page they aren't meant to see.
To prevent unauthorised access, you may want to use your web server to reject all requests to URLs containing this string: `/pages/viewpagesrc.action`. You may judge it necessary to disable public access.

Vulnerability

If a user knows the ID of a page that they do not have **'View Page**' permission for they can use the view source URL to view the Wiki Markup of a page. This will allow them to copy and paste the contents of the page to another location, or simply read the markup and deduce its final content.

Note: the user will need to know the page ID of a page. Confluence will not provide any links to the restricted page through a search or other navigation.

Fix

This issue has been fixed in Confluence 2.9.1 (see the release notes), which you can download from the download centre.

For more information see issue CONF-12845.

Access Vulnerability in Copy Page Function

Severity

Atlassian rates this vulnerability as **HIGH**, according to the scale published in Confluence Security. The scale allows us to rank a vulnerability as critical, high, moderate or low.

Risk Assessment

We have identified and fixed a security flaw which allows users who don't have the correct 'View Page' permission in a space to copy a page and therefore see its content.

The following Confluence versions are vulnerable: All versions from **1.0 to 2.9**.

Risk Mitigation

If a user knows the URL to copy a page they will be able to bypass Confluence's security checks. This will allow the user to view the contents of a page they aren't meant to see.
To prevent unauthorised access, you may want to use your web server to reject all requests to URLs containing this string: `/pages/copypage.action`. You may judge it necessary to disable public access.

Vulnerability

If a user knows the ID of a page they do not have permissions for, they can use the copy page URL to copy the page to a space where they do have permission. This will allow them to create a new page based on the content of a page they aren't meant to see.

Fix

This issue has been fixed in Confluence 2.9.1 (see the release notes), which you can download from the download centre.

Alternatively, you can download and install the patch for Confluence 2.7.3 or 2.8.2 from our JIRA site – see issue CONF-12859.

Instruction on installing the patch can be found here.

Access Vulnerability in Diff Page Function

Severity

Atlassian rates this vulnerability as **HIGH**, according to the scale published in Confluence Security. The scale allows us to rank a vulnerability as critical, high, moderate or low.

Risk Assessment

We have identified and fixed a security flaw which allows users who don't have the correct '**View Page**' permission in a space to create a diff of a page (a comparison of its contents with another page) and therefore see its content.

The following Confluence versions are vulnerable: All versions from **1.0 to 2.9**.

Risk Mitigation

If a user knows the URL to perform a diff of a page they will be able to bypass Confluence's security checks. This will allow the user to view the contents of a page they aren't meant to see.
To prevent unauthorised access, you may want to use your web server to reject all requests to URLs containing this string: `/pages/diffpages.action`. You may judge it necessary to disable public access.

Vulnerability

If a user knows the ID of a page they do not have permissions for, they can use the 'Diff Page' URL to compare the contents of that page with one where they do. This will allow them to deduce the contents of a page they don't have access to.

Fix

This issue has been fixed in Confluence 2.9.1 (see the release notes), which you can download from the download centre.

Alternatively, you can download and install the patch for Confluence 2.7.3 or 2.8.2 from our JIRA site – see issue CONF-12860.

Instruction on installing the patch can be found here.

> Our thanks to **Neeraj Jhanji** from Atlassian Partner ImaHima, who reported the copy and diff page issues to Atlassian. We fully support the reporting of vulnerabilities and we appreciate it when people work with us towards identifying and solving a problem.

Confluence Security Advisory 2008-10-14

In this advisory:

Parameter Injection Vulnerability in Confluence

Severity

Atlassian rates this vulnerability as **critical**, according to the scale published in Confluence Security. The scale allows us to rank a vulnerability as critical, high, moderate or low.

Risk Assessment

We have identified and fixed a flaw which would allow a malicious user (hacker) to inject their own values into a Confluence request by adding parameters to the URL string. This would allow a hacker to bypass Confluence's security checks and perform actions that they are not authorised to perform.

Risk Mitigation

To address the issue, you should upgrade Confluence as soon as possible or follow the patch instructions below. If you judge it necessary, you can block all untrusted IP addresses from accessing Confluence.

Vulnerability

A hacker can design a URL string containing parameters which perform specific actions on the Confluence server, bypassing Confluence's security checks. This is because Confluence does not adequately sanitise user input before applying it as an action on the server.

Exploiting this issue could allow an attacker to access or modify data and compromise the Confluence application.

The following Confluence versions are vulnerable: All versions from **1.3 to 2.9.1**.

Fix

This issue has been fixed in Confluence 2.9.2 (see the release notes), which you can download from the download centre.

If you do not wish to upgrade to Confluence 2.9.2, a patch is available that will work with any affected version of Confluence. You can download and install the patch from on our JIRA site. For more information, please refer to CONF-13092.

XSS Vulnerability in Various Confluence Actions and Plugins

Severity

Atlassian rates these vulnerabilities as **high**, according to the scale published in Confluence Security. The scale allows us to rank a vulnerability as critical, high, moderate or low.

Risk Assessment

We have identified and fixed a number of security flaws which may affect Confluence instances in a public environment. The flaws are all XSS (cross-site scripting) vulnerabilities in various Confluence actions. Each vulnerability potentially allows a malicious user (hacker) to embed their own JavaScript into a Confluence page.

- The hacker might take advantage of the flaw to steal other users' session cookies or other credentials, by sending the credentials back to the hacker's own web server.
- The hacker's text and script might be displayed to other people viewing the Confluence page. This is potentially damaging to your company's reputation.

You can read more about XSS attacks at cgisecurity, CERT and other places on the web.

Risk Mitigation

If you judge it necessary, you can disable public access (e.g. anonymous access and public signon) to your wiki until you have applied the necessary patch or upgrade. For even tighter control, you could restrict access to trusted groups.

Vulnerability

A hacker can inject their own JavaScript into the Confluence actions listed in the table below. Each of the actions is invoked when a user performs a specific function in Confluence, such as clicking a link or a button. The actions can also be invoked by simply entering the URL into the browser address bar. The rogue JavaScript will be executed when a user invokes the URL.

For more details please refer to the related JIRA issue, also shown in the table below.

Confluence Actions	Affected Confluence Versions	More Details	Reporter (If Not Atlassian)

View children via the Pagetree plugin (bundled with Confluence)	2.8.0 to 2.9.1 inclusive	CONF-13043	Thomas Jaehnel
Update bookmark via the Social Bookmarking plugin (bundled with Confluence)	2.6.0 to 2.9.1 inclusive	CONF-13041	Thomas Jaehnel
Build RSS feed	2.0 to 2.9.1 inclusive	CONF-13042	Thomas Jaehnel
Search via Search macro	All versions from 1.0 to 2.9.1 inclusive	CONF-13040	Thomas Jaehnel
Search	All versions from 1.0 to 2.9.1 inclusive	CONF-12944	

Fix

These issues have been fixed in Confluence 2.9.2 (see the release notes), which you can download from the download centre.

If you do not wish to upgrade to Confluence 2.9.2, you can download and install the patches provided on our JIRA site. For more information, please refer to the specific JIRA issues shown in the table of vulnerabilities above.

> Our thanks to **Thomas Jaehnel** of **OPTIMAbit**, who reported most of the XSS vulnerabilities listed above. We fully support the reporting of vulnerabilities and we appreciate it when people work with us to identify and solve the problem.

Privilege Escalation Vulnerability in Confluence Watches

Severity

Atlassian rates this vulnerability as **high**, according to the scale published in Confluence Security. The scale allows us to rank a vulnerability as critical, high, moderate or low.

Risk Assessment

We have identified and fixed a flaw which would allow an unauthorised user to add a Confluence page to the list of pages they are watching, even if the user does not have permission to view that page. Under some circumstances, the unauthorised user may thus have access to information they are not authorised to see.

Risk Mitigation

This flaw does not allow the unauthorised user to update the page, but it may give the user access to information that they do not have permission to see.

Vulnerability

An unauthorised user can manipulate the HTTP request, so that it adds a watch to a page which the user does not have permission to view. The page then appears in the user's list of watched pages, displaying the page title and the corresponding space name. In this way, the user can bypass Confluence's permission checks and gain access to information they are not authorised to see.

The following Confluence versions are vulnerable: All versions from **1.0 to 2.9.1**.

Fix

This issue has been fixed in Confluence 2.9.2 (see the release notes), which you can download from the download centre.

If you do not wish to upgrade to Confluence 2.9.2, you can download and install the patches provided on our JIRA site. For more information, please refer to CONF-13039.

> Our thanks to **Thomas Jaehnel** of **OPTIMAbit**, who reported the vulnerability listed above. We fully support the reporting of vulnerabilities and we appreciate it when people work with us to identify and solve the problem.

Privilege Escalation Vulnerability in Confluence Favourites

Severity

Atlassian rates this vulnerability as **moderate**, according to the scale published in Confluence Security. The scale allows us to rank a vulnerability as critical, high, moderate or low.

Risk Assessment

We have identified and fixed a flaw which would allow an unauthorised user to add a Confluence page to their list of favourites, even if the user does not have permission to view that page. Under some circumstances, the unauthorised user may thus have access to information they are not authorised to see.

Risk Mitigation

This flaw does not allow the unauthorised user to update the page, and it gives the user only very limited access to the information they do not have permission to see.

Vulnerability

An unauthorised user can manipulate the HTTP request, so that it marks as 'favourite' a page which the user does not have permission to view. The page is then added to the number of favourites for the user. The user cannot see the page title or content, but can see that the favourite count has been incremented.

The following Confluence versions are vulnerable: All versions from **1.0 to 2.9.1**.

Fix

This issue has been fixed in Confluence 2.9.2 (see the release notes), which you can download from the download centre.

If you do not wish to upgrade to Confluence 2.9.2, you can download and install the patches provided on our JIRA site. For more information, please refer to CONF-13044.

> Our thanks to **Thomas Jaehnel** of **OPTIMAbit**, who reported the vulnerability listed above. We fully support the reporting of vulnerabilities and we appreciate it when people work with us to identify and solve the problem.

Confluence Security Advisory 2008-12-03

In this advisory:

XSS Vulnerability in Various Confluence Actions

Severity

Atlassian rates these vulnerabilities as **high**, according to the scale published in Confluence Security. The scale allows us to rank a vulnerability as critical, high, moderate or low.

Risk Assessment

We have identified and fixed a number of security flaws which may affect Confluence instances in a public environment. The flaws are all XSS (cross-site scripting) vulnerabilities in various Confluence actions. Each vulnerability potentially allows a malicious user (hacker) to embed their own JavaScript into a Confluence page.

- The hacker might take advantage of the flaw to steal other users' session cookies or other credentials, by sending the credentials back to the hacker's own web server.
- The hacker's text and script might be displayed to other people viewing the Confluence page. This is potentially damaging to your company's reputation.

You can read more about XSS attacks at cgisecurity, CERT and other places on the web.

Risk Mitigation

If you judge it necessary, you can disable public access (e.g. anonymous access and public signon) to your wiki until you have applied the necessary patch or upgrade. For even tighter control, you could restrict access to trusted groups.

Vulnerability

A hacker can inject their own JavaScript into various Confluence URLs — see the table below for the affected functional areas. A URL may be invoked when a user performs a specific function in Confluence, such as clicking a link or a button. The URL can also be invoked by simply entering it into the browser address bar. If rogue JavaScript is injected into such a URL, the JavaScript will be executed when a user invokes the URL.

For more details please refer to the related JIRA issue, also shown in the table below.

Affected Confluence Functionality	Affected Confluence Versions	Fix Availability	More Details	Reporter (If Not Atlassian)
Handling of error messages. (Vulnerability in the DWR code library used by Confluence.)	2.7.3 to 2.9.2 inclusive	2.9.2 and 2.10	CONF-11808	Bjoern Froebe

Attachments macro.	2.8 to 2.9.2 inclusive	2.8.2, 2.9.2 and 2.10**	CONF-13713	
Uploading of attachments.	2.6 to 2.9.2 inclusive	2.8.2, 2.9.2 and 2.10	CONF-13717	
Inserting images as thumbnails.	2.8 to 2.9.2 inclusive	2.8.2, 2.9.2 and 2.10	CONF-13625	
Log events listed in the Confluence 500 error page.	2.9 to 2.9.2 inclusive	2.10 only	CONF-13584	
Wiki Markup link rendering.	2.7 to 2.9.2 inclusive	2.7.x, 2.8.x, 2.9.x, 2.10	CONF-13451	

** The patch for CONF-13717 also addresses the bug in CONF-13736.*
*** To fix this issue, please upgrade your Attachments plugin to the latest version. This plugin is available for Confluence 2.8.2, 2.9.2 and 2.10, via the Confluence Plugin Repository.*

Fix

These issues have been fixed in Confluence 2.10 (see the release notes), which you can download from the download centre.

If you do not wish to upgrade to Confluence 2.10, you can download and install the patches provided on our JIRA site. You will need to upgrade to the latest point release for the major version of Confluence that you are running (e.g. if you are running Confluence 2.8, you will need to upgrade to version 2.8.2) and then apply the patches. For more information, please refer to the specific JIRA issues shown in the table of vulnerabilities above.

Please note that one of the issues can **only be fixed by upgrading to Confluence 2.10**. Please see the table above for details.

> Our thanks to **Bjoern Froebe**, who reported one of the XSS vulnerabilities listed above. We fully support the reporting of vulnerabilities and we appreciate it when people work with us to identify and solve the problem.

Users can View a List of All Attachments by Supplying an Edited URL

Severity

Atlassian rates this vulnerability as **medium**, according to the scale published in Confluence Security. The scale allows us to rank a vulnerability as critical, high, moderate or low.

Risk Assessment

We have identified and fixed a security flaw which allows a user to view the list of all attachments for all pages in a Confluence instance, regardless of space-level or page-level permissions.

While the user cannot open the files, a range of metadata is available for viewing, including file name, the page that the file is attached to, the creator, and the creation and last-modified date of the attachment.

Risk Mitigation

If you judge it necessary, you can disable anonymous access to your wiki until you have applied the necessary patch or upgrade.

Vulnerability

If a user removes the space key from the URL while viewing attachments for a space, Confluence will display the full list of all attachments for all spaces. For more details, please refer to CONF-13874.

Fix

These issues have been fixed in Confluence 2.10 (see the release notes), which you can download from the download centre.

If you do not wish to upgrade to Confluence 2.10, you can download and install the patches provided in the JIRA issue, CONF-13874. You will need to upgrade to the latest point release for the major version of Confluence that you are running (e.g. if you are running Confluence 2.8, you will need to upgrade to version 2.8.2) and then apply the patch.

> Our thanks to **Matthew Goonan**, who reported this vulnerability. We fully support the reporting of vulnerabilities and we appreciate it when people work with us to identify and solve the problem.

Confluence Security Advisory 2009-01-07

In this advisory:

Content Overwrite Vulnerability in the Office Connector Plugin

Severity

Atlassian rates this vulnerability as **high**, according to the scale published in Confluence Security. The scale allows us to rank a vulnerability as critical, high, moderate or low.

Risk Assessment

We have identified a risk that makes it possible for users with read-only access to a Confluence wiki space to modify its contents via the document import feature of the Office Connector plugin. This issue, however, does not expose restricted content on a Confluence wiki space to unauthorised users.

Risk Mitigation

Please see the 'Fix' section below. If you cannot apply the fix immediately, you can consider taking one or more of the following steps:

- Disable the whole Office Connector plugin, as explained here.
- If you judge it necessary, you can disable public access (e.g. anonymous access and public signon) to your wiki until you have applied the necessary patch or upgrade.
- For even tighter control, you could restrict access to trusted groups.

Vulnerability

The Office Connector plugin was first bundled in Confluence version 2.10.0. Hence, this vulnerability affects Confluence **2.10.0** where the Office Connector Plugin is enabled. Additionally, this plugin is compatible with all versions of Confluence **from 2.3.0** onwards. Hence, if you have installed the plugin, this vulnerability will affect your Confluence instance.

Fix

Please download and install the latest version of the Office Connector plugin via the Confluence Plugin Repository (instructions here). If you wish to install this plugin manually, you can download it from here.

Alternatively, install or upgrade to Confluence version 2.10.1. (See the release notes.) The Confluence 2.10.1 installation files can be downloaded from the download centre.

For more information, please refer to CONF-14014.

> Our thanks to **Justin Wong**, who reported this vulnerability. We fully support the reporting of vulnerabilities and we appreciate it when people work with us to identify and solve the problem.

Confluence Security Advisory 2009-02-18

In this advisory:

- HTTP Header Injection Flaw
    - Severity
    - Risk Assessment
    - Risk Mitigation
    - Vulnerability
    - Fix

HTTP Header Injection Flaw

Severity

Atlassian rates this vulnerability as **high**, according to the scale published in Confluence Security. The scale allows us to rank a vulnerability as critical, high, moderate or low.
ℹ An Advanced Warning of this Security Advisory published last week stated the severity of this vulnerability as **critical**. After further assessing the likelihood of attack, however, we have amended this to **high**.

Risk Assessment

We have identified and fixed a security flaw which may affect Confluence instances in a public environment. This flaw is an HTTP header injection vulnerability in the Seraph web framework that is used by Confluence. This potentially allows a malicious user (attacker) to modify the HTTP response to insert malicious code. An attacker could present a modified URL to users (e.g. disguised in an email message). If any user clicks the URL, the malicious code would be executed in the user's session.

- The attacker may take advantage of this flaw to steal other users' session cookies or other credentials, by sending the credentials back to the attacker's own web server.
- The attacker could also gain control over the underlying system, based on the privileges of the user whose session cookie has been stolen.
- The attacker could redirect the user to undesirable web sites. This is potentially damaging to your company's reputation.

Atlassian recommends that you upgrade to Confluence 2.10.2 to fix the vulnerabilities described below.

Risk Mitigation

We strongly recommend either patching or upgrading your Confluence installation to fix this vulnerability. Please see the 'Fix' section below.

Alternatively, you may consider taking the following step, although the time required to fix this vulnerability and the extent of its effectiveness will depend on your application server running Confluence and its configuration:

- Consult the vendor of your application server to see whether your application server is immune to header injection vulnerabilities or has configuration options to prevent such attacks. For example, the Coyote (HTTP) connector in Tomcat version 5.5 and later is immune to header injection attacks, as acknowledged in this reference.
  Technical note: In your application server, header injection vulnerabilities can be mitigated if the setHeader(), addHeader(), and sendRedirect() methods in the HttpServletResponse class have their parameters properly checked for header termination characters.
  ℹ You may wish to forward this technical note to the vendor of your application server to help them assess the vulnerability of your application server to header injection attacks.

Vulnerability

All versions of Confluence prior to 2.10.2 are vulnerable to this security flaw.

Fix

The fix updates the Seraph framework to a version which correctly encodes and validates redirect URLs before sending them back to the user.

To patch your existing installation of Confluence, please refer to CONF-14275. This JIRA issue contains the downloadable patch file and instructions on how to patch your existing Confluence installation.

Alternatively, install or upgrade to Confluence version 2.10.2. (See the release notes.) The Confluence 2.10.2 installation files can be downloaded from the download centre.

For more information, please refer to CONF-14275.

Confluence Security Advisory 2009-04-15

In this advisory:

XSS Vulnerability in Various Confluence Macros

Severity

Atlassian rates this vulnerability as **high**, according to the scale published in Confluence Security. The scale allows us to rank a vulnerability as critical, high, moderate or low.

Risk Assessment

We have identified and fixed two security flaws which may affect Confluence instances in a public environment. These flaws are all cross-site scripting (XSS) vulnerabilities in Confluence's Index and Widget Macros. Each vulnerability potentially allows a malicious user (attacker) to embed their own JavaScript into a Confluence page, which will be executed when the page is rendered.

- The hacker might take advantage of the flaw to steal other users' session cookies or other credentials, by sending the credentials back to the hacker's own web server.
- The hacker's text and script might be displayed to other people viewing the Confluence page. This is potentially damaging to your company's reputation.

You can read more about XSS attacks at cgisecurity, CERT and other places on the web.

Risk Mitigation

We recommend either patching or upgrading your Confluence installation to fix this vulnerability. Please see the 'Fix' section below.

Alternatively if you are not in a position to undertake this immediately and you judge it necessary, you can disable public access (e.g. anonymous access and public sign-on) to your wiki until you have applied the necessary patch or upgrade. For even tighter control, you could restrict access to trusted groups.

You could also temporarily disable the **Widget Connector** plugin and the **Index Macro module of the Confluence Advanced Macros** plugin until you have applied the necessary patch or upgrade. Be aware, however, that this will cause any occurrence of these macros on existing pages or blogs in your Confluence site to render with 'Unknown Macro' indications.

Vulnerability

All versions of Confluence prior to 2.10.3 are vulnerable to this security flaw.

Fix

The fixes include an update to the Index Macro, such that it correctly renders content on the page and an update to the Widget Macro, such that it correctly encodes all parameters passed to it.

To patch your existing installation of Confluence, please refer to CONF-14753 for the Index Macro and CONF-14337 for the Widget Macro. These JIRA issues contain the downloadable patch files and instructions on how to patch your existing Confluence installation.

Alternatively, install or upgrade to Confluence version 2.10.3. (See the release notes.) The Confluence 2.10.3 installation files can be downloaded from the download centre.

For more information, please refer to CONF-14753 and CONF-14337.

> Our thanks to **Igor Minar**, who reported one of the XSS vulnerabilities listed above. We fully support the reporting of vulnerabilities and we appreciate it when people work with us to identify and solve the problem.

HTTP Header Injection Flaw with Attachment Filenames

Severity

Atlassian rates this vulnerability as **high**, according to the scale published in Confluence Security. The scale allows us to rank a vulnerability as critical, high, moderate or low.

Risk Assessment

We have identified and fixed a security flaw with attachment filenames. This vulnerability could lead to an HTTP Header Injection attack through the upload of attachments with modified filenames designed to exploit this flaw. An attacker could insert malicious code into the HTTP response, which would be executed in the user's session.

- The attacker may take advantage of this flaw to steal other users' session cookies or other credentials, by

sending the credentials back to the attacker's own web server.
- The attacker could also gain control over the underlying system, based on the privileges of the user whose session cookie has been stolen.
- The attacker could redirect the user to undesirable web sites. This is potentially damaging to your company's reputation.

Risk Mitigation

We strongly recommend either patching or upgrading your Confluence installation to fix this vulnerability. Please see the 'Fix' section below.

If you judge it necessary, you can disable public access (e.g. anonymous access and public sign-on) to your wiki until you have applied the necessary patch or upgrade. For even tighter control, you could restrict access to trusted groups.

Alternatively, you may consider taking the following step, although the time required to fix this vulnerability and the extent of its effectiveness will depend on your application server running Confluence and its configuration:

- Consult the vendor of your application server to see whether your application server is immune to header injection vulnerabilities or has configuration options to prevent such attacks. For example, the Coyote (HTTP) connector in Tomcat version 5.5 and later is immune to header injection attacks, as acknowledged in this reference.
  Technical note: In your application server, header injection vulnerabilities can be mitigated if the setHeader(), addHeader(), and sendRedirect() methods in the HttpServletResponse class have their parameters properly checked for header termination characters.
  ℹ You may wish to forward this technical note to the vendor of your application server to help them assess the vulnerability of your application server to header injection attacks.

Vulnerability

All versions of Confluence prior to 2.10.3 are vulnerable to this security flaw.

Fix

The fix includes a new header-injection prevention filter in Confluence, which ensures attachment filenames or any other user-provided data is correctly encoded before being included in HTTP headers.

To patch your existing installation of Confluence, please refer to CONF-14704. This JIRA issue contains the downloadable patch files and instructions on how to patch your existing Confluence installation.

Alternatively, install or upgrade to Confluence version 2.10.3. (See the release notes.) The Confluence 2.10.3 installation files can be downloaded from the download centre.

For more information, please refer to CONF-14704.

Confluence Security Advisory 2009-06-01

In this advisory:

XSS Vulnerability in Various Confluence Actions and Macros

Severity

Atlassian rates these vulnerabilities as **high**, according to the scale published in Confluence Security. The scale allows us to rank a vulnerability as critical, high, moderate or low.

Risk Assessment

We have identified and fixed a number of security flaws which may affect Confluence instances in a public environment. These are cross-site scripting (XSS) that affect various Confluence page/blog features and functions.

- The hacker might take advantage of the flaw to steal other users' session cookies or other credentials, by sending the credentials back to the hacker's own web server.
- The hacker's text and script might be displayed to other people viewing the Confluence page. This is potentially damaging to your company's reputation.

You can read more about XSS attacks at cgisecurity, CERT and other places on the web.

Risk Mitigation

We recommend either patching or upgrading your Confluence installation to fix these vulnerabilities. Please see the 'Fix' section below.

Alternatively, if you are not in a position to undertake this immediately and you judge it necessary, you can disable public access (e.g. anonymous access and public sign-on) to your wiki until you have applied the necessary patch or upgrade. For even tighter control, you could restrict access to trusted groups.

Vulnerability

A hacker can inject their own JavaScript into various Confluence URLs — see the table below for the affected functional areas. A URL may be invoked when a user performs a specific function in Confluence, such as clicking a link or a button. The URL can also be invoked by simply entering it into the browser address bar. If rogue JavaScript is injected into such a URL, the JavaScript will be executed when a user invokes the URL.

For more details please refer to the related JIRA issue, also shown in the table below.

Affected Confluence Functionality	Affected Confluence Versions	Fix Availability	More Details
Concurrent page edit message	All versions (1.0 to 2.10.3 inclusive)	2.9.2 and 2.10.3	CONF-15883
Gallery Macro (Confluence Advanced Macros Plugin)	All versions (1.0 to 2.10.3 inclusive)	2.10.3	CONF-15376
View File Macro (Office Connector Plugin)	2.10.0 to 2.10.3 inclusive *	2.10.3	CONF-15402
Instant Messenger Macro	All versions (1.0 to 2.10.3 inclusive)	2.8.2, 2.9.2 and 2.10.3	CONF-15397
Contributors Macro	2.3 to 2.10.3 inclusive	2.9.2 and 2.10.3	CONF-15399
JIRA Issues Macro	All versions (1.0 to 2.10.3 inclusive)	2.10.3	CONF-15754

* This vulnerability may be present in earlier Confluence versions with the Office Connector plugin installed.

Fix

These issues have been fixed in Confluence 3.0 (see the release notes), which you can download from the download centre.

If you do not wish to upgrade to Confluence 3.0, you can download and install the patches provided on our JIRA site. You will need to upgrade to the latest point release for the major version of Confluence that you are running (e.g. if you are running Confluence 2.9, you will need to upgrade to version 2.9.2) and then apply the patches. For more information, please refer to the specific JIRA issues shown in the table of vulnerabilities above.

Confluence Security Advisory 2009-06-16

In this advisory:

Page Content Vulnerabilities

> ℹ If you have already upgraded to Confluence 3.0, then you are not affected by the vulnerabilities described on this page and there is no need to take any further action.

Severity

Atlassian rates these vulnerabilities as **high**, according to the scale published in Confluence Security. The scale allows us to rank a vulnerability as critical, high, moderate or low.

Risk Assessment

We have identified and fixed two security vulnerabilities which may affect Confluence instances in a public environment. Both of these fixes are associated with a tightening of user access restrictions when either viewing specific page content or adding new page content.

The first of these vulnerabilities allows a user without permission to view a given page, to view the contents of any files attached to that page using the view file macro. This assumes that the user has permission to edit or create another page within the Confluence site and knows the name of the file attached to the page they cannot view. For more information, please refer to the JIRA issue CONF-15809.

The second of these vulnerabilities allows users with space administrator permissions to import pages to a Confluence space. The security level of this function has been tightened to permit only users with the system administration permission to access it. For more information, please refer to CONF-15267.

Risk Mitigation

If you have not already upgraded to Confluence 3.0, then we recommend either patching or upgrading your Confluence installation to fix these vulnerabilities. Please see the 'Fix' section below.

Alternatively, if you are not in a position to undertake this immediately and you judge it necessary, you can disable public access (e.g. anonymous access and public sign-on) to your wiki until you have applied the necessary patch or upgrade. For even tighter control, you could restrict access to trusted groups.

Vulnerability

All versions of Confluence up to and including version 2.10.3 with the Office Connector plugin installed are affected by the first view file macro vulnerability.

All versions of Confluence 2.10.x are affected by the second page imports vulnerability.

Fix

These issues have been fixed in Confluence 3.0 (see the release notes), which you can download from the download centre.

If you do not wish to upgrade to Confluence 3.0, you can download and install the patches provided on our JIRA site. You will need to upgrade to the latest point release for the major version of Confluence that you are running (e.g. if you are running Confluence 2.10.0, you will need to upgrade to version 2.10.3) and then apply the patches. For more information, please refer to the specific JIRA issues shown below.

To download the patch to fix the first view file macro vulnerability, please refer to CONF-15809.

To download the patch to fix the second page import vulnerability, please refer to CONF-15267.

Confluence Security Advisory 2009-08-20

In this advisory:

Privilege Escalation Vulnerability in Profile Picture Handling

Severity

Atlassian rates this vulnerability as **high**, according to the scale published in Confluence Security. The scale allows us to rank a vulnerability as critical, high, moderate or low.

Risk Assessment

We have identified a privilege escalation vulnerability, which could provide an attacker with access to administrative areas and functions of Confluence when specifying a profile picture. Under some circumstances, the attacker could gain access to Confluence administrative functions that they are not authorised to use.

Risk Mitigation

To address the issue, you should upgrade to Confluence 3.0.1 as soon as possible or follow the patch instructions in the Fix section below. If you judge it necessary, you can disable public signon to your wiki until you have applied the necessary patch or have performed the upgrade. For even tighter control, you could also restrict access to trusted groups or additionally, disable anonymous access until your system is patched or upgraded.

Vulnerability

The profile picture handling feature in all versions of Confluence up to 3.0.0 are affected by this issue. However, the Form Token Handling mechanism available in Confluence 3.0.0 and later means that the administrative areas in these versions of Confluence cannot be compromised by this vulnerability.

Fix

This issue has been fixed in Confluence 3.0.1 (see the release notes), which you can download from the download centre.

If you do not wish to upgrade to Confluence 3.0.1 and you are running Confluence 2.10.x, you can download and install the patches provided on our JIRA site. We strongly recommend that you upgrade to the latest point release (2.10.3) before applying the patch. For more information, please refer to CONF-16141.

> Our thanks to **Elliot Kendall** of **Emory University**, who reported this vulnerability. We fully support the reporting of vulnerabilities and we appreciate it when people work with us to identify and solve the problem.

XSS Vulnerability in Various Page and Blog Post Features and Functions

Severity

Atlassian rates these vulnerabilities as **high**, according to the scale published in Confluence Security. The scale allows us to rank a vulnerability as critical, high, moderate or low.

Risk Assessment

We have identified and fixed a number of XSS vulnerabilities in various Confluence page/blog features and functions, which may affect Confluence instances in a public environment.

XSS vulnerabilities potentially allow a malicious user (attacker) to embed their own JavaScript into a Confluence page.

- The attacker might take advantage of the vulnerability to steal other users' session cookies or other credentials, by sending the credentials back to the attacker's own web server.
- The attacker's text and script might be displayed to other people viewing the Confluence page. This is potentially damaging to your company's reputation.

You can read more about XSS attacks at cgisecurity, CERT and other places on the web.

Risk Mitigation

We recommend either patching or upgrading your Confluence installation to fix these vulnerabilities. Please see the 'Fix' section below.

Alternatively, if you are not in a position to undertake this immediately and you judge it necessary, you can disable public access (e.g. anonymous access and public sign-on) to your wiki until you have applied the necessary patch or upgrade. For even tighter control, you could restrict access to trusted groups.

Vulnerability

An attacker can inject their own JavaScript into the Confluence actions listed in the table below. Each of the actions is invoked when a user performs a specific function in Confluence, such as clicking a link or a button. The actions can also be invoked by simply entering the URL into the browser address bar. The rogue JavaScript will be executed when a user invokes the URL.

For more details please refer to the related JIRA issue, also shown in the table below.

Confluence action	Affected Confluence Versions	Fix Availability	More Details
Clicking a username link	3.0.0	3.0.0 and 3.0.1	CONF-15970
Moving pages between spaces	2.8 to 2.10.3 inclusive	2.10.x and 3.0.1	CONF-16019* CONF-16135*
Entering content into the WebDAV Configuration page	3.0.0 2.10.x with version 2.0 of the WebDAV plugin	2.10.x, 3.0.0 and 3.0.1	CONF-16136
Entering content into the PDF Export Stylesheet	3.0.0	3.0.0 and 3.0.1	CONF-16209

* Applying the patch for one of these issues fixes the other.

Fix

These issues have been fixed in Confluence 3.0.1 (see the release notes), which you can download from the download centre.

If you do not wish to upgrade to Confluence 3.0.1, you can patch your existing installation by downloading and installing the patched files provided on our JIRA site. For the WebDAV plugin vulnerability, this would involve upgrading the version of the plugin. We strongly recommend that you upgrade to the latest point release of the major version of Confluence that you are running before applying the patches. For example, if you are running Confluence 2.10.1, you should upgrade to version 2.10.3 and then apply the patches. For more information, please refer to the specific JIRA issues shown in the table of vulnerabilities above.

Confluence Security Advisory 2009-10-06

In this advisory:

Session Fixation Vulnerability

Severity

Atlassian rates these vulnerabilities as **high**, according to the scale published in Confluence Security. The scale allows us to rank a vulnerability as critical, high, moderate or low.

Risk Assessment

We have identified and fixed a security vulnerability which may affect Confluence instances in a public environment. This vulnerability could lead to a session fixation attack, in which the malicious user (attacker) can gain access to a victim's Confluence resources whilst the victim is logged in to their Confluence user account.

The attacker does this by fixating (or setting) their session ID onto the victim's computer. While the victim is logged in, all the victim's privileges are associated with the attacker's session ID, effectively granting the attacker access to all of the Confluence data and resources accessible to the victim.

For more information about session fixation attacks, please refer to the following sources:

- Chris Shiflett's Security Corner article
- The Web Application Security Consortium's overview

Risk Mitigation

We recommend either patching or upgrading your Confluence installation to fix these vulnerabilities. Please see the 'Fix' section below.

Alternatively, if you are not in a position to undertake this immediately and you judge it necessary, you can disable public access (e.g. anonymous access and public sign-on) to your wiki until you have applied the necessary patch or upgrade. For even tighter control, you could restrict access to trusted groups.

Vulnerability

All versions of Confluence prior to 3.0.2 are vulnerable to this security issue.

Fix

These issues have been fixed in Confluence 3.0.2 (see the release notes), which you can download from the download centre.

If you do not wish to upgrade to Confluence 3.0.2 and you are currently running Confluence version 2.10.x or 3.0.x, you can patch your existing installation by downloading the appropriate patch file attached to JIRA issue CONF-15108 and installing the patch file using the instructions provided in this JIRA issue.

> Our thanks to **Ben L Broussard** who reported this vulnerability. We fully support the reporting of vulnerabilities and we appreciate it when people work with us to identify and solve the problem.

XSS Vulnerability in Various Confluence Macros

Severity

Atlassian rates these vulnerabilities as **high**, according to the scale published in Confluence Security. The scale allows us to rank a vulnerability as critical, high, moderate or low.

Risk Assessment

We have identified and fixed a number of security vulnerabilities which may affect Confluence instances in a public environment. These flaws are cross-site scripting (XSS) vulnerabilities in Confluence's pagetree, userlister and content by label macros. These XSS vulnerabilities potentially allow an attacker to embed their own JavaScript into a Confluence page.

- The attacker might take advantage of the vulnerability to steal other users' session cookies or other credentials, by sending the credentials back to the attacker's own web server.
- The attacker's text and script might be displayed to other people viewing the Confluence page. This is potentially damaging to your company's reputation.

You can read more about XSS attacks at cgisecurity, CERT and other places on the web.

Risk Mitigation

We recommend either patching or upgrading your Confluence installation to fix these vulnerabilities. Please see the 'Fix' section below.

Alternatively, if you are not in a position to undertake this immediately and you judge it necessary, you can disable public access (e.g. anonymous access and public sign-on) to your wiki until you have applied the necessary patch or upgrade. For even tighter control, you could restrict access to trusted groups.

Vulnerability

An attacker can inject their own JavaScript into the Confluence actions listed in the table below. Each of the actions is invoked when a user performs a specific function in Confluence, such as clicking a link or a button. The actions can also be invoked by simply entering the URL into the browser address bar. The rogue JavaScript will be executed when a user invokes the URL.

For more details please refer to the related JIRA issue, also shown in the table below.

Confluence action	Affected Confluence Versions	Fix Availability	More Details
Pagetree Macro	2.8.0 – 3.0.1	2.10.0 – 3.0.2 inclusive	CONF-16651
Userlister Macro	2.6.0 – 3.0.1	2.10.0 – 3.0.2 inclusive	CONF-16644
Content by Label Macro	2.10.0 – 3.0.1	2.10.0 – 3.0.2 inclusive	CONF-15440

Fix

These issues have been fixed in Confluence 3.0.2 (see the release notes), which you can download from the download centre.

If you do not wish to upgrade to Confluence 3.0.2, you can patch your existing installation by upgrading the plugins for these macros via the Confluence Plugin Repository to the version indicated in the JIRA issues listed in the vulnerability section (above).

Confluence Security Advisory 2009-12-08

In this advisory:

XSS Vulnerability in Various Confluence Actions and Macros

Severity

Atlassian rates these vulnerabilities as **high**, according to the scale published in Severity Levels for Security Issues. The scale allows us to rank a vulnerability as critical, high, moderate or low.

Risk Assessment

We have identified and fixed a number of security vulnerabilities which may affect Confluence instances in a public environment. These flaws are cross-site scripting (XSS) vulnerabilities that could occur when creating a page or blog post in a personal space, using the `indexbrowser.jsp` form and when using the gallery macro.

- The attacker might take advantage of the vulnerability to steal other users' session cookies or other credentials, by sending the credentials back to the attacker's own web server.
- The attacker's text and script might be displayed to other people viewing the Confluence page. This is potentially damaging to your company's reputation.

You can read more about XSS attacks at cgisecurity, CERT and other places on the web.

Risk Mitigation

We recommend either patching or upgrading your Confluence installation to fix these vulnerabilities. Please see the 'Fix' section below.

Alternatively, if you are not in a position to undertake this immediately and you judge it necessary, you can disable public access (e.g. anonymous access and public sign-on) to your wiki until you have applied the necessary patch or upgrade. For even tighter control, you could restrict access to trusted groups.

Vulnerability

An attacker can inject their own JavaScript into the Confluence actions listed in the table below. Each of the actions is invoked when a user performs a specific function in Confluence, such as clicking a link or a button. The actions can also be invoked by simply entering the URL into the browser address bar. The rogue JavaScript will be executed when a user invokes the URL.

For more details please refer to the related JIRA issue, also shown in the table below.

Confluence action	Affected Confluence Versions	Fix Availability	More Details
Page or blog post creation in a personal space	2.10 – 3.0.2	3.0.0 – 3.1 inclusive	CONF-17031
Using the `indexbrowser.jsp` form	All versions prior to and including 3.0.2	3.0.0 – 3.1 inclusive	CONF-17165
Gallery macro	2.9 – 3.0.2	3.0.0 – 3.1 inclusive	CONF-17361
Page tree and page tree search macros	2.9 – 3.0.2	2.8 – 3.1 inclusive	CONF-17967
Status updates tab of the user profile area	3.0.0 – 3.0.2	3.0.0 – 3.1 inclusive	CONF-17933

Fix

These issues have been fixed in Confluence 3.1 (see the release notes), which you can download from the download centre.

If you do not wish to upgrade to Confluence 3.1, you can patch your existing installation by upgrading the plugins for these macros via the Confluence Plugin Repository to the version indicated in the JIRA issues listed in the vulnerability section (above).

Confluence Security Advisory 2010-05-04

This advisory announces a number of security vulnerabilities in earlier versions of Confluence that we have found and fixed in Confluence 3.2.1. In addition to releasing Confluence 3.2.1, we also provide patches for the most important vulnerabilities mentioned. You will be able to apply these patches to older versions of Confluence. There will, however, be a number of security improvements in Confluence 3.2.1 that cannot be patched or backported. We recommend upgrading to Confluence 3.2.1 rather than applying the patches.

In this advisory:

XSS Vulnerabilities

Severity

Atlassian rates these vulnerabilities as **high**, according to the scale published in Severity Levels for Security Issues. The scale allows us to rank a vulnerability as critical, high, moderate or low.

Risk Assessment

We have identified and fixed a number of security vulnerabilities which may affect Confluence instances in a public environment. These flaws are cross-site scripting (XSS) vulnerabilities exposed in the Confluence functions described in the table below.

- An attacker might take advantage of the vulnerability to steal other users' session cookies or other credentials, by sending the credentials back to such an attacker's own web server.
- An attacker's text and script might be displayed to other people viewing the Confluence page. This is potentially damaging to your company's reputation.

You can read more about XSS attacks at cgisecurity, CERT and other places on the web.

Vulnerability

We identified and fixed vulnerabilities in the Confluence features described in the table below.

Confluence Feature	Affected Confluence Versions	Fix Availability	More Details	Severity
Index browser JSP (JavaServer Page)	2.7.0 – 3.2.0	3.2.1 and patch	CONF-19404	High
A JSP that provides an administrator with the location on the file system where the attachments for a given space are stored	2.8.3 – 3.2.0	3.2.1 and patch	CONF-19404	High
A JSP that allows and administrator to reset null emails addresses to dummyvalue@nowhere.org	2.8.3 – 3.2.0	3.2.1 and patch	CONF-19404	High
Colour scheme settings	3.1.2 – 3.2.0	3.2.1 and patch	CONF-19384	High
Error messages	2.7.0 – 3.2.0	3.2.1 and patch	CONF-19390 and CONF-19402	High
Searching Confluence	2.7.4 – 3.2.0	3.2.1 and patch	CONF-19382	High
Attachment upload	3.0.2 – 3.2.0	3.2.1 and patch	CONF-19388	High
Content rendering	3.0.0 – 3.2.0	3.2.1 and patch	CONF-19441	High
Advanced Macros plugin	3.1.0 – 3.2.0	3.2.1 and plugin upgrade	CONF-19403	High

Social Bookmarking plugin	3.0.0 – 3.2.0	3.2.1 and plugin upgrade	CONF-19381	High

Risk Mitigation

We recommend either patching or upgrading your Confluence installation to fix these vulnerabilities. Please see the 'fix' section below.

Alternatively, if you are not in a position to upgrade or patch immediately and you judge it necessary, you can disable public access (such as anonymous access and public sign-on) to your wiki until you have applied the necessary patch or upgrade. For even tighter control, you could restrict access to trusted groups.

Fix

Confluence 3.2.1 fixes all of these issues. See the release notes. You can download Confluence 3.2.1 from the download centre.

If you cannot upgrade to Confluence 3.2.1, you can patch your existing installation using the patches and plugin upgrades listed below. We strongly recommend upgrading to 3.2.1 however, since it adds even more security features than the patches.

Changed behaviour in Confluence

We have removed the `indexbrowser.jsp` and the `viewdocument.jsp` pages that used to provide access to the Confluence index browser. Instead, if you need to see more details of the indexed pages in your Confluence site, you can download and run Luke. Luke is a development and diagnostic tool that accesses existing Lucene indexes and allows you to display and modify their content in several ways. See our document on content index administration.

> Our thanks to **Brett Porter** of **The Apache Software Foundation** and to **David Belcher** of **Research in Motion**, who reported some of the vulnerabilities mentioned above. We fully support the reporting of vulnerabilities and we appreciate it when people work with us to identify and solve the problem.

XSS Vulnerability in Database Check Utility (Not Bundled with Confluence)

Severity

Atlassian rates this vulnerability as **high**, according to the scale published in Confluence Security.

Risk Assessment

We have identified and fixed a cross-site scripting (XSS) vulnerability in the Atlassian database check utility that some customers may have installed. The utility is a JSP file, supplied as an attachment to a documentation page.

Note that this utility is not bundled with Confluence. This vulnerability applies to you only if you have downloaded and installed the JSP.

Vulnerability

An attacker can inject their own JavaScript when invoking the database check utility. The rogue JavaScript will be executed when a user invokes the URL. For more details, please refer to CONF-19406.

Risk Mitigation

If you have previously downloaded and installed the `testdatabase.jsp` utility from the documentation page, you should now remove the `testdatabase.jsp` file from your `<confluence-install>\confluence` directory.

When you need to use the utility again, you can download the updated version from the same documentation page.

Fix

If you have previously downloaded and installed the `testdatabase.jsp` utility from the documentation page, you should now remove the `testdatabase.jsp` file from your `<confluence-install>\confluence` directory.

When you need to use the utility again, you can download the updated version from the same documentation page.

> ⚠ **This fix is not part of Confluence 3.2.1**
>
> Because the JSP file is not shipped with the Confluence installation, there is no patch for this vulnerability and there is no fix for it in Confluence 3.2.1. Please check your installation and remove or update the JSP if present.

Unnecessary Exposure of and Access to Information

Severity

Atlassian rates these vulnerabilities as **high** and **moderate**, according to the scale published in Confluence Security.

Risk Assessment

We have identified a number of areas where Confluence exposes an unnecessary amount of information that may be useful to an attacker if such an attacker gained access to the information.

Vulnerability

We have identified a number of areas where Confluence exposes an unnecessary amount of information, including sensitive information such as usernames and passwords. If an attacker gains access to such information, it may allow such an attacker to gain access to administrative areas and functions of Confluence that they are not authorised to use. Details of each vulnerability are in the table below.

For more details please refer to the related JIRA issues, also shown in the table below.

Confluence action	Affected Confluence Versions	Fix Availability	More Details	Severity

Support request form	3.1.0 – 3.2.0	3.2.1 only	The Confluence support request form automatically generates a zip file containing system information and log files, and submits the file to a given email address along with the support request. The zip file includes configuration files containing usernames, passwords and license details. See CONF-19391	High
Support request form	2.7.0 – 3.2.0	3.2.1 only	The Confluence support request form offers a 'CC' email address, allowing the support request and all attached information to be sent to any email address. In addition, it is also possible to set the default email address to any email address, via the Confluence Administration Console. See CONF-19392	High
XML site backup	2.7.0 – 3.2.0	3.2.1 only	It is possible to download an XML backup of the Confluence site from the Confluence Administration Console. See CONF-19393	High

Daily site backup	2.7.0 – 3.2.0	3.2.1 only	The path to the daily site backup is configurable via the Confluence Administration Console. It is possible to set the daily backup path and (partial) name through the web UI. This allows an attacker to put the backup in a location that is served by the application server. See CONF-19397	Moderate
SOAP and XML-RPC APIs	2.7.0 – 3.2.0	3.2.1 only	The SOAP and XML-RPC APIs give too much information when returning an error about an incorrect login. See CONF-19398	High
Information about Confluence administrators	2.7.0 – 3.2.0	3.2.1 only	The list of Confluence administrators is accessible via a URL and shows the username, full name and email address of all administrators. See CONF-19395	Moderate

Risk Mitigation

We recommend that you upgrade your Confluence installation to fix these vulnerabilities. Please see the 'fix' section below.

Alternatively, if you are not in a position to upgrade or patch immediately, consider applying these measures:

- Control the access to your administrator accounts, as described in our document on best practices for configuring Confluence security.
- Disable access to the SOAP and XML-RPC APIs, if these remote APIs are not required. (Remote API access is disabled by default.) See the page about enabling remote APIs.
- Manually remove the list of Confluence administrators that is accessible via a URL, by editing the relevant Velocity template file as follows:
  1. Edit the `administrators.vm` file, located in `{confluence-install}/confluence` for standalone installations, or at the root of the web app for WAR installations.
  2. Replace the content with a message that you would like to be displayed whenever someone accesses this URL. For example:

```
<html>
  <head>
    <title>$action.getText("title.administrators")</title>
  </head>
  <body>
    The list of Confluence administrators is no longer available.
If you would like to contact an administrator, please email admins
at example dot com.
  </body>
</html>
```

3. Save the file. (There is no need to restart Confluence.)

Fix

Confluence 3.2.1 fixes these issues. See the release notes. You can download Confluence 3.2.1 from the download centre.

Changed Behaviour in Confluence

In order to fix these problems, we have changed Confluence's behaviour as follows:

- We have removed all license, username and password information from the zip file generated by the Confluence support request form.
- It is no longer possible to specify a 'CC' email address on the Confluence support request form.
- By default, it is no longer possible to specify a site support email address in the 'General Configuration' section of the Confluence Administration Console. Administrators can restore this functionality by updating the `confluence.cfg.xml` file found in the Confluence Home directory. Confluence now recognises a new property in this configuration file, called `admin.ui.allow.site.support.email`. If the value of the property is 'true', it will be possible to specify a site support email address via the Confluence Administration Console. If the value of this property is 'false' or the property is not present in the file, the email address is not configurable. By default in Confluence 3.2.1 and later, the value is 'false'.
- By default, the path to the daily site backup is no longer configurable via the Confluence Administration Console. Confluence now recognises a new property called `admin.ui.allow.daily.backup.custom.location` in the `confluence.cfg.xml` file. If the value of this property is 'true', the administrator can change the daily backup path. If the value of this property is 'false' or the property is not present in the file, the backup path is not configurable. By default in Confluence 3.2.1 and later, the value is 'false'.
- By default, it is no longer possible to download an XML backup of the Confluence site from the Confluence Administration Console. Instead, you need access to the Confluence server machine in order to retrieve the XML site backup file. Confluence now recognises a new property called `admin.ui.allow.manual.backup.download` in the `confluence.cfg.xml` file. If the value of this property is 'true', the Administration Console provides an option to download the XML site backup file. If the value of this property is 'false' or the property is not present in the file, the XML download is not available from the Administration Console. By default in Confluence 3.2.1 and later, the value is 'false'.
- On invalid login attempts, the SOAP and XML-RPC APIs no longer give away the specific information that the user does not exist or that the password is invalid.
- The `administrators.action` URL no longer opens a page showing the list of Confluence administrators. Instead, the URL will now present a form which you can use to email all the administrators of the site. This is preferable since it does not give the user any information about who these administrators are. See our documentation on configuring the administrator contact page.

General Tightening of the Confluence Security Model

Severity

Atlassian rates these vulnerabilities as **high** and **moderate**, according to the scale published in Confluence Security.

Risk Assessment

We have improved the security of the following areas in Confluence:

- Prevention of brute force attacks by imposing a maximum number of repeated login attempts.
- Handling of decorator layouts.

Vulnerability

We have identified and fixed a problem where Confluence allows an unlimited number of repeated login attempts, potentially opening Confluence to a brute force attack. We have also improved the security around the handling of decorator layouts. Details of each improvement are in the table below.

For more details please refer to the related JIRA issues, also shown in the table below.

Confluence action	Affected Confluence Versions	Fix Availability	More Details	Severity
Site and space decorator layouts	All versions up to and including 3.2.0	3.2.1 and patch	The BootstrapManager exposed in site and space layout templates should be read only. See CONF-19401	High
Login	All versions up to and including 3.2.0	3.2.1 only	Confluence does not set a maximum to the number of repeated login attempts. This makes Confluence vulnerable to a brute force attack. See CONF-19396	Moderate

Risk Mitigation

We recommend that you upgrade your Confluence installation to fix these vulnerabilities. Please see the 'fix' section below.

Alternatively, if you are not in a position to upgrade immediately, you can patch your existing installation using the patches listed below. The patch will fix the problem with the decorator layouts.

You can prevent brute force attacks by following our guidelines on using Fail2Ban to limit login attempts.

Fix

Confluence 3.2.1 fixes these issues. See the release notes. You can download Confluence 3.2.1 from the download centre.

Alternatively, if you are not in a position to upgrade immediately, you can patch your existing installation using the patches listed below. The patch will fix the problem with the decorator layouts.

Changed Behaviour in Confluence

In order to fix these problems, we have changed Confluence's behaviour as follows:

- We have improved the security in the way Confluence handles decorator layouts. The BootstrapManager is now read only.
- After three failed login attempts, Confluence will display a Captcha form asking the user to enter a given word when attempting to log in again. This will prevent brute force attacks via the login screen. In addition, after three failed login attempts via the XML-RPC or SOAP API, an error message will be returned instructing the user to log in via the web interface. Captcha will automatically be activated when they attempt this login.

Available Patches and Plugin Upgrades

If for some reason you cannot upgrade to Confluence 3.2.1, you can apply the following patches and plugin upgrades to fix the most pressing vulnerabilities described in this security advisory.

Step 1 of the Patch Procedure: Install the Patches

Patches are available for Confluence 3.2.0, 3.1.2, 3.0.2, 2.10.4, 2.9.3 and 2.8.3. You need to upgrade to the specified bug-fix release of the relevant major version before applying the patches. For example, if your version is Confluence 3.0.0, first upgrade to 3.0.2 and then apply the relevant patch.

The available patches address the following issues:

- XSS in search (CONF-19382).
- XSS in attachment upload (CONF-19388).
- XSS in the index browser JSP (CONF-19404).
- XSS in the JSP that provides an administrator with the location on the file system where the attachments for a given space are stored (CONF-19404).
- XSS in the JSP that allows an administrator to reset null emails addresses (CONF-19404).
- XSS in colour scheme settings (CONF-19384).
- XSS in error messages (CONF-19390 and CONF-19402).
- XSS in content rendering (CONF-19441).
- Secure handling of site and space decorator layouts (CONF-19401).

Each patch covers all of the above issues, and is applicable to the specific version of Confluence. To install the patch, download the appropriate version and follow the instructions below.

Your Confluence Version	File
3.2.0	confluence-project-3.2.0-stable.zip
3.1.2	confluence-project-3.1-stable.zip
3.0.2	confluence-project-3.0-stable.zip
2.10.4	confluence-project-2.10-stable.zip
2.9.3	confluence-project-2.9-stable.zip
2.8.3	confluence-project-2.8-stable.zip

Applying the patch

If you are using the Standalone distribution of Confluence:

1. Make a backup of the `<confluence_install_dir>/confluence/` directory.
2. Download the `confluence-x-patch.zip` file from the location given in the table above, for your version of Confluence.
3. Expand the zip file into `<confluence_install_dir>/confluence/`, overwriting the existing files in that location.
4. Restart Confluence.

If you are using the WAR distribution of Confluence:

1. Make a backup of the `<confluence_exploded_war>/confluence/ directory`.
2. Download the `confluence-x-patch.zip` file from the location given in the table above, for your version of Confluence.
3. Expand the zip file into `<confluence_exploded_war>/confluence/`, overwriting the existing files in that location.
4. Run '`build.sh clean`' on UNIX, or '`build.bat clean`' on Windows.
5. Run '`build.sh`' on UNIX or '`build.bat`' on Windows.
6. Redeploy the Confluence web app into your application server.

Step 2 of the Patch Procedure: Upgrade your Plugins

Two of the above vulnerabilities exist in plugins and are therefore not included in the patch. To fix these vulnerabilities, you will need to upgrade the affected plugin to get the fixed version. You can upgrade the plugins in the normal manner, via the **Confluence Plugin Repository**. Please refer to the documentation for more details on installing plugins.

1. If you are running **Confluence 3.1.0 or later**, you will need to install the latest version of the Confluence Advanced Macros plugin. Earlier versions of Confluence are not affected and therefore do not need an upgraded plugin.
2. If you are running **Confluence 3.0.0 or later**, you will need to install the latest version of the Social Bookmarking plugin. Earlier versions of Confluence are not affected and therefore do not need an upgraded plugin.

Step 3 of the Patch Procedure: Remove the Database Check Utility if Previously Installed

If you have previously downloaded and installed the `testdatabase.jsp` utility from the documentation page, you should now remove the `testdatabase.jsp` file from your `<confluence-install>\confluence` directory. See above for more details of this utility.

Confluence Security Advisory 2010-06-02

This security advisory announces a vulnerability in the Confluence Mail Page plugin that may expose a Confluence site to XSS (cross-site scripting) attacks, if it is enabled (note, the Confluence Mail Page plugin is disabled by default). If you do not have this plugin enabled, your site will not be affected. However, we recommend that you still read the advisory below.

In this advisory:

XSS Vulnerability in Confluence Mail Page Plugin

Severity

Atlassian rates this vulnerability as **high**, according to the scale published in Severity Levels for Security Issues. The scale allows us to rank a vulnerability as critical, high, moderate or low.

Risk Assessment

We have identified and fixed a security vulnerability which may affect Confluence instances in a public environment. This flaw is a cross-site scripting (XSS) vulnerability that could occur if you have the Confluence Mail Page plugin enabled. The Confluence Mail Page plugin is bundled with Confluence, although it is disabled by default.

- The attacker might take advantage of the vulnerability to steal other users' session cookies or other credentials, by sending the credentials back to the attacker's own web server.
- The attacker's text and script might be displayed to other people viewing the Confluence page. This is potentially damaging to your company's reputation.

You can read more about XSS attacks at cgisecurity, CERT and other places on the web.

Vulnerability

An attacker can execute their own JavaScript when a user enters a custom URL into the browser address bar (e.g. the user clicks a crafted link in an email). The rogue JavaScript will be executed when the user invokes the URL. For more details, please refer to CONF-19802.

Risk Mitigation

We recommend installing the updated Confluence Mail Page plugin into your Confluence installation to fix this vulnerabilities. Please see the 'Fix' section below.

Alternatively, if you are not in a position to undertake this immediately and you judge it necessary, you can disable the Confluence Mail Page plugin (note, the plugin is disabled by default). You may also wish to disable public access (e.g. anonymous access and public sign-on) to your wiki until you have applied the necessary patch or upgrade. For even tighter control, you could restrict access to trusted groups.

Fix

These issues have been fixed in the latest version (v1.10) of the Confluence Mail Page plugin, which you can download from the Atlassian Plugin Exchange. Installation instructions are available on the plugin documentation page.

Please note, version 1.10 of the Confluence Mail Page plugin will only work with Confluence 3.2. You will need to upgrade to Confluence 3.2 before installing the updated plugin.

Confluence Security Advisory 2010-07-06

This advisory announces a number of security vulnerabilities in earlier versions of Confluence that we have found and fixed in Confluence 3.3. In addition to releasing Confluence 3.3, we also provide patches (in the form of plugin upgrades) for the vulnerabilities mentioned. You will be able to apply these plugin upgrades to older versions of Confluence. There will, however, be a number of security improvements in Confluence 3.3 that cannot be patched or backported. We recommend upgrading to Confluence 3.3 rather than applying the plugin upgrades.

In this advisory:

XSS Vulnerabilities

Severity

Atlassian rates the severity level of these vulnerabilities as **high**, according to the scale published in Severity Levels for Security Issues. The scale allows us to rank the severity as critical, high, moderate or low.

Risk Assessment

We have identified and fixed a number of cross-site scripting (XSS) vulnerabilities which may affect Confluence instances in a public environment. These vulnerabilities are exposed in the Confluence functions described in the table below.

- An attacker might take advantage of the vulnerability to steal other users' session cookies or other credentials, by sending the credentials back to such an attacker's own web server.
- XSS vulnerabilities potentially allow an attacker to embed their own JavaScript into a Confluence page. An attacker's text and script might be displayed to other people viewing the page. This is potentially damaging to your company's reputation.

You can read more about XSS attacks at cgisecurity, CERT and other places on the web.

Vulnerability

We have identified and fixed vulnerabilities in the Confluence features described in the table below.

Confluence Feature	Affected Confluence Versions	Issue Tracking
PDF export	3.1.0 – 3.2.1	CONF-20121
Clickr theme	2.7.0 – 3.2.1	CONF-20126
Tasklist macro	2.8.0 – 3.2.1	CONF-20119
Contributors plugin (Contributors macro and Contributors Summary macro)	3.0.0 – 3.2.1	CONF-20122 CONF-20125

Risk Mitigation

We recommend that you upgrade your Confluence installation to fix these vulnerabilities. Please see the 'fix' section below.

Alternatively, if you are not in a position to upgrade immediately and you judge it necessary, you can apply one or both of the following mitigations:

- Disable every one of the affected plugins, as listed below. You can disable plugins via the Confluence Administration Console. See our documentation on installing and configuring plugins.
- Disable public access (such as anonymous access and public sign-on) to your wiki until you have applied the necessary patch or upgrade. For even tighter control, you could restrict access to trusted groups.

In addition, please refer to our guidelines on best practices for configuring Confluence security. In particular, please read our guidelines on using Apache to limit access to the Confluence administration interface.

Fix

Please choose one of the options below that best suits your Confluence version and your ability to upgrade immediately.

Option 1 (Recommended): Upgrade to Confluence 3.3

We recommend that you upgrade to **Confluence 3.3**, which fixes all of the security issues reported in this advisory. See the Confluence 3.3 release notes. You can download Confluence 3.3 from the download centre.

Option 2: Upgrade or Disable the Affected Plugins

If you cannot upgrade your Confluence installation, you can upgrade or disable the affected plugins to fix the vulnerabilities described in this security advisory.

- You can upgrade the plugins in the normal manner, via the **Confluence Plugin Repository** or by manually uploading the JAR. Please refer to the documentation for more details on installing plugins.
- You can disable plugins via the Confluence Administration Console. See our documentation on installing and configuring plugins.

Affected Feature	Confluence Versions that Can Update the Plugin	Upgrade or Disable Plugin
PDF export plugin	3.1 – 3.3	If you cannot upgrade to Confluence 3.3: • If you are running Confluence 3.1.x or 3.2.x, you should install version 1.9 of the PDF Export plugin. • If you are running Confluence 3.0.2 or earlier, you do not need to take any action as these versions are not affected by the security flaw.
Clickr theme	3.2 – 3.3	If you cannot upgrade to Confluence 3.3: • If you are running Confluence 3.2.x, you should install version 2.10 of the Clickr Theme plugin. • If you are running Confluence 3.1.2 or earlier, you should **disa ble** the 'Clickr Theme' plugin.

Tasklist macro	3.1 – 3.3	If you cannot upgrade to Confluence 3.3: - If you are running Confluence 3.1.x or 3.2.x, you should install version 3.2.5.2 of the Dynamic Task List 2 plugin. - If you are running Confluence 2.8.x to 3.0.x, you should **disable** the 'Dynamic Task List 2' plugin. - If you are running Confluence 2.7.x or earlier, you do not need to take any action as these versions are not affected by the security flaw.
Contributors plugin	3.0 – 3.3	If you cannot upgrade to Confluence 3.3: - If you are running Confluence 3.0.x to 3.2.x, you should install version 1.2.6 of the Contributors plugin. - If you are running Confluence 2.10.4 or earlier, you do not need to take any action as these versions are not affected by the security flaw.

Confluence Security Advisory 2010-08-17

This advisory announces a security vulnerability in Confluence 3.3 that we have found and fixed in Confluence 3.3.1. We recommend that you upgrade to Confluence 3.3.1 to fix this vulnerability.

In this advisory:

Secure Administrator Session Vulnerability

Severity

Atlassian rates this vulnerability as **high**, according to the scale published in Severity Levels for Security Issues. The scale allows us to rank a vulnerability as critical, high, moderate or low.

Risk Assessment

We have identified and fixed a vulnerability in the Secure Administrator Sessions feature, introduced in Confluence 3.3, that allows it to be bypassed.

Vulnerability

If an attacker is able to gain access to a session with administrator privileges, they will be able to access all administrator functions without having to re-authenticate.

This vulnerability exists in **Confluence 3.3 only**.

See CONF-20508 for more details.

Risk Mitigation

We recommend upgrading your Confluence installation to fix these vulnerabilities. Please see the 'fix' section below.

Alternatively, if you are not in a position to upgrade immediately and you judge it necessary, you can disable public access (such as anonymous access and public sign-on) to your wiki until you have applied the necessary upgrade. For even tighter control, you could restrict access to trusted groups.

Fix

Confluence 3.3.1 fixes this issue. See the release notes. You can download Confluence 3.3.1 from the download centre.

Confluence Security Advisory 2010-09-21

This advisory announces a number of security vulnerabilities in earlier versions of Confluence that we have found and fixed in Confluence 3.3.3. We recommend that you upgrade to Confluence 3.3.3 to fix these vulnerabilities.

In this advisory:

Path Traversal Vulnerability in Various Confluence Actions

Severity

Atlassian rates this vulnerability as **critical**, according to the scale published in Severity Levels for Security Issues. The scale allows us to rank a vulnerability as critical, high, moderate or low.

Risk Assessment

We have identified and fixed a path traversal vulnerability in various Confluence actions. By exploiting a path traversal vulnerability, attackers may be able to retrieve any file on the server that is running Confluence, based on the permissions of the user under which Confluence is running. Path traversal attacks are also called 'directory traversal' or 'dot-dot-slash' (../) attacks.

The degree to which a Confluence instance is vulnerable depends on a number of factors in the implementation of the instance. See the mitigation strategies below, for details of how you can reduce your vulnerability.

You can read more about path traversal attacks at Open Web Application Security Project (OWASP) and other places on the web.

Vulnerability

The path traversal vulnerability exists in various Confluence actions, in **all versions of Confluence up to and including 3.3.1**.

See CONF-20668 for issue tracking.

Risk Mitigation

We recommend that you upgrade your Confluence installation to fix this vulnerability.

Alternatively, if you are not in a position to upgrade immediately, please consider the following mitigation strategies:

- Make sure that you do not start Confluence from the root directory when starting Confluence automatically. Instead, start it from a reduced-scope directory such as the `{Confluence-installation}/bin` directory.
- Upgrade your Tomcat version to 6.0.26 or later. This is relevant if you are using a WAR distribution of Confluence in your own Tomcat server.
- If you are running Confluence under UNIX, you should run Confluence inside a `chroot` jail. See Best Practices for UNIX chroot() Operations from Steve Friedl.
- In addition, please refer to our guidelines on Tomcat security best practices. (This is a JIRA document but the principles apply to Confluence.) In particular, you should restrict the file access of the username under which Confluence is running.

Fix

Confluence 3.3.3 fixes this issue. See the release notes. You can download Confluence 3.3.3 from the download centre.

If you cannot upgrade to Confluence 3.3.3, you can patch your existing installation using the patches listed below.

Our thanks to **Warren Leung** of **UCLA**, who reported this vulnerability. We fully support the reporting of vulnerabilities and we appreciate it when people work with us to identify and solve the problem.

Configuration of Office Connector Temporary Storage Location

Severity

Atlassian rates this vulnerability as **high**, according to the scale published in Severity Levels for Security Issues.

Risk Assessment

Earlier versions of Confluence allow the administrator to set the temporary storage location for the View File macro, part of the Office Connector. Provided an attacker has gained administrative access to the system in some way, they could then exploit this vulnerability to save malicious files onto the file system.

Vulnerability

This vulnerability exists in the Office Connector configuration, made available to Confluence administrators via the Confluence Administration Console and the related Confluence action.

This vulnerability affects **versions of Confluence from 2.8 up to and including 3.3.1**, where the Office Connector is installed. Please note that the Office Connector is bundled in Confluence 2.10 and later.

See CONF-20669 for issue tracking.

Risk Mitigation

We recommend that you upgrade your Confluence installation to fix this vulnerability.

Alternatively, if you are not in a position to upgrade immediately and you judge it necessary, you can choose one of the following mitigation strategies:

- Disable the Office Connector plugin. You can disable plugins via the Confluence Administration Console. See our documentation on installing and configuring plugins.
- Disable public access (such as anonymous access and public sign-on) to your wiki until you have applied the necessary upgrade. For even tighter control, you could restrict access to trusted groups.

In addition, please refer to our guidelines on best practices for configuring Confluence security.

Fix

Confluence 3.3.3 fixes this issue. Administrators must edit a properties file to configure the path. See the release notes for more information. You can download Confluence 3.3.3 from the download centre.

If you cannot upgrade to Confluence 3.3.3, you can patch your existing installation using the patches listed belo w.

XSS Vulnerability in the Office Connector

Severity

Atlassian rates the severity level of this vulnerability as **high**, according to the scale published in Severity Levels for Security Issues.

Risk Assessment

We have identified and fixed a cross-site scripting (XSS) vulnerability which may affect Confluence instances, including publicly available instances.

- An attacker might take advantage of the vulnerability to steal other users' session cookies or other credentials, by sending the credentials back to such an attacker's own web server.
- XSS vulnerabilities potentially allow an attacker to embed their own JavaScript into a Confluence page. An attacker's text and script might be displayed to other people viewing the page. This is potentially damaging to your company's reputation.

You can read more about XSS attacks at cgisecurity, CERT and other places on the web.

Vulnerability

The XSS vulnerability is exposed in the document import function of the Confluence Office Connector.

This vulnerability exists in **Confluence 3.3.1 only**, where the Office Connector is enabled. Please note that the Office Connector is bundled in Confluence.

See CONF-20670 for issue tracking.

Risk Mitigation

We recommend that you upgrade your Confluence installation to fix this vulnerability.

Alternatively, if you are not in a position to upgrade immediately and you judge it necessary, you can disable the Office Connector plugin. You can disable plugins via the Confluence Administration Console. See our documentation on installing and configuring plugins.

In addition, please refer to our guidelines on best practices for configuring Confluence security. In particular, please read our guidelines on using Apache to limit access to the Confluence administration interface.

Fix

Confluence 3.3.3 fixes this issue. See the release notes. You can download Confluence 3.3.3 from the download centre.

XSRF Vulnerability in Confluence Mail Page Plugin

Severity

Atlassian rates the severity level of this vulnerability as **high**, according to the scale published in Severity Levels for Security Issues.

Risk Assessment

We have identified and fixed a cross-site request forgery (XSRF) vulnerability which may affect Confluence instances, including publicly available instances.

An attacker might take advantage of the vulnerability to trick users into emailing the contents of restricted pages to an arbitrary address without their knowledge. An XSRF attack works by exploiting the trust that a site has for the user. If a user is logged in to Confluence and an attacker tricks their browser into making a request to a Confluence URL, then the task is performed as the logged in user.

You can read more about XSRF attacks at cgisecurity and other places on the web.

Vulnerability

The XSRF vulnerability is exposed in the Confluence Mail Page plugin.

This vulnerability exists in **versions of Confluence from 2.4 up to and including 3.3.1**, where the Mail Page plugin is enabled. Note that the Mail Page plugin is disabled by default. If you do not have this plugin enabled, your site will not be affected.

See CONF-20671 for issue tracking.

Risk Mitigation

We recommend that you upgrade your Confluence installation, or install the updated Confluence Mail Page plugin into your Confluence installation to fix this vulnerability.

Alternatively, if you are not in a position to upgrade immediately and you judge it necessary, you can disable the Confluence Mail Page plugin. (Note that the plugin is disabled by default).

Fix

Confluence 3.3.3 fixes this issue. See the release notes. You can download Confluence 3.3.3 from the download centre.

The latest version (v1.12) of the Confluence Mail Page plugin also fixes this issue. You can download the plugin from the Atlassian Plugin Exchange. Please refer to the documentation for instructions on installing plugins.

Available Patches and Plugin Upgrades

If for some reason you cannot upgrade to Confluence 3.3.3, you can apply the following patches and plugin upgrades to fix the vulnerabilities described in this security advisory.

Step 1 of the Patch Procedure: Install the Patch

A patch is available for Confluence 3.2.1. (That is, the Confluence 3.2.1_01 distribution.) If you have Confluence 3.2.0, you need to upgrade to Confluence 3.2.1 before applying the patch.

The patch addresses the following issue:

- Path traversal vulnerability (CONF-20668).

Applying the patch

If you are using the Confluence 3.2.1 distribution:

1. Shut down Confluence.
2. Make a backup of the `<confluence_install_dir>/confluence/` directory.
3. Download the confluence-3.2.1-to-3.3.2-security-patch.zip file.
4. Expand the zip file into `<confluence_install_dir>/confluence/`, overwriting the existing files.
5. Restart Confluence.

If you are using the WAR distribution of Confluence:

1. Shut down Confluence.
2. Make a backup of the `<confluence_exploded_war>/confluence/ directory`.
3. Download the confluence-3.2.1-to-3.3.2-security-patch.zip file.
4. Expand the zip file into `<confluence_exploded_war>/confluence/`, overwriting the existing files.
5. Run '`build.sh clean`' on UNIX, or '`build.bat clean`' on Windows.
6. Run '`build.sh`' on UNIX or '`build.bat`' on Windows.
7. Redeploy the Confluence web app into your application server.
8. Restart Confluence.

Step 2 of the Patch Procedure: Upgrade your Plugins

Some of the above vulnerabilities exist in plugins and are therefore not included in the patch. To fix these vulnerabilities, you will need to upgrade the affected plugin to get the fixed version. You can upgrade the plugins in the normal manner, via the **Confluence Plugin Repository**. Please refer to the documentation for more details on installing plugins.

1. Install the latest version (v1.12) of the Mail Page plugin.
2. Install version 1.7.1 of the Office Connector plugin.

Confluence Security Advisory 2010-10-12

This advisory announces a number of security vulnerabilities in earlier versions of Confluence that we have found and fixed in Confluence 3.4. In addition to releasing Confluence 3.4, we also provide patches for the vulnerabilities mentioned below. You will be able to apply these patches to existing installations of Confluence 3.3.3. However, we recommend that you upgrade to Confluence 3.4 to fix these vulnerabilities.

In this advisory:

XSS Vulnerabilities

Severity

Atlassian rates the severity level of these vulnerabilities as **high**, according to the scale published in Severity Levels for Security Issues. The scale allows us to rank the severity as critical, high, moderate or low.

Risk Assessment

We have identified and fixed a number of cross-site scripting (XSS) vulnerabilities which may affect Confluence instances, including publicly available instances.

- An attacker might take advantage of an XSS vulnerability to steal other users' session cookies or other credentials, by sending the credentials back to such an attacker's own web server.
- XSS vulnerabilities potentially allow an attacker to embed their own JavaScript into a Confluence page. An attacker's text and script might be displayed to other people viewing the page. This is potentially damaging to your company's reputation.

You can read more about XSS attacks at cgisecurity, CERT and other places on the web.

Vulnerability

The table below describes the parts of Confluence affected by the XSS vulnerabilities.

Confluence Feature	Affected Confluence Versions	Issue Tracking
Space names	2.9 – 3.3.3	CONF-20740

Office Connector	3.0 – 3.3.3	CONF-20963
Tasklist macro	1.3 – 3.3.3	CONF-20964

Risk Mitigation

We recommend that you upgrade your Confluence installation to fix these vulnerabilities.

Alternatively, if you are not in a position to upgrade immediately and you judge it necessary, you can disable public access (such as anonymous access and public signup) to your wiki until you have applied the necessary patch or upgrade. For even tighter control, you could restrict access to trusted groups.

We also recommend that you read our guidelines on best practices for configuring Confluence security and using Apache to limit access to the Confluence administration interface.

Fix

Confluence 3.4 fixes these issues. For a full description of this release, see the release notes. You can download Confluence 3.4 from the download centre.

If you cannot upgrade to Confluence 3.4, you can patch your existing installation using the patches listed below.

Available Patches and Plugin Upgrades

If for some reason you cannot upgrade to Confluence 3.4, you can apply the following patches and plugin upgrades to fix the vulnerabilities described in this security advisory.

Step 1 of the Patch Procedure: Install the Patch

A patch is available for Confluence 3.3.3.

The patch addresses the following issues:

- XSS vulnerability in space names (CONF-20740).
- XSS vulnerability in Office Connector (CONF-20963).

If you are using the Confluence distribution:

1. Shut down Confluence.
2. Make a backup of the `<confluence_install_dir>/confluence/` directory.
3. Download the confluence-3.3.3-to-3.4-security-patch.zip file.
4. Expand the zip file into `<confluence_install_dir>/confluence/`, overwriting the existing files.
5. Restart Confluence.

If you are using the WAR distribution of Confluence:

1. Shut down Confluence.
2. Make a backup of the `<confluence_exploded_war>/confluence/` directory.
3. Download the confluence-3.3.3-to-3.4-security-patch.zip file.
4. Expand the zip file into `<confluence_exploded_war>/confluence/`, overwriting the existing files.
5. Run '`build.sh clean`' on UNIX, or '`build.bat clean`' on Windows.
6. Run '`build.sh`' on UNIX or '`build.bat`' on Windows.
7. Redeploy the Confluence web app into your application server.
8. Restart Confluence.

Step 2 of the Patch Procedure: Upgrade the Affected Plugins

Some of the above vulnerabilities exist in plugins and are therefore not included in the patch. To fix these vulnerabilities, you will need to upgrade the affected plugins. You can upgrade the plugins in the normal manner, via the **Confluence Plugin Repository**. Please refer to the documentation for more details on installing plugins.

- Install the latest version (v3.3.1) of the Dynamic Tasklist 2 plugin.
- Install the latest version (v1.2.2) of the Documentation Theme plugin.

Confluence Security Advisory 2010-11-15

Security Vulnerability in Confluence Remote API

Severity

Atlassian rates the severity level of this vulnerability as **critical**, according to the scale published in Severity Levels for Security Issues. The scale allows us to rank the severity as critical, high, moderate or low.

Risk Assessment

We have identified and fixed a vulnerability in the Remote API which affects Confluence instances, including publicly available instances. The Remote API allows an attacker to escalate user privileges, excluding the level of system administrator privileges.

Vulnerability

The table below describes the Confluence versions and the specific functionality affected by the RPC vulnerability.

Confluence Feature	Affected Confluence Versions	Fixed Version	Issue Tracking
User Access	2.7 – 3.4	3.4.2	CONF-21162

Risk Mitigation

We recommend that you upgrade your Confluence installation to fix this vulnerability.

We strongly advise that you disable the remote APIs until your Confluence instance is patched or upgraded. If the Remote API is vital, we recommend you disable anonymous access to the remote API.

We also recommend that you read our guidelines on best practices for configuring Confluence security.

Fix

Confluence 3.4.2 fixes this issue. For a full description of this release, see the release notes. You can download Confluence 3.4.2 from the download centre.

If you cannot upgrade to Confluence 3.4.2, you can patch your existing installation using the patch listed below.

Available Patch

If for some reason you cannot upgrade to the latest version of Confluence, you can apply the following patch to fix the vulnerability described in this security advisory.

Vulnerability	Patch
Security vulnerability in Confluence Remote API	confluence-3.4.2-security-patch-for-2.7-to-3.4.1.zip

Patch Procedure: Install the Patch

A patch is available for Confluence 2.7 – 3.4.1.

The patch addresses the following issue:

- Security vulnerability in Confluence RPC (CONF-21162).

Applying the patch

If you are using the Confluence 2.7 – 3.4.1 distributions:

1. Shut down Confluence.
2. Make a backup of the `<confluence_install_dir>/confluence/` directory.
3. Download the confluence-3.4.2-security-patch-for-2.7-to-3.4.1.zip file.
4. Expand the zip file into `<confluence_install_dir>/confluence/`, overwriting the existing files.
5. Restart Confluence.
6. Visit <Confluence base url>/admin/patch342applied.jsp and confirm that it reports: "The Patch for Confluence 3.4.2 has been correctly applied."

If you are using the WAR distribution of Confluence:

1. Shut down Confluence.
2. Make a backup of the `<confluence_exploded_war>/confluence/ directory`.
3. Download the confluence-3.4.2-security-patch-for-2.7-to-3.4.1.zip file.
4. Expand the zip file into `<confluence_exploded_war>/confluence/`, overwriting the existing files.
5. Run '`build.sh clean`' on UNIX, or '`build.bat clean`' on Windows.
6. Run '`build.sh`' on UNIX or '`build.bat`' on Windows.
7. Redeploy the Confluence web app into your application server.
8. Restart Confluence.
9. Visit <Confluence base url>/admin/patch342applied.jsp and confirm that it reports: "The Patch for Confluence 3.4.2 has been correctly applied."

Confluence Security Advisory 2011-01-18

This advisory announces a number of security vulnerabilities that we have found and fixed in recent versions of Confluence. We also provide patches that you will be able to apply to existing installations of Confluence to fix these vulnerabilities. However, we recommend that you upgrade your Confluence installation rather than applying the patches. Enterprise Hosted customers should request an upgrade by raising a support request at http://support.atlassian.com. JIRA Studio is not vulnerable to any of the issues described in this advisory.

Atlassian is committed to improving product security. The vulnerabilities listed in this advisory have been discovered by Atlassian, unless noted otherwise. The reporter may also have requested that we do not credit them.

In this advisory:

XSS Vulnerabilities

Severity

Atlassian rates the severity level of these vulnerabilities as **high**, according to the scale published in Severity Levels for Security Issues. The scale allows us to rank the severity as critical, high, moderate or low.

Risk Assessment

We have identified and fixed a number of cross-site scripting (XSS) vulnerabilities which may affect Confluence instances, including publicly available instances (that is, internet-facing servers). XSS vulnerabilities potentially allow an attacker to embed their own JavaScript into a Confluence page. You can read more about XSS attacks at cgisecurity.com, The Web Application Security Consortium and other places on the web.

Vulnerability

The table below describes the Confluence versions and the specific functionality affected by the XSS vulnerabilities.

Confluence Feature	Affected Confluence Versions	Issue Tracking
Code macro	2.7 – 3.4	CONF-21098
Attachments macro	3.3 – 3.4	CONF-21099
Bookmarks macro	3.1 – 3.4.3	CONF-21390
Global Reports macro	2.7 – 3.4.3	CONF-21391
Recently Updated macro	3.0 - 3.4.3	CONF-21392
Pagetree macro	2.7 - 3.4.3	CONF-21393
Create Space Button macro	2.7 - 3.4.3	CONF-21394
Documentation Link macro	2.7 – 3.4.5	CONF-21508

Our thanks to **dave b**, who reported the vulnerability in the Documentation Link macro. We fully support the reporting of vulnerabilities and we appreciate it when people work with us to identify and solve the problem.

Risk Mitigation

We recommend that you upgrade your Confluence installation to fix these vulnerabilities.

Alternatively, if you are not in a position to upgrade immediately and you judge it necessary, you can disable public signup to your wiki until you have applied the necessary patch or upgrade. For even tighter control, you could restrict access to trusted groups.

We also recommend that you read our guidelines on best practices for configuring Confluence security.

Fix

Confluence 3.4.6 fixes these issues. For a full description of this release, see the release notes. You can download the latest version of Confluence from the download centre.

Patches

If for some reason you cannot upgrade to the latest version of Confluence, you can apply patches to fix the vulnerabilities described in this security advisory. The patches are attached to the relevant issues, as listed in the table above.

> ⚠ Please note that we have released a number of advisories about Confluence recently. We recommend that you review them and upgrade to the most recent release of the product or apply external security controls if you cannot. Most of the disclosed vulnerabilities are not critical and often present less risk when used in a corporate environment with no access from the Internet.
>
> We usually provide patches only for vulnerabilities of critical severity, as an interim solution until you can upgrade. You should not expect that you can continue patching your system instead of upgrading. Our patches are often non-cumulative – we do not recommend that you apply multiple patches from different advisories on top of each other, but strongly recommend to upgrade to the most recent version regularly.
>
> **We recommend patching only when you can neither upgrade nor apply external security controls.**

Supported Version	Confluence Feature	File Name	Issue Tracking	Download Security Update
3.4.x	Code Macro	atlassian-renderer-6.2.jar	CONF-21098	Download
3.3.x	Code Macro	atlassian-renderer-6.0.6.jar	CONF-21098	Download

Customers running Confluence 3.4.x:

Please replace the following JAR file with the updated atlassian-renderer-6.2.jar:

```
CONFLUENCE_INSTALL_DIR/confluence/WEB-INF/lib/atlassian-renderer.jar
```

Customers running Confluence 3.3.x:

Please replace the following JAR file with the updated atlassian-renderer-6.0.6.jar:

```
CONFLUENCE_INSTALL_DIR/confluence/WEB-INF/lib/atlassian-renderer.jar
```

Supported Version	Confluence Feature	File Name	Issue Tracking	Download Security Update
3.4.x	Attachments macro	attachments-table.vm-3.4.x.zip	CONF-21099	Download
3.3.x	Attachments macro	attachments-table.vm.zip	CONF-21099	Download

Customers running Confluence 3.4.x:

Please replace the following *vm* file with the updated attachments-table.vm-3.4.x.zip:

```
CONFLUENCE_INSTALL_DIR/confluence/pages/includes/attachments-table.vm
```

Customers running Confluence 3.3.x:

Please replace the following *vm* file with the updated attachments-table.vm:

```
CONFLUENCE_INSTALL_DIR/confluence/pages/includes/attachments-table.vm
```

Supported Version	Confluence Feature	File Name	Issue Tracking	Download Security Update
3.4.x, 3.3.x	Bookmarks macro	socialbookmarking-1.3.4.jar	CONF-21390	Download

Update the *.jar* file with the fix contained in the file archive (*zip*). Follow these steps to do so:

- Browse to `CONFLUENCE_INSTALL_DIR/confluence/WEB-INF/classes/com/atlassian/confluence/setup`
- Open the file **atlassian-bundled-plugins.zip**
- Decompress the contents into another location
- Replace the current **socialbookmarking.jar** with the correct file according to your version.
- Compress all the *jar* files into another zip with the same name as the original file (*atlassian-bundled-plugins.zip*)
- Please note, make sure you place the files directly inside the *zip*, not contained inside another folder.

Supported Version	Confluence Feature	File Name	Issue Tracking	Download Security Update
3.4.x	Global Reports Macro	confluence-dashboard-macros-3.4.4.jar	CONF-21391	Download
3.3.x	Global Reports Macro	confluence-dashboard-macros-1.13.1.jar	CONF-21391	Download

Update the *.jar* file with the fix contained in the file archive (*zip*). Follow these steps to do so:

- Browse to `CONFLUENCE_INSTALL_DIR/confluence/WEB-INF/classes/com/atlassian/confluence/setup`
- Open the file **atlassian-bundled-plugins.zip**
- Decompress the contents into another location
- Replace the current **confluence-dashboard-macros.jar** the correct file according to your version.
- Compress all the *jar* files into another zip with the same name as the original file (*atlassian-bundled-plugins.zip*)
- Please note, make sure you place the files directly inside the *zip*, not contained inside another folder.

Supported Version	Confluence Feature	File Name	Issue Tracking	Download Security Update
3.4.x	Code Macro	confluence-advanced-macros-1.12.3.jar	CONF-21392	Download
3.3.x	Code Macro	confluence-advanced-macros-1.9.2.jar	CONF-21392	Download

Update the *.jar* file with the fix contained in the file archive (*zip*). Follow these steps to do so:

- Browse to `CONFLUENCE_INSTALL_DIR/confluence/WEB-INF/classes/com/atlassian/confluence/setup`
- Open the file **atlassian-bundled-plugins.zip**
- Decompress the contents into another location
- Replace the current **confluence-advanced-macros.jar** with the correct file according to your version.
- Compress all the *jar* files into another zip with the same name as the original file (*atlassian-bundled-plugins.zip*)
- Please note, make sure you place the files directly inside the *zip*, not contained inside another folder.

Supported Version	Confluence Feature	File Name	Issue Tracking	Download Security Update
3.4.x	Pagetree Macro	pagetree-1.20.jar	CONF-21393	Download

Update the *.jar* file with the fix contained in the file archive (*zip*). Follow these steps to do so:

- Browse to `CONFLUENCE_INSTALL_DIR/confluence/WEB-INF/classes/com/atlassian/confluence/setup`
- Open the file **atlassian-bundled-plugins.zip**
- Decompress the contents into another location
- Replace the current **pagetree.jar** with the correct file according to your version.
- Compress all the *jar* files into another zip with the same name as the original file (*atlassian-bundled-plugins.zip*)
- Please note, make sure you place the files directly inside the *zip*, not contained inside another folder.

Supported Version	Confluence Feature	File Name	Issue Tracking	Download Security Update
3.4.x	Create Space Button macro	confluence-dashboard-macros-3.4.4.jar	CONF-21394	Download
3.3.x	Create Space Button macro	confluence-dashboard-macros-1.13.1.jar	CONF-21394	Download

Update the *.jar* file with the fix contained in the file archive (*zip*). Follow these steps to do so:

- Browse to `CONFLUENCE_INSTALL_DIR/confluence/WEB-INF/classes/com/atlassian/confluence/setup`
- Open the file **atlassian-bundled-plugins.zip**
- Decompress the contents into another location

- Replace the current **confluence-dashboard-macros.jar** with the correct file according to your version.
- Compress all the *jar* files into another zip with the same name as the original file (*atlassian-bundled-plugins.zip*)
- Please note, make sure you place the files directly inside the *zip*, not contained inside another folder.

Supported Version	Confluence Feature	File Name	Issue Tracking	Download Security Update
3.4.x	Documentation Link macro	confluence-advanced-macros-1.12.3.jar	CONF-21508	Download
3.3.x	Documentation Link macro	confluence-advanced-macros-1.9.2.jar	CONF-21508	Download

Update the *.jar* file with the fix contained in the file archive (*zip*). Follow these steps to do so:

- Browse to `CONFLUENCE_INSTALL_DIR/confluence/WEB-INF/classes/com/atlassian/confluence/setup`
- Open the file **atlassian-bundled-plugins.zip**
- Decompress the contents into another location
- Replace the current **confluence-advanced-macros.jar** with the correct file according to your version.
- Compress all the *jar* files into another zip with the same name as the original file (*atlassian-bundled-plugins.zip*)
- Please note, make sure you place the files directly inside the *zip*, not contained inside another folder.

Confluence Security Advisory 2011-03-24

This cumulative advisory announces a number of security vulnerabilities that we have found in Confluence and fixed in recent versions of Confluence. We also provide upgraded plugins and patches that you will be able to apply to existing installations of Confluence to fix these vulnerabilities. However, we recommend that you upgrade your complete Confluence installation rather than upgrading only the affected plugins. **Enterprise Hosted** customers should request an upgrade by raising a support request at http://support.atlassian.com. **JIRA Studio** is not vulnerable to any of the issues described in this advisory.

Atlassian is committed to improving product security. The vulnerabilities listed in this advisory have been discovered by Atlassian, unless noted otherwise. The reporter may also have requested that we do not credit them.

In this advisory:

XSS Vulnerabilities

Severity

Atlassian rates the severity level of these vulnerabilities as **high**, according to the scale published in Severity Levels for Security Issues. The scale allows us to rank the severity as critical, high, moderate or low.

These vulnerabilities are **not** critical. This is an independent assessment and you should evaluate its applicability to your own IT environment.

Risk Assessment

We have identified and fixed a number of cross-site scripting (XSS) vulnerabilities which may affect Confluence instances, including publicly available instances (that is, Internet-facing servers). XSS vulnerabilities allow an attacker to embed their own JavaScript into a Confluence page. You can read more about XSS attacks at cgisecurity.com, The Web Application Security Consortium and other places on the web.

Vulnerability

The table below describes the Confluence versions and the specific functionality affected by each of the XSS vulnerabilities.

Confluence Feature	Affected Confluence Versions	Issue Tracking
Include Page macro	2.7 – 3.4.6	CONF-21604
Activity Stream gadget	3.1 – 3.4.6	CONF-21606
Action links of attachments lists	2.7 – 3.4.7	CONF-21766
Table of Contents macro	2.9 – 3.4.8	CONF-21819

> Our thanks to **Dave B**, who reported the vulnerability in the action links of attachments lists. We fully support the reporting of vulnerabilities and we appreciate it when people work with us to identify and solve the problem.

Risk Mitigation

We recommend that you upgrade your Confluence installation to fix these vulnerabilities.

Alternatively, if you are not in a position to upgrade immediately and you judge it necessary, you can disable public signup to your wiki until you have applied the necessary patch or upgrade. For even tighter control, you could restrict access to trusted groups.

We also recommend that you read our guidelines on best practices for configuring Confluence security.

Fix

Confluence 3.4.9 or later fixes all of these issues. Some issues have been fixed in earlier versions as described in the table above. For a full description of this release, see the release notes. You can download the latest version of Confluence from the download centre. The most recent version at the time of this advisory is Confluence 3.5.

Patches

If for some reason you cannot upgrade to the latest version of Confluence, you can upgrade the relevant plugins (below) in your Confluence installation to fix the vulnerabilities described in this security advisory.

For details on upgrading Confluence's plugins using the plugin manager, see:

- Upgrading your Existing Plugins (for Confluence 3.4.x) or
- Installing and Configuring Plugins using the Plugin Repository Client (for Confluence 3.3.x).

Patches are also attached to the relevant issues (listed in the table above) if you need to apply these fixes manually.

> Please note that we have released a number of advisories about Confluence recently. We recommend that you review them and upgrade to the most recent release of the product or apply external security controls if you cannot. Most of the disclosed vulnerabilities are not critical and often present less risk when used in a corporate environment with no access from the Internet.
>
> We usually provide patches only for vulnerabilities of critical severity, as an interim solution until you can upgrade. You should not expect that you can continue patching your system instead of upgrading. Our patches are often non-cumulative – we do not recommend that you apply multiple patches from different advisories on top of each other, but strongly recommend to upgrade to the most recent version regularly.
>
> **We recommend patching only when you can neither upgrade nor apply external security controls.**

Include Page Macro

Supported Confluence Versions	Issue Tracking	File Name	Downloadable Patch
3.4.x	CONF-21604	confluence-advanced-macros-1.12.4.jar	Download
3.3.x	CONF-21604	confluence-advanced-macros-1.9.3.jar	Download

To apply this fix, use the plugin manager to upgrade the **Advanced Macros** plugin to a version greater than or equal to that specified in the file name above.

Activity Stream Gadget

Supported Confluence Versions	Issue Tracking	File Name	Downloadable Patch
3.3.x	CONF-21606	streams-confluence-plugin-3.3-CONF-21606.jar	Download
3.4.x	CONF-21606	streams-confluence-plugin-3.4.6.jar	Download

It's currently not possible to upgrade the Activity Streams Plugin automatically using the 3.4 plugin manager or the 3.3 plugin repository. Instead, you will need to manually install the plugin as follows:

1. Download the JAR file for your version of Confluence (see above).
2. Install the plugin manually using the "Upload Plugin" link on the "Install" tab of the plugin manager.

Action links of attachments lists

Supported Confluence Versions	Issue Tracking	File Name	Downloadable Patch
3.3.x, 3.4.x	CONF-21766	confluence-attachments-plugin-2.20.jar	Download

To apply this fix, use the plugin manager to upgrade the **Confluence Attachments Plugin** plugin to a version greater than or equal to that specified in the file name above.

Table of Contents macro

Supported Confluence Versions	Issue Tracking	File Name	Downloadable Patch
3.3.x, 3.4.x	CONF-21819	toc-plugin-2.4.12.jar	Download

To apply this fix, use the plugin manager to upgrade the **Table of Contents Plugin** plugin to a version greater than or equal to that specified in the file name above.

Confluence Security Advisory 2011-05-31

It has been incorrectly advised previously that CONF-22479 (User Preferences) affects all versions starting 2.7 while in fact it is exploitable only in 3.5 and above. Our sincere apologies, this will not happen again.

You can still apply the patch to 3.4 in order to remove the root cause of this bug and potentially prevent other similar vulnerabilities from appearing

This advisory announces security vulnerabilities that we have found in Confluence and fixed in a recent version of Confluence. We also provide upgraded plugins and patches that you will be able to apply to existing installations of Confluence to fix these vulnerabilities. However, we recommend that you upgrade your complete Confluence installation rather than upgrading only the affected plugins. **Enterprise Hosted** customers should request an upgrade by raising a support request at http://support.atlassian.com. **JIRA Studio** is not vulnerable to the issues described in this advisory.

Atlassian is committed to improving product security. The vulnerabilities listed in this advisory have been discovered by Atlassian, unless noted otherwise. The reporter may also have requested that we do not credit them.

In this advisory:

XSS Vulnerabilities

Severity

Atlassian rates the severity level of both these vulnerabilities as **high**, according to the scale published in Severity Levels for Security Issues. The scale allows us to rank the severity as critical, high, medium or low. These vulnerabilities are **not** critical. This is an independent assessment and you should evaluate its applicability to your own IT environment.

Risk Assessment

We have identified and fixed cross-site scripting (XSS) vulnerabilities that may affect Confluence instances, including publicly available instances (that is, Internet-facing servers). XSS vulnerabilities allow an attacker to embed their own JavaScript into a Confluence page. You can read more about XSS attacks at cgisecurity.com, The Web Application Security Consortium and other places on the web.

Vulnerability

The table below describes the Confluence versions and the specific functionality affected by the XSS vulnerabilities.

Confluence Feature	Affected Confluence Version	Fixed Version	Issue Tracking
Login	3.5 – 3.5.2	3.5.3	CONF-22402
User Preferences	3.5 – 3.5.2	3.5.3	CONF-22479

Our thanks to Marian Ventuneac (http://www.ventuneac.net) who reported the vulnerabilities mentioned above. We fully support the reporting of vulnerabilities and we appreciate it when people work with us to identify and solve the problem.

Risk Mitigation

We recommend that you upgrade your Confluence installation to fix these vulnerabilities.

Alternatively, if you are not in a position to upgrade immediately and you judge it necessary, you can disable public signup to your wiki until you have applied the necessary patch or upgrade. For even tighter control, you could restrict access to trusted groups.

We also recommend that you read our guidelines on best practices for configuring Confluence security.

Fix

These vulnerabilities (CONF-22402 and CONF-22479) are both fixed in Confluence 3.5.3, and later versions. For a full description of the latest version of Confluence, see the release notes. You can download the latest version of Confluence from the download centre.

If you cannot upgrade to the latest version of Confluence, you can temporarily patch your existing installation using the patch listed below. We strongly recommend upgrading and not patching.

Patches

If you are running Confluence 3.5, we highly recommend that you upgrade to Confluence 3.5.3, or later.
If you are running Confluence 3.4, you can apply the following patch to fix the CONF-22479 vulnerability. The CONF-22402 vulnerability does not affect Confluence 3.4.

Vulnerability	Patch	Patch File Name
User Preferences	Attached to issue CONF-22479	CONF-22479_patch.zip

Patch Procedure: Install the Patch

A patch is available for Confluence 3.4 – 3.4.9.

The patch addresses the following issue:

Security vulnerability in Confluence User Preferences (CONF-22479).

Applying the patch

If you are using Confluence 3.4 – 3.4.9:

1. Download the CONF-22479_patch.zip file that is attached to the CONF-22479 issue.
2. Stop Confluence.
3. Make a backup of the <confluence_install_dir> directory.
4. Expand the downloaded zip file into <confluence_install_dir>, overwriting the existing files.
5. Check that the following files were created:
    - confluence/WEB-INF/classes/com/atlassian/confluence/core/ConfluenceActionSupport.properties
    - confluence/WEB-INF/classes/com/atlassian/confluence/languages/DefaultLocaleManager.class
    - confluence/WEB-INF/classes/com/atlassian/confluence/user/actions/EditMySettingsAction.class
6. Restart Confluence.

XSRF Vulnerability

Severity

Atlassian rates the severity level of both this vulnerability as **medium**, according to the scale published in Severity Levels for Security Issues for Security Issues. The scale allows us to rank the severity as critical, high, medium or low.
This vulnerability is **not** critical. This is an independent assessment and you should evaluate its applicability to your own IT environment.

Risk Assessment

We have identified and fixed a cross-site request forgery (XSRF) vulnerability that may affect Confluence instances, including publicly available instances (that is, Internet-facing servers). XSRF vulnerabilities allow an attacker to trick users into unintentionally adding bookmarks to Confluence spaces. You can read more about XSRF attacks at http://www.cgisecurity.com/csrf-faq.html and other places on the web.

Vulnerability

The table below describes the Confluence versions and the specific functionality affected by the XSRF vulnerability.

Confluence Feature	Affected Confluence Version	Fixed Version	Issue Tracking
Social Bookmarking plugin	3.0 – 3.4.9	3.5	CONF-22565

Risk Mitigation

We recommend that you upgrade your Confluence installation to fix these vulnerabilities.

Alternatively, if you are not in a position to upgrade immediately and you judge it necessary, you can disable public signup to your wiki until you have applied the necessary patch or upgrade. For even tighter control, you could restrict access to trusted groups.

We also recommend that you read our guidelines on best practices for configuring Confluence security for configuring Confluence security.

Fix

This vulnerability (CONF-22565) is fixed in Confluence 3.5, and later versions.
For a full description of the latest version of Confluence, see the release notes. You can download the latest version of Confluence from the download centre.

If you cannot upgrade to the latest version of Confluence, you can temporarily patch your existing installation using the patch listed below. We strongly recommend upgrading and not patching.

Patches

If you are running Confluence 3.5, the CONF-22565 vulnerability is already fixed, but we highly recommend that you upgrade to the latest version of Confluence.
If you are running Confluence 3.4, you can apply the following patch to fix the CONF-22565 vulnerability.

For details on upgrading Confluence's plugins using the plugin manager, see:

- Upgrading your Existing Plugins

Vulnerability	Patch	Patch File Name
Social Bookmarking plugin	Attached to issue CONF-22565	socialbookmarking-1.3.9.jar

Patch Procedure: Install the Patch

A patch is available for Confluence 3.4 – 3.4.9.

The patch addresses the following issue:

- Security vulnerability in Confluence Settings Social Bookmarking plugin (CONF-22565).

Applying the patch

If you are using Confluence 3.4 – 3.4.9, use the plugin manager to upgrade the Social Bookmarking plugin to a version equal to or greater than that specified in the file name above.
For details on using the plugin manager, see Upgrading your Existing Plugins.

Configuring Confluence Security

This section gives guidelines on configuring the security of your Confluence site.

Other topics:

- For information about user management, groups and permissions, please refer to the internal security overview.
- For an overview of Confluence application security, see the page on Confluence security.

Setting up a Secure Confluence Site

- Confluence Cookies
- Configuring Secure Administrator Sessions
- Using Fail2Ban to limit login attempts
- Securing Confluence with Apache
  - Using Apache to limit access to the Confluence administration interface
- Enabling or Disabling Public Signup
- Managing External Referrers
  - Excluding external referrers
  - Hiding external referrers
  - Ignoring External Referrers
- Best Practices for Configuring Confluence Security
- Hiding the People Directory
- Configuring Captcha for Spam Prevention
- Hiding External Links From Search Engines
- Configuring Captcha for Failed Logins
- Configuring XSRF Protection
- User Email Visibility
- Anonymous Access to Remote API
- Running Confluence Over SSL or HTTPS
- Connecting to LDAP or JIRA or Other Services via SSL
- Configuring RSS Feeds

Confluence Cookies

Confluence uses Seraph, an open source framework, for HTTP cookie authentication.

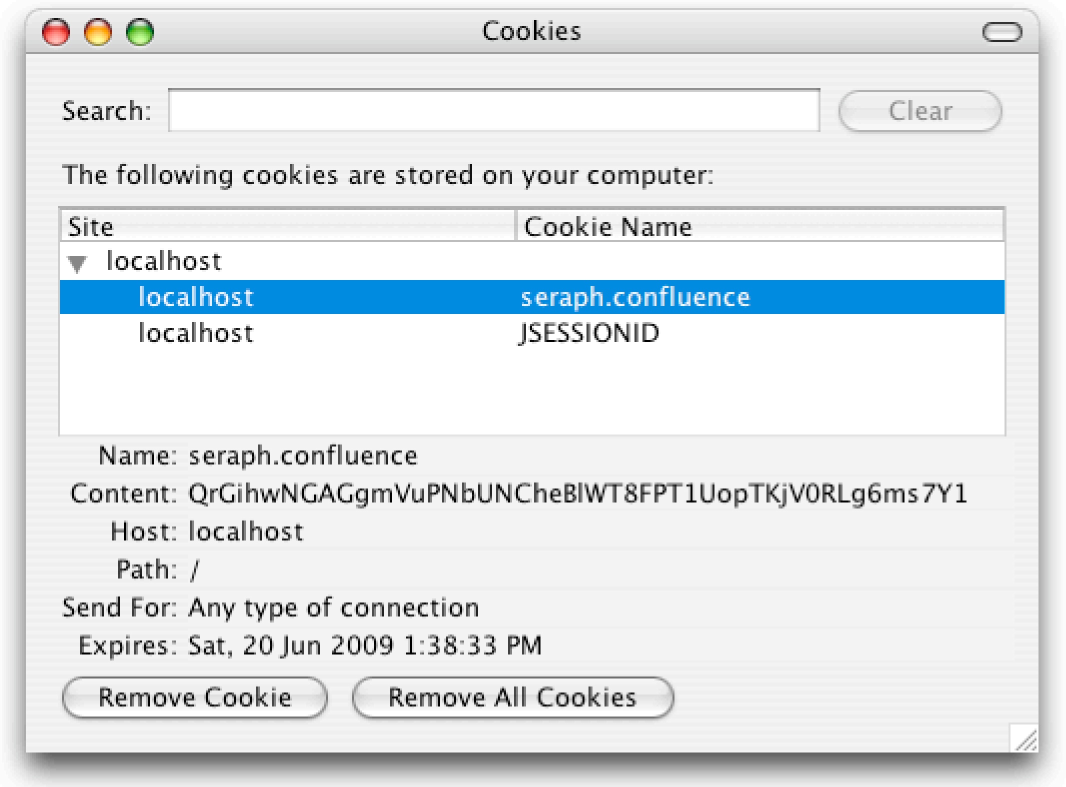
> ⚠ *The information on this page does not apply to Confluence OnDemand.*

Cookies

Confluence uses two cookies:

- The JSESSIONID cookie is created by the application server and used for session tracking purposes.
- The 'remember me' cookie, `seraph.confluence`, is generated by Confluence when the user selects the 'Remember me' checkbox on the login page.

ⓘ You can read about cookies on the Wikipedia page.



Site	Cookie Name
▼ localhost	
localhost	seraph.confluence
localhost	JSESSIONID

Name: seraph.confluence
Content: QrGihwNGAGgmVuPNbUNCheBlWT8FPT1UopTKjV0RLg6ms7Y1
Host: localhost
Path: /
Send For: Any type of connection
Expires: Sat, 20 Jun 2009 1:38:33 PM

The 'Remember Me' Cookie

The 'remember me' cookie is a long-lived HTTP cookie. This cookie can be used to authenticate an unauthenticated session. Confluence generates this cookie when the user selects the 'Remember me' checkbox on the login page.

Cookie Key and Value

By default, the cookie key is `seraph.confluence`. This key is defined in the `CONFLUENCE-INSTALLATION/confluence/WEB-INF/classes/seraph-config.xml` file, in the `login.cookie.key` parameter.

The cookie contains a unique identifier plus a securely-generated random string.

Use of Cookie for Authentication

When a user requests a web page, if the request is not already authenticated via session-based authentication or otherwise, Confluence will match the 'remember me' cookie (if present) against the token stored for the user in the Confluence database (if present).

If the random string matches the value stored in the database and the cookie has not expired, the user is authenticated.

Life of 'Remember Me' Cookies

You can configure the maximum age of the cookie. To do that you will need to modify the `CONFLUENCE-INSTALLATION/confluence/WEB-INF/classes/seraph-config.xml` file and insert the following lines below the other `init-param` elements:

```
<init-param>

<param-name>autologin.cookie.age</param-name>

<param-value>2592000</param-value><!-- 30 days in seconds -->
        </init-param>
```

Automatic Cleanup of 'Remember Me' Tokens

Every cookie issued by Confluence has a corresponding record in the database. A scheduled job runs on 20th of every month to clean up expired tokens. The name of the trigger is `clearExpiredRememberMeTokensTrigger`.

Note: The only purpose of this job is to prevent the database table from growing too big. For authentication purposes, Confluence will ignore expired tokens even if they still exist in the database.

Is it Possible to Disable the 'Remember Me' Feature?

Confluence does not offer an option for disabling the 'Remember Me' feature. See the workaround.

Notes

- The *autocomplete* that happens when a user logs in is a browser feature, not a Confluence feature. Confluence cannot enable or disable the autocompletion.

RELATED TOPICS

Administrators Guide Home Confluence Documentation Home

Configuring Secure Administrator Sessions

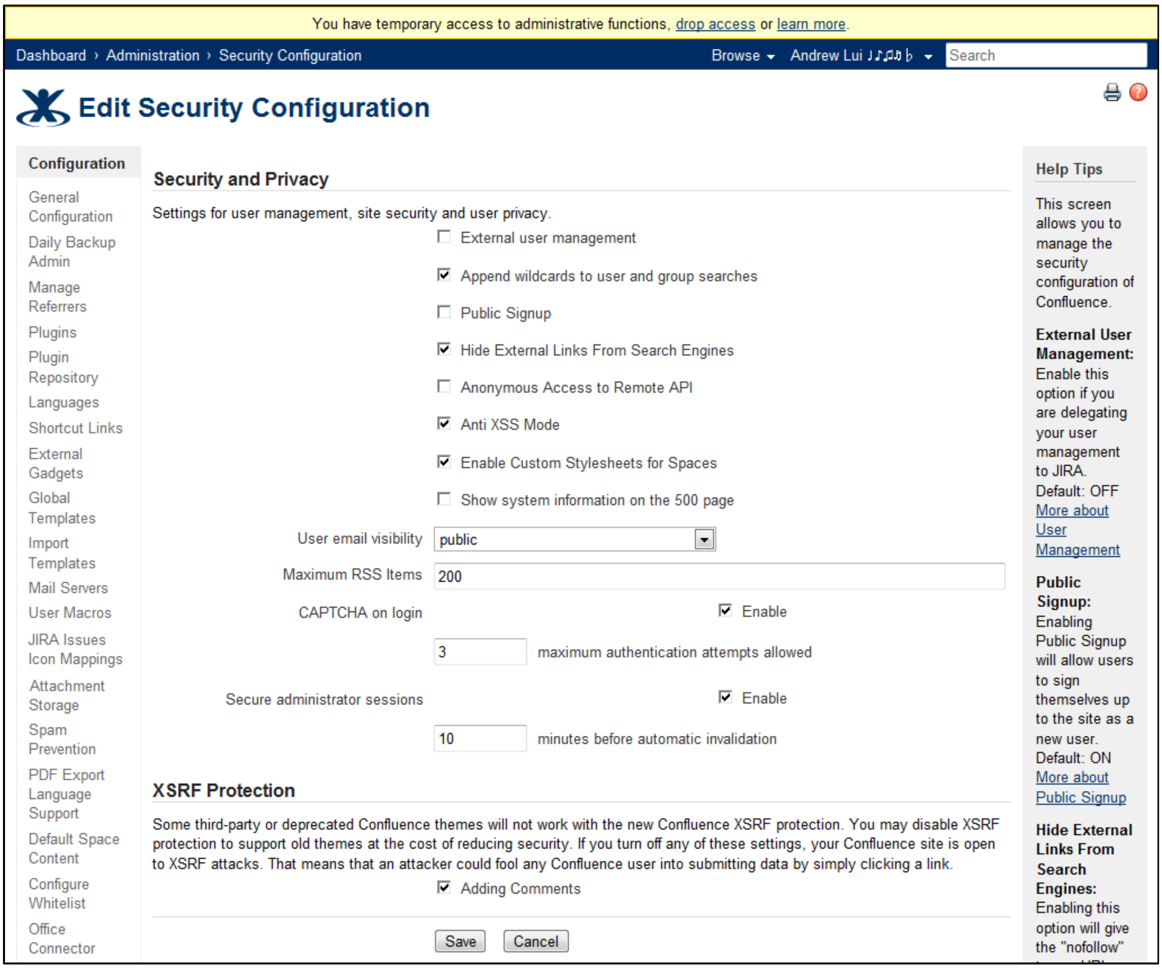
Confluence protects access to its administrative functions by requiring a secure administration session to use the Confluence administration console or administer a space. When a Confluence administrator (who is logged into Confluence) attempts to access an administration function, they are prompted to log in again. This logs the administrator into a temporary secure session that grants access to the Confluence/space administration console.

The temporary secure session has a rolling timeout (defaulted to 10 minutes). If there is no activity by the administrator in the Confluence/space administration console for a period of time that exceeds the timeout, then the administrator will be logged out of the secure administrator session (note, they will remain logged into Confluence). If the administrator does click an administration function, the timeout will reset.

⚠ *The information on this page does not apply to Confluence OnDemand.*

To configure secure administrator sessions:

1. Choose **Browse** > **Confluence Admin**.
2. Click '**Security Configuration**' in the '**Security**' section. The 'Edit Security Configuration' screen will be displayed.
3. Click the '**Edit**' link.
    - To disable secure administrator sessions (i.e. administrators will not be required to log into a secure session to access the administration console), uncheck the '**Enable**' checkbox next to '**Secure administrator sessions**'.
    - To change the timeout for secure administrator sessions, update the value in textbox next to '**minutes before invalidation**'. The default timeout for a secure administration session is 10 minutes.
4. Click the '**Save**' button.



You have temporary access to administrative functions, drop access or learn more.

Edit Security Configuration

Security and Privacy

Settings for user management, site security and user privacy.

□ External user management

☑ Append wildcards to user and group searches

□ Public Signup

☑ Hide External Links From Search Engines

□ Anonymous Access to Remote API

☑ Anti XSS Mode

☑ Enable Custom Stylesheets for Spaces

□ Show system information on the 500 page

User email visibility: public

Maximum RSS Items: 200

CAPTCHA on login: ☑ Enable

3 maximum authentication attempts allowed

Secure administrator sessions: ☑ Enable

10 minutes before automatic invalidation

XSRF Protection

Some third-party or deprecated Confluence themes will not work with the new Confluence XSRF protection. You may disable XSRF protection to support old themes at the cost of reducing security. If you turn off any of these settings, your Confluence site is open to XSRF attacks. That means that an attacker could fool any Confluence user into submitting data by simply clicking a link.

☑ Adding Comments

Help Tips

This screen allows you to manage the security configuration of Confluence.

External User Management: Enable this option if you are delegating your user management to JIRA. Default: OFF More about User Management

Public Signup: Enabling Public Signup will allow users to sign themselves up to the site as a new user. Default: ON More about Public Signup

Hide External Links From Search Engines: Enabling this option will give the "nofollow"

Screenshot above: Configuring secure administrator sessions

Notes

- **Disabling password confirmation.** Confluence installations that use a custom authentication mechanism may run into problems with the Confluence security measure that requires password confirmation. If necessary, you can set the `password.confirmation.disabled` system property to disable the password confirmation functionality. See Recognised System Properties. See issue CONF-20958 "Confluence features that require password confirmation (websudo, captcha) do not work with custom authentication".
- **WebSudo.** The feature that provides secure administrator sessions is also called 'WebSudo'.
- **Manually ending a secure session.** An administrator can choose to manually end their secure session by clicking the '**drop access**' link in the banner displayed at the top of their screen.
- **Note for developers.** Secure administrator sessions can cause exceptions when developing against Confluence or deploying a plugin. Please read this FAQ: How do I develop against Confluence with Secure Administrator Sessions? Note: The Confluence XML-RPC and REST APIs are not affected by secure administration sessions.

Using Fail2Ban to limit login attempts

What is Fail2Ban?

We need a means of defending sites against brute-force login attempts. Fail2Ban is a Python application which trails logfiles, looks for regular expressions and works with Shorewall (or directly with iptables) to apply temporary blacklists against addresses that match a pattern too often. This can be used to limit the rate at which a given machine hits login URLs for Confluence.

⚠ *The information on this page does not apply to Confluence OnDemand.*

Prerequisites

- Requires Python 2.4 or higher to be installed
- Needs a specific file to follow, which means your Apache instance needs to log your Confluence access to a known logfile. You **should adjust the configuration below** appropriately.

How to set it up

This list is a skeletal version of the instructions

- There's an RPM available for RHEL on the download page, but you can also download the source and set it up manually
- Its configuration files go into `/etc/fail2ban`
- The generic, default configuration goes into `.conf` files (`fail2ban.conf` and `jail.conf`). Don't change these, as it makes upgrading difficult.
- Overrides to the generic configuration go into `.local` files corresponding to the `.conf` files. These only need to contain the specific settings you want overridden, which helps maintainability.
- Filters go into `filter.d` — this is where you define regexps, each going into its own file
- Actions go into `action.d` — you probably won't need to add one, but it's handy to know what's available
- "jails" are a configuration unit that specify one regexp to check, and one or more actions to trigger when the threshold is reached, plus the threshold settings (e.g. more than 3 matches in 60 seconds causes that address to be blocked for 600 seconds)
- Jails are defined in `jail.conf` and `jail.local`. Don't forget the `enabled` setting for each one — it can be as bad to have the wrong ones enabled as to have the right ones disabled.

Running Fail2Ban

- Use `/etc/init.d/fail2ban {start|stop|status}` for the obvious operations
- Use `fail2ban-client -d` to get it to dump its current configuration to STDOUT. Very useful for troubleshooting.
- Mind the CPU usage; it can soak up resources pretty quickly on a busy site, even with simple regexp
- It can log either to syslog or a file, whichever suits your needs better

Common Configuration

jail.local

```
# The DEFAULT allows a global definition
of the options. They can be override
# in each jail afterwards.

[DEFAULT]
```

```
# "ignoreip" can be an IP address, a CIDR
mask or a DNS host. Fail2ban will not
# ban a host which matches an address in
this list. Several addresses can be
# defined using space separator.
# ignoreip = <space-separated list of IPs>

# "bantime" is the number of seconds that
a host is banned.
bantime  = 600

# A host is banned if it has generated
"maxretry" during the last "findtime"
# seconds.
findtime  = 60

# "maxretry" is the number of failures
before a host get banned.
maxretry = 3


[ssh-iptables]

enabled  = false


[apache-shorewall]

enabled  = true
filter   = cac-login
action   = shorewall
logpath =
/var/log/httpd/confluence-access.log
bantime = 600
maxretry = 3
```

```
findtime = 60
backend = polling
```

Configuring for Confluence

> ⚠ The following is an example only, and you should adjust it for your site.

filter.d/confluence-login.conf

```
[Definition]

failregex = <HOST>.*"GET /login.action

ignoreregex =
```

Securing Confluence with Apache

The following outlines some basic techniques to secure a Confluence instance using Apache. These instructions are basic to-do lists and should not be considered comprehensive. For more advanced security topics see the "Further Information" section below.

- Using Apache to limit access to the Confluence administration interface
- Using Fail2Ban to limit login attempts

Further Information

Running Confluence behind Apache

> ⚠ *The information on this page does not apply to Confluence OnDemand.*

Using Apache to limit access to the Confluence administration interface

Limiting administration to specific IP addresses

The Confluence administration interface is a critical part of the application; anyone with access to it can potentially compromise not only the Confluence instance but the entire machine. As well as limiting access to users who really need it, and using strong passwords, you should consider limiting access to it to certain machines on the network or internet. If you are using an Apache web server, this can be done with Apache's **Location** functionality as follows:

> ⚠ *The information on this page does not apply to Confluence OnDemand.*

1. Create a file that defines permission settings

This file can be in the Apache configuration directory or in a system-wide directory. For this example we'll call it "sysadmin_ips_only.conf". The file should contain the following:

```
Order Deny,Allow
 Deny from All

 # Mark the Sysadmin's workstation
 Allow from 192.168.12.42
```

2. Add the file to your Virtual Host

In your Apache Virtual Host, add the following lines to restrict the administration actions to the Systems Administrator:

> This configuration assumes you've installed Confluence under '/confluence'. If you have installed under '/' or elsewhere, adjust the paths accordingly.

```
<Location /confluence/admin>
  Include sysadmin_ips_only.conf
</Location>
<Location /confluence/plugins/servlet/oauth/consumers/list>
  Include sysadmin_ips_only.conf
</Location>
<Location /confluence/plugins/servlet/oauth/view-consumer-info>
  Include sysadmin_ips_only.conf
</Location>
<Location /confluence/plugins/servlet/oauth/service-providers/list>
  Include sysadmin_ips_only.conf
</Location>
<Location /confluence/plugins/servlet/oauth/service-
```

```
providers/add>
  Include sysadmin_ips_only.conf
</Location>
<Location
/confluence/plugins/servlet/oauth/consumer
s/add>
  Include sysadmin_ips_only.conf
</Location>
<Location
/confluence/plugins/servlet/oauth/consumer
s/add-manually>
  Include sysadmin_ips_only.conf
</Location>
<Location
/confluence/plugins/servlet/oauth/update-c
onsumer-info>
  Include sysadmin_ips_only.conf
</Location>
<Location
/confluence/pages/templates/listpagetempla
tes.action>
  Include sysadmin_ips_only.conf
</Location>
<Location
/confluence/pages/templates/createpagetemp
late.action>
  Include sysadmin_ips_only.conf
</Location>
<Location
/confluence/spaces/spacepermissions.action
>
  Include sysadmin_ips_only.conf
</Location>
```

```
<Location
/confluence/pages/listpermissionpages.acti
on>
  Include sysadmin_ips_only.conf
</Location>
<Location
/confluence/spaces/removespace.action>
  Include sysadmin_ips_only.conf
</Location>
<Location
/confluence/spaces/importmbox.action>
  Include sysadmin_ips_only.conf
</Location>
<Location
/confluence/spaces/viewmailaccounts.action
>
  Include sysadmin_ips_only.conf
</Location>
<Location
/confluence/spaces/addmailaccount.action?>
  Include sysadmin_ips_only.conf
</Location>
<Location
/confluence/spaces/importpages.action>
  Include sysadmin_ips_only.conf
</Location>
<Location
/confluence/spaces/flyingpdf/flyingpdf.act
ion>
  Include sysadmin_ips_only.conf
</Location>
<Location
/confluence/spaces/exportspacehtml.action>
```

```
  Include sysadmin_ips_only.conf
</Location>
<Location
/confluence/spaces/exportspacexml.action>
  Include sysadmin_ips_only.conf
</Location>
<Location
/confluence/plugins/servlet/embedded-crowd
>
  Include sysadmin_ips_only.conf
</Location>
```

```
<Location /confluence/plugins/servlet/upm>
  Include sysadmin_ips_only.conf
</Location>
```

Enabling or Disabling Public Signup

When public signup is enabled on your Confluence site, people can add their own usernames and log in to the site immediately.

If you want to restrict your site to a particular set of users, you may want to disable public signup. This means that your signup mode is **private**. In both public and private signup modes, you can invite new users to sign up or add them manually.

You need Confluence Administrator or System Administrator permissions to change the signup mode.

Choosing public or private signup

You can set your signup mode to public or private at the same time as adding or inviting new users to the site. See Adding Users.

On this page:

- Choosing public or private signup
- Another way of enabling public signup
- Enabling and disabling notifications about user signup

Related pages:

- User Management
- Setting Up Public Access
- Configuring Confluence Security
- Global Permissions Overview

⚠ *The information on this page does not apply to Atlassian OnDemand sites with multiple apps. If you are using Confluence-only OnDemand, the information does apply.*

Another way of enabling public signup

The option to enable public signup is also available on the 'Security Configuration' screen. The public signup option has the same effect as described above. Disabling public signup is the same as setting signup mode to **private**.

To enable or disable public signup:

1. Choose **Browse** > **Confluence Admin**.
2. Select **Security Configuration** in the left-hand panel.
3. Click **Edit**.
4. Tick the **Public Signup** checkbox to enable public signup. Clear the checkbox to disable public signup.
5. Click **Save**.

Enabling and disabling notifications about user signup

By default, Confluence will send an email notification to all Confluence administrators whenever someone signs up to the Confluence site, either by clicking the 'Sign Up' link or by clicking the invitation URL sent by an administrator.

To disable this notification:

1. Choose **Browse** > **Confluence Admin**.
2. Choose **Users** > **Add User**.
3. Remove the tick from **Notify administrators when users sign up**.

Managing External Referrers

An external referrer is any site that links to your Confluence instance. Each time someone clicks on the external link, your Confluence site can record the click as a referral.

By default, external referrers for a page are listed under '**Hot Referrers**' on the '**Info**' screen of the page. (See *S creenshot 1* below.) Confluence shows a maximum of 10 referrers. If there are more than 10, confluence shows the 10 with the highest number of hits.

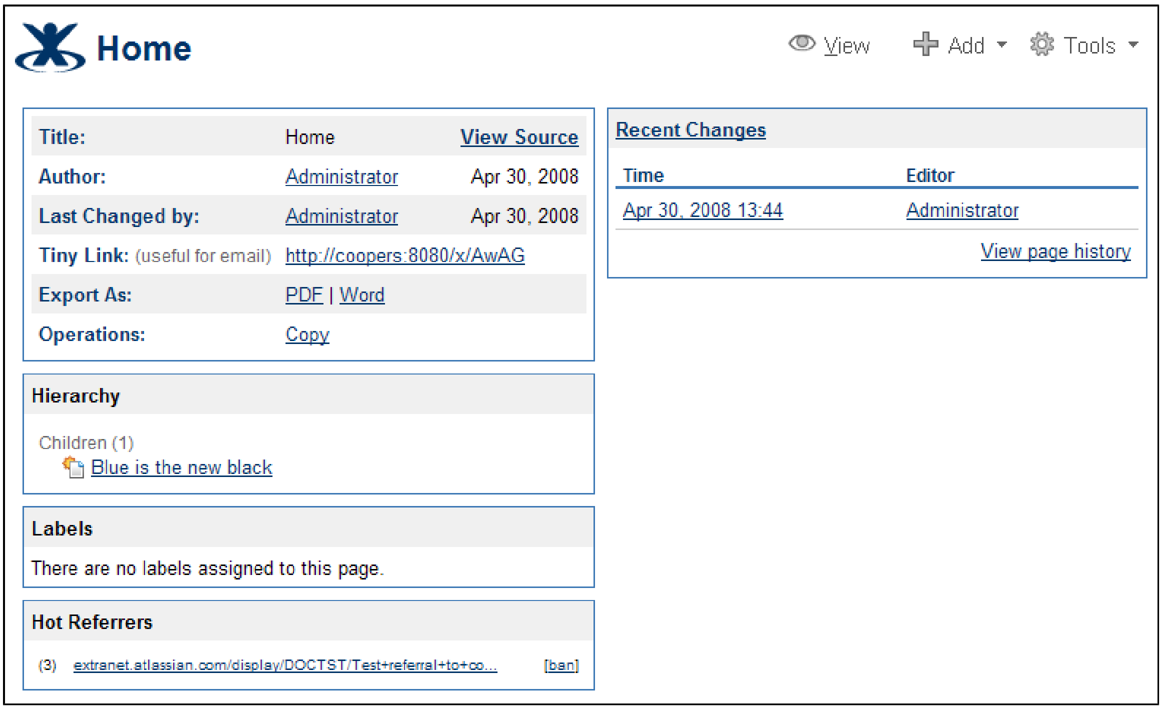
Note that you do *not* need to enable trackback in order to have external referrers enabled.

To manage your external referrers:

1. Choose **Browse** > **Confluence Admin**.
2. Select the '**Manage Referrers**' option (See *Screenshot 2* below.).

The following actions will be available:

- Record or ignore all external referrers: By default, Confluence records the number of hits made to a page from the link on the external site. If you turn this option off, Confluence will not record the hits.
- Show or hide all external referrers: By default, Confluence lists the external referrers as '**Hot Referrers**' on the '**Info**' screen of a page, as shown below. If you turn this option off, external referrers will not be listed on the page.
- Specify which external referrers to exclude: You can decide which referrers you want to exclude from being displayed on your site.



Title:	Home	View Source
Author:	Administrator	Apr 30, 2008
Last Changed by:	Administrator	Apr 30, 2008
Tiny Link: (useful for email)	http://coopers:8080/x/AwAG	
Export As:	PDF | Word	
Operations:	Copy	

Recent Changes

Time	Editor
Apr 30, 2008 13:44	Administrator

View page history

Hierarchy

Children (1)
Blue is the new black

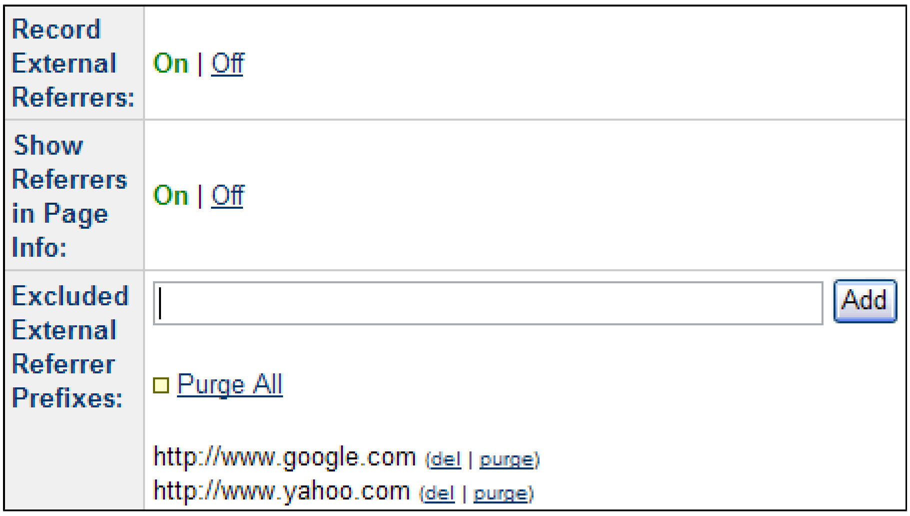
Labels

There are no labels assigned to this page.

Hot Referrers

(3) extranet.atlassian.com/display/DOCTST/Test+referral+to+co... [ban]

Screenshot above: Hot Referrers showing on a page's Info screen



Record External Referrers:	On | Off
Show Referrers in Page Info:	On | Off
Excluded External Referrer Prefixes:	Add □ Purge All http://www.google.com (del | purge) http://www.yahoo.com (del | purge)

Screenshot above: Managing external referrers

Related Topics

No content found for label(s) security-options.

Administrators Guide Home Confluence Documentation Home

Excluding external referrers

An external referrer is any site that links to your Confluence instance. Each time someone clicks on the external link, your Confluence site can record the click as a referral.

You can exclude external referrers to prevent them from being recorded or displayed anywhere on your site. Once you have specified your list of blocked URLs, any incoming links from URLs that match the list will no longer be recorded. Referrer URLs are blocked if they start with any of the URLs in the exclusion list. So http://evilspamsite.blogspot.com will also match http://evilspamsite.blogspot.com/nastypage.html

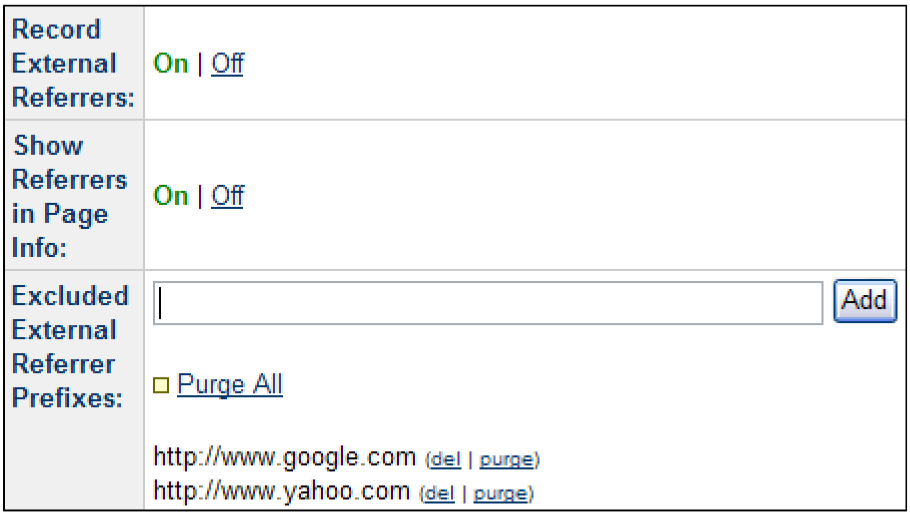
There are two instances where you may want to do this:

1. If you are running a Confluence installation that is open to public:
   In a site that is open to public, one unfortunate problem is that malicious sites can spam the display of a page's incoming links statistics. This is usually done to get the site's URL to appear in the sidebar. By adding these sites to the 'excluded referrers' list, you can prevent them from being listed on your site.
2. If Confluence is installed on a server with multiple domain names or IP addresses:
   Confluence will consider any URL originating from the domain name where Confluence is installed as an internal link. However, if Confluence is installed on a server with multiple domain names or IP addresses, you will need to add the other domain name prefixes to this list to let Confluence know that any links from these domains should not be considered external links.

ⓘ You need to be a Confluence administrator and to know the URL of the site to add it to the excluded referrers list.

To add a URL to the excluded referrers list:

1. Choose **Browse** > **Confluence Admin**.
2. Select **Manage Referrers** in the left-hand panel.
3. Add the URL to the 'Excluded External Referrer Prefixes' section.
   - You must include 'http://' at the front of the URL.
   - You can add more than one URL by putting each URL on a new line.



Record External Referrers:	On | Off
Show Referrers in Page Info:	On | Off
Excluded External Referrer Prefixes:	[ ] Add □ Purge All http://www.google.com (del | purge) http://www.yahoo.com (del | purge)

Screenshot above: Excluding external referrers

Related Topics

No content found for label(s) security-options.

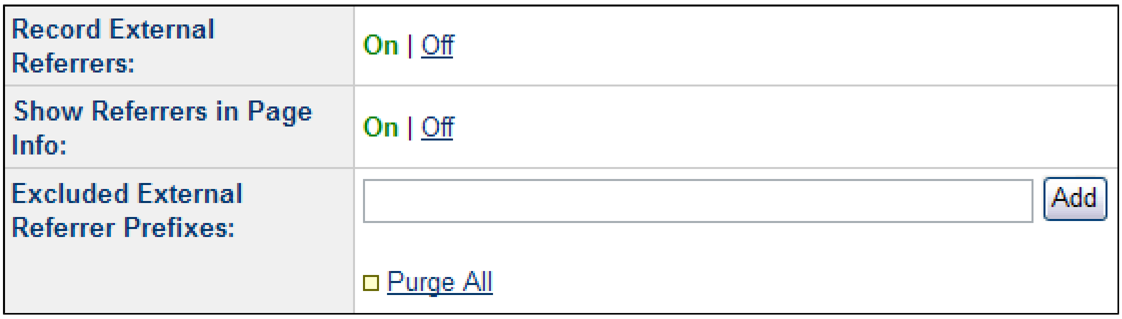
Administrators Guide Home Confluence Documentation Home

Hiding external referrers

By default, Confluence lists the external referrers as '**Hot Referrers**' on the '**Info**' screen of a page. If you turn this option off, external referrers will not be listed on the page.

To hide external referrers:

1. Choose **Browse** > **Confluence Admin**.
2. Select '**Manage Referrers**' in the left-hand panel.
3. Click '**Off**' beside '**Show Referrers in Page Info**'.



Record External Referrers:	On | Off
Show Referrers in Page Info:	On | Off
Excluded External Referrer Prefixes:	Add □ Purge All

Screenshot: Managing external referrers

Related Topics

No content found for label(s) security-options.

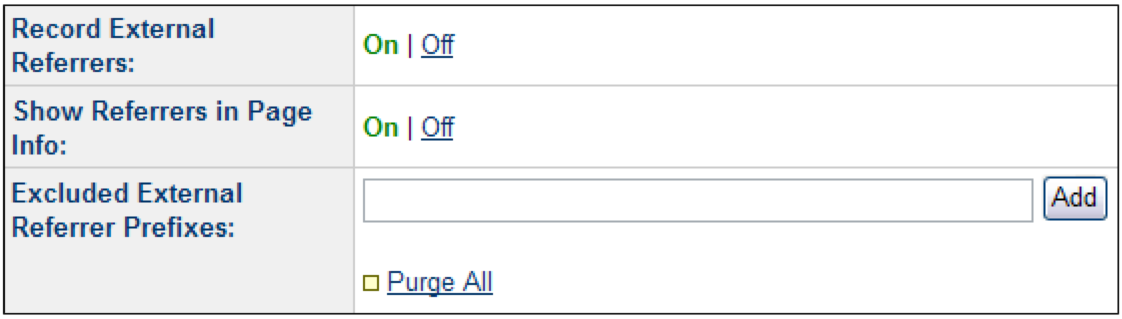
Administrators Guide Home Confluence Documentation Home

Ignoring External Referrers

An external referrer is any site that links to your Confluence instance. Each time someone clicks on the external link, your Confluence site can record the click as a referral. By default, Confluence records the number of hits made to a page from any link on an external site. If you turn this option off, Confluence will not record the hits.

To ignore external referrers:

1. Choose **Browse** > **Confluence Admin**.
2. Select '**Manage Referrers**' in the left-hand panel.
3. Click '**Off**' beside '**Record External Referrers**'.



Record External Referrers:	On | Off
Show Referrers in Page Info:	On | Off
Excluded External Referrer Prefixes:	Add □ Purge All

Screenshot above: Managing external referrers

Related Topics

No content found for label(s) security-options.

Administrators Guide Home Confluence Documentation Home

Best Practices for Configuring Confluence Security

The best way to harden a system is to look at each of the involved systems individually. Contact your company's security officer or department to find out what security policies you should be using. There are many things to consider, such as the configuration of your underlying operating systems, application servers, database servers, network, firewall, routers, etc. It would be impossible to outline all of them here.

This page contains guidelines on good security practices, to the best of our knowledge.

⚠ *The information on this page does not apply to Confluence OnDemand.*

Configuring the Web Server

Please refer to the following guides for system administrators:

- How to configure Apache to lock down the administration interface to those people who really need it: Using Apache to limit access to the Confluence administration interface.
- How to reduce the risk of brute force attacks: Using Fail2Ban to limit login attempts.

Configuring the Application Server

See the following system administrator guide for general hints on the application server level:

- Tomcat security best practices

Configuring the Application

The way you set up Confluence roles, permissions and processes makes a big difference in the security of your Confluence site.

Below are some more Confluence-specific items to consider. None of these provides 100% security. They are measures to reduce impact and to slow down an intruder in case your system does become compromised.

- Keep the number of Confluence administrators extremely low. For example, 3 system administrator accounts should be the maximum.
- Similarly, restrict the number of users with powerful roles or group memberships. If only one department should have access to particularly sensitive data, then do restrict access to the data to those users. Do not let convenience over-rule security. Do not give all staff access to sensitive data when there is no need.
- The administrators should have separate Confluence accounts for their administrative roles and for their day to day roles. If John Doe is an administrator, he should have a regular user account without administrator access to do his day to day work (such as writing pages in the wiki). This could be a 'john.doe' account. In addition, he should have an entirely separate account (that cannot be guessed by an outsider and that does not even use his proper name) for administrative work. This account could be 'jane smith' – using a username that is so obscure or fake that no outsider could guess it. This way, even if an attacker singles out the actual person John Doe and gets hold of his password, the stolen account would most likely be John's regular user account, and the attacker cannot perform administrative actions with that account.
- Lock down administrative actions as much as you can. If there is no need for your administrators to perform administrative actions from outside the office, then lock down access to those actions to known IP adresses, for example. See Using Apache to limit access to the Confluence administration interface.
- Put documented procedures in place for the case of employees leaving the company.
- Perform security audits regularly. Know who can help in case a security breach occurs. Perform 'what if' planning exercises. ('What is the worst thing that could happen if a privileged user's password were stolen while he's on vacation? What can we do to minimise damage?').
- Make sure the Confluence database user (and all datasource database users) only has the amount of database privileges it really needs.
- Monitor your binaries. If an attacker compromises an account on your system, he will usually try to gain access to more accounts. This is sometimes done by adding malicious code, such as by modifying files on the system. Run routine scripts that regularly verify that no malicious change has been made.

As another precaution:

- Regularly monitor the above requirements. There are many things that could start out well, but deteriorate over time:
  - A system may start out with just 3 administrators, but over the course of a year this could grow to

30 administrators if no one prevents expansion.
- Apache administration restrictions may be in place at the start of the year, but when the application server is migrated after a few months, people may forget to apply the rules to the new system.

Again, keep in mind that the above steps may only be a fraction of what could apply to you, depending on your security requirements. Also, keep in mind that none of the above rules can guarantee anything. They just make it harder for an intruder to move quickly.

Hiding the People Directory

The People Directory provides a list of all users in your Confluence system.

If you need to disable the People Directory set the following system properties on your application server command line:

- **To disable the People Directory for anonymous users,**

```
-Dconfluence.disable.peopledirectory.anonymous=true
```

- **To disable the People Directory entirely,**

```
-Dconfluence.disable.peopledirectory.all=true
```

⚠ *The information on this page does not apply to Confluence OnDemand.*

This workaround will prevent the People directory from appearing on the dashboard, but if you navigate to the profile of a user, and then click on the "People" in the breadcrumb link (Dashboard >> **People** >> FullName >> Profile) or you go to the URL directly `<CONFLUENCE_INSTALL>/browsepeople.action`, you will be able to access the people directory.

To workaround this, set up Apache webserver in front of confluence and redirect requests to this URL.

To remove the link on the dashboard:

Procedure for Confluence 2.5.2 to 2.9.x. only

ⓘ This only applies to Confluence 2.5.2 to 2.9.x. Confluence 2.10.x or later only needs to configure system properties using the above.
Edit the <confluence-install>/confluence/decorators/global.vmd:
Comment out line 37:

```
<!--                    <img
src="$req.contextPath/images/icons/people_directory_32.gif" align='absmiddle'
height="32" width="32"> <b><a
class="fontSizeDefault"
href="$req.contextPath/peopledirectory.action">
$action.getText("people.directory.title")</a></b><span class="smalltext"> -
$action.getText("people.directory.description")</span><br> -->
```

Related Topics

No content found for label(s) security-options.

Administrators Guide Home Confluence Documentation Home

Configuring Captcha for Spam Prevention

ⓘ You need to be a Confluence administrator to configure Captcha for spam prevention in Confluence.

If your Confluence site is open to the public you may find that automated spam is being added, in the form of comments or new pages.

You can configure Confluence to deter automated spam by asking users to prove that they are human before they are allowed to:

- Sign up for an account.
- Add a comment.
- Create a page.
- Edit a page.
- Send a request to the Confluence administrators.

Captcha is the technical term for a test that can distinguish a human being from an automated agent such as a web spider or robot. You can read more about Captcha on Wikipedia.

When Captcha is switched on, users will need to recognise a distorted picture of a word, and must type the word into a text field. This is easy for humans to do, but very difficult for computers.

Screenshot above: Example of a Captcha test

You can configure Confluence to enforce Captcha for certain types of users. You can exempt logged-in users (they will have completed a Captcha when they signed up) or members of particular groups.

By default, Captcha for spam prevention is disabled. If you enable it, the default is that Captcha for spam prevention will apply to anonymous users only. Only anonymous users will have to perform the Captcha test when creating comments or editing pages. Captcha images will not be shown to logged-in users.

To enable Captcha for spam prevention in Confluence:

1. Choose **Browse** > **Confluence Admin**.
2. Select '**Spam Prevention**' from the 'Configuration' menu on the left.
3. Turn on Captcha by clicking the '**ON**' link.
4. If you want to disable Captcha for certain groups:
   - Select '**No one**' if you want everyone to see Captchas.
   - Select '**Signed in users**' if you want only anonymous users to see Captchas.
   - If you want everyone to see Captchas except members of specific groups, select the '**Members of the following groups**' and enter the group names in the text box.
     You can click the magnifying-glass icon to search for groups. Search for all or part of a group name and click the '**Select Groups**' button to add one or more groups to the list.
   - To remove a group from the list, delete the group name.
5. Click the '**Save**' button.

Related Topics

No content found for label(s) security-options.

Administrators Guide Home Confluence Documentation Home

Hiding External Links From Search Engines

Hiding external links from search engines helps to discourage spammers from posting links on your site. If you turn this option on, any URLs inserted in pages and comments will be given the 'nofollow' attribute, which prevents search engines from following them.

ℹ Shortcut links (e.g. CONF-2622@JIRA) and internal links to other pages within Confluence are not tagged.

The information on this page does not apply to Atlassian OnDemand sites with multiple apps. If you are using Confluence-only OnDemand, the information does apply.

To hide external links from search engines:

1. Choose **Browse** > **Confluence Admin**.
2. Click '**Security Configuration**' in the left panel.
3. This will display the '**Security Configuration**' screen. Click '**Edit**'.
4. Check the '**Hide External Links From Search Engines**' checkbox.
5. Click the '**Save**' button.

Background to the nofollow attribute

As part of the effort to combat the spamming of wikis and blogs (Confluence being both), Google came up with some markup which instructs search engines not to follow links. By removing the main benefit of wiki-spamming it's hoped that the practice will stop being cost-effective and eventually die out.

Related Topics

No content found for label(s) security-options.

Administrators Guide Home Confluence Documentation Home

Configuring Captcha for Failed Logins

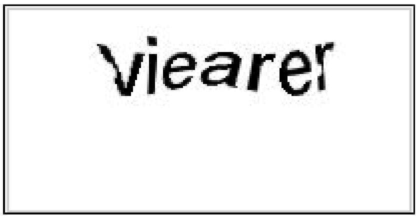
If you have confluence administrator permissions, you can configure Confluence to impose a maximum number of repeated login attempts. After a given number of failed login attempts (the default is three) Confluence will display a Captcha form asking the user to enter a given word when attempting to log in again. This will prevent brute force attacks on the Confluence login screen.

Similarly, after three failed login attempts via the XML-RPC or SOAP API, an error message will be returned instructing the user to log in via the web interface. Captcha will automatically be activated when they attempt this login.

The information on this page does not apply to Confluence OnDemand.

'Captcha' is the technical term for a test that can distinguish a human being from an automated agent such as a web spider or robot. You can read more about Captcha on Wikipedia.

When Captcha is activated, users will need to recognise a distorted picture of a word, and must type the word into a text field. This is easy for humans to do, but very difficult for computers.



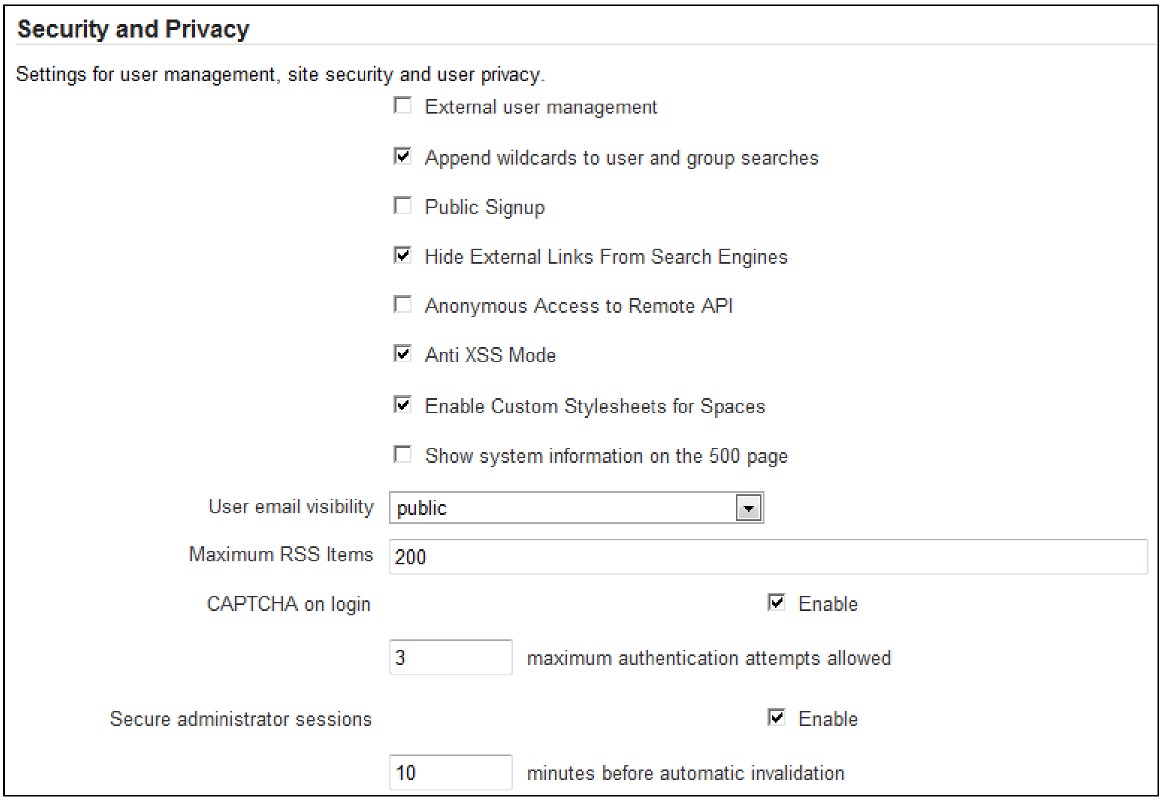
Screenshot above: Example of a Captcha test

Enabling, Disabling and Configuring Captcha for Failed Logins

By default, Captcha for failed logins is enabled and the number of failed login attempts is set to three.

To enable, disable and configure Captcha for failed logins:

1. Choose **Browse** > **Confluence Admin**.
2. Select '**Security Configuration**' from the 'Security' menu on the left.
3. Click the '**Edit**' button.
4. To enable Captcha:
   - Check the '**Enable**' checkbox next to '**CAPTCHA on login**'.
   - Set the maximum number of failed logins next to '**Maximum Authentication Attempts Allowed**'. You must enter a number greater than zero.
5. To **disable** Captcha, remove the check from the '**Enable**' checkbox.
6. Click the '**Save**' button.



Security and Privacy

Settings for user management, site security and user privacy.

☐ External user management

☑ Append wildcards to user and group searches

☐ Public Signup

☑ Hide External Links From Search Engines

☐ Anonymous Access to Remote API

☑ Anti XSS Mode

☑ Enable Custom Stylesheets for Spaces

☐ Show system information on the 500 page

User email visibility: public

Maximum RSS Items: 200

CAPTCHA on login: ☑ Enable

3 maximum authentication attempts allowed

Secure administrator sessions: ☑ Enable

10 minutes before automatic invalidation

Screenshot above: Configuring Captcha for failed logins

Notes

- **Disabling all password confirmation requests, including Captcha on login.** Confluence installations that use a custom authentication mechanism may run into problems with the Confluence security measure that requires password confirmation. If necessary, you can set the `password.confirmation.disabled` system property to disable the password confirmation functionality on administrative actions, change of email address and Captcha for failed logins. See Recognised System Properties.

Related Topics

Administrators Guide Home Confluence Documentation Home

Configuring XSRF Protection

Confluence requires an XSRF token to be present on comment creation, to prevent users being tricked into unintentionally submitting malicious data (read more about XSRF (Cross Site Request Forgery)). All of the themes bundled with Confluence have been designed to use this feature. However, if you are using a custom theme that does not support this security feature, you can disable it.

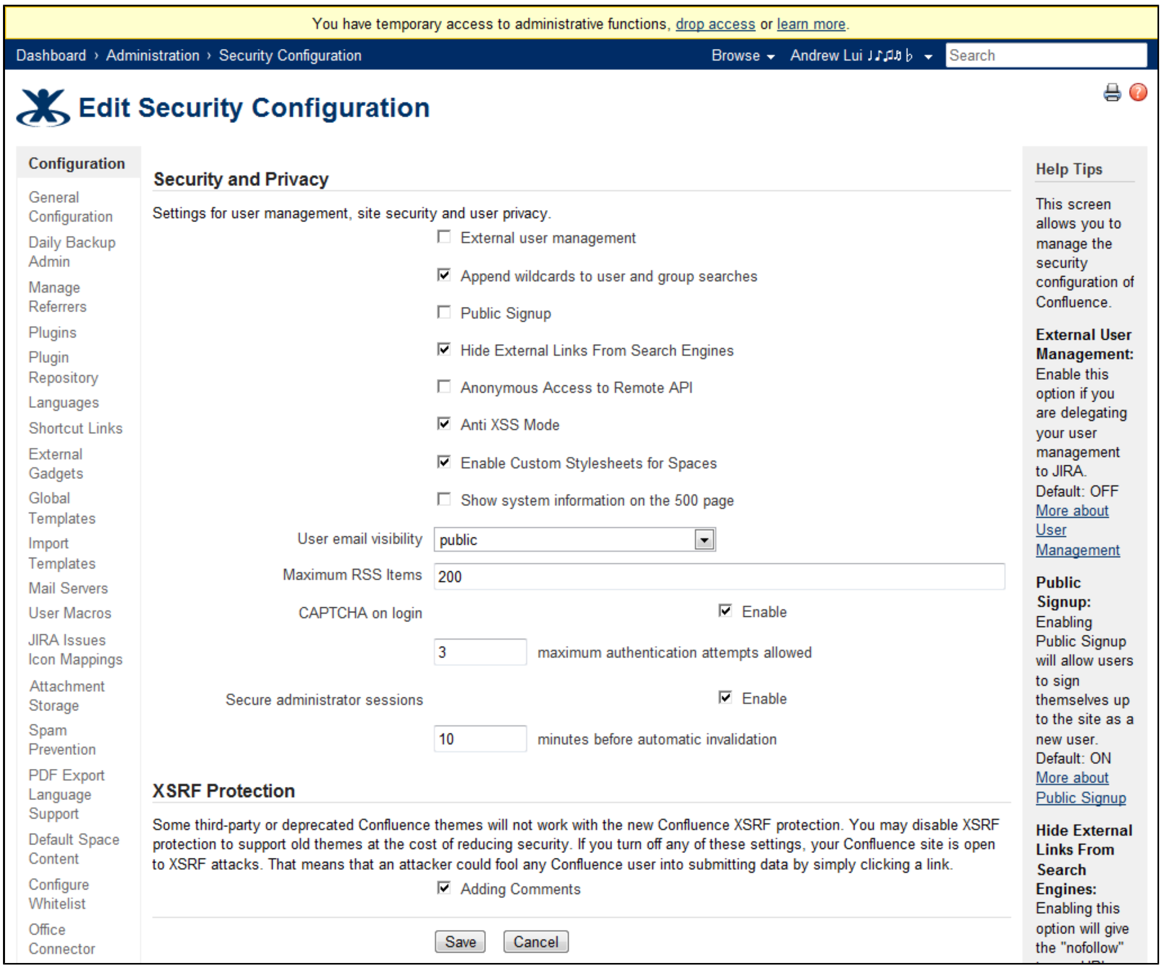
⚠ **Please carefully consider the security risks before you disable XSRF protection in your Confluence**

installation.

⚠ *Some functionality described on this page is restricted in* ***Confluence OnDemand****.*

To configure XSRF protection:

1. Choose **Browse** > **Confluence Admin**.
2. Click '**Security Configuration**' in the '**Security**' section. The 'Edit Security Configuration' screen will be displayed.
3. Click the '**Edit**' link.
4. To disable XSRF protection, uncheck the '**Add Comments**' checkbox in the '**XSRF Protection**' section.
5. Click the '**Save**' button.



Security and Privacy

Settings for user management, site security and user privacy.

☐ External user management

☑ Append wildcards to user and group searches

☐ Public Signup

☑ Hide External Links From Search Engines

☐ Anonymous Access to Remote API

☑ Anti XSS Mode

☑ Enable Custom Stylesheets for Spaces

☐ Show system information on the 500 page

User email visibility: public

Maximum RSS Items: 200

CAPTCHA on login: ☑ Enable

3 maximum authentication attempts allowed

Secure administrator sessions: ☑ Enable

10 minutes before automatic invalidation

XSRF Protection

Some third-party or deprecated Confluence themes will not work with the new Confluence XSRF protection. You may disable XSRF protection to support old themes at the cost of reducing security. If you turn off any of these settings, your Confluence site is open to XSRF attacks. That means that an attacker could fool any Confluence user into submitting data by simply clicking a link.

☑ Adding Comments

Help Tips

This screen allows you to manage the security configuration of Confluence.

External User Management: Enable this option if you are delegating your user management to JIRA. Default: OFF More about User Management

Public Signup: Enabling Public Signup will allow users to sign themselves up to the site as a new user. Default: ON More about Public Signup

Hide External Links From Search Engines: Enabling this option will give the "nofollow"

Screenshot: Configuring XSRF protection

User Email Visibility

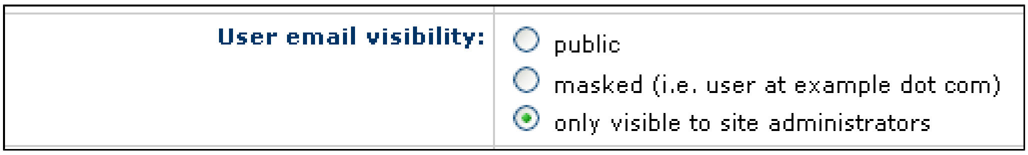
Confluence provides three options for email address privacy which can be configured by a Confluence administrator from the **Administration Console**:

- **Public**: email addresses are displayed publicly.
- **Masked**: email addresses are still displayed publicly, but masked in such a way to make it harder for spam-bots to harvest them.
- **Only visible to site administrators**: only Confluence administrators can see the email addresses. Note that, if you select this option, email addresses will not be available in the 'User Search' popup (e.g. when setting Page Restrictions).

⚠ *The information on this page does not apply to Confluence OnDemand.*

To configure user email visibility:

1. Choose **Browse** > **Confluence Admin**.
2. Select '**Security Configuration**' in the left-hand panel. The '**Security Configuration**' screen will be displayed.
3. Click '**Edit**'. The fields on the '**Security Configuration**' screen will be editable.
4. Select one of the options from the '**User email visibility**' dropdown: '**public**', '**masked**', or '**only visible to site administrators**'.
5. Click the '**Save**' button.



User email visibility: ○ public
○ masked (i.e. user at example dot com)
● only visible to site administrators

Screenshot above: Email Visibility

Related Topics

No content found for label(s) security-options.

Administrators Guide Home Confluence Documentation Home

Anonymous Access to Remote API

Sites may wish to disable anonymous access to the remote API to make it harder for malicious users to write 'bots' that perform bulk changes to the site. If you wish to enable the Remote APIs but do not want anonymous users to access Confluence remotely, you can disable anonymous access from the **Administration Console**.

To disable anonymous access to Remote APIs:

1. Choose **Browse** > **Confluence Admin**.
2. Click '**Security Configuration**' in the left panel. The '**Security Configuration**' screen will be displayed.
3. Click '**Edit**'. The fields on the '**Security Configuration**' screen will now be editable.
4. Uncheck the '**Anonymous Access to API**' checkbox.
5. Click the '**Save**' button.

Related Topics

No content found for label(s) security-options.

Administrators Guide Home Confluence Documentation Home

Running Confluence Over SSL or HTTPS

This document tells you how to configure Confluence to enable access via HTTPS (HTTP over SSL), so that your Confluence logins and data are encrypted during transport to and from Confluence. SSL encryption is a good way to safeguard your Confluence data and user logins from being intercepted and read by outsiders.

These instructions apply to the following platforms:

- **Confluence or Confluence WAR distribution using Tomcat.** Apache Tomcat is the application server shipped with Confluence, and is the only supported application server. If you are using a different application server or Apache HTTP Server ("httpd"), see the page on Apache with mod_proxy for instructions on how to terminate an SSL connection at the Apache web server.
- **Java 6.** JDK 1.6 is the supported Java version for Confluence. Note that you need the JDK, since it

includes the `keytool` utility used in the instructions below. The JRE is not enough. If you are using JDK 1.5, please refer to the Java SE documentation to see the differences in the `keytool` utility from JDK 1.5 to JDK 1.6.

ℹ The default connector port for Confluence is 8090, while a plain Tomcat installation (used for EAR / WAR distribution) will default to 8080.

On this page:

⚠ *The information on this page does not apply to Confluence OnDemand.*

Step 1. Create or Request a New SSL Certificate

You will need a valid SSL certificate before you can enable HTTPS. If you already have a certificate prepared, skip to step 2 below.

You can choose to create a self-signed certificate or to use a certificate issued by a certificate authority (CA, sometimes also called a 'certification authority'). We described both options below.

Certificate Option 1 – Create a Self-Signed Certificate

Self-signed certificates are useful if you require encryption but do not need to verify the identity of the requesting website. In general, you might use a self-signed certificate on a test environment and on internal corporate networks (intranets).

Because the certificate is not signed by a certificate authority (CA), users may receive a message that the site is not trusted and may have to perform several steps to accept the certificate before they can access the site. This usually will only occur the first time they access the site.

Follow the steps below to generate a certificate using Java's `keytool` utility. This tool is included in the JDK.

1. Use Java's `keytool`utility to generate the certificate:
   - On Windows, run the following command at the command prompt:

     ```
     "%JAVA_HOME%\bin\keytool" -genkeypair -alias tomcat -keyalg RSA
     ```

   - On OS X or UNIX-based systems, run the following command at the command prompt:

     ```
     $JAVA_HOME/bin/keytool -genkeypair -alias tomcat -keyalg RSA
     ```

2. When asked for a **password**:
    - Specify the password you want to use for the certificate (private key). Note that the password text will not appear as you type it.
    - Make a note of the password you choose, because you will need it in the next step when editing the configuration file.
    - The default password is '`changeit`'.
3. Follow the prompts to specify your name, organisation and location. This information is used to construct the X.500 Distinguished Name (DN) of the entity. The DN must match the fully-qualified hostname of the server running Confluence. For example:
`CN=Java Duke, OU=Java Software Division, O=Sun Microsystems Inc, C=US`
4. Enter 'y' to confirm the details.
5. When asked for the **password** for '`tomcat`' (the alias you entered in the keytool command above), press the 'Enter' key. This specifies that your keystore entry will have the **same password** as your private key. You MUST use the same password here as was used for the keystore password itself. This is a restriction of the Tomcat implementation.
6. You certificate is now ready. Go to step 2 below.

Certificate Option 2 – Use a Certificate Issued by a Certificate Authority

When running Confluence in a production environment, you will need a certificate issued by a certificate authority (CA, sometimes also called a 'certification authority') such as VeriSign, Thawte or TrustCenter. The instructions below are adapted from the Tomcat documentation.

First you will generate a local certificate and create a 'certificate signing request' (CSR) based on that certificate. You will submit the CSR to your chosen certificate authority. The CA will use that CSR to generate a certificate for you.

1. Use Java's `keytool` utility to generate a local certificate, as described in the previous section.
2. Use the `keytool` utility to generate a CSR, replacing the text `<MY_KEYSTORE_FILENAME>` with the path to and file name of the `.keystore`file generated for your local certificate:

```
keytool -certreq -keyalg RSA -alias tomcat -file certreq.csr -keystore
<MY_KEYSTORE_FILENAME>
```

3. Submit the generated file called `certreq.csr` to your chosen certificate authority. Refer to the documentation on the CA's website to find out how to do this.
4. The CA will send you a certificate.
5. Import the new certificate into your local keystore:

```
keytool -importcert -alias tomcat -keystore <MY_KEYSTORE_FILENAME>
-file <MY_CERTIFICATE_FILENAME>
```

Step 2. Modify the Server Configuration File in your Confluence Installation

1. Edit the server configuration file at this location: `{CONFLUENCE-INSTALLATION}>/conf/server.xml`.
2. Uncomment the following lines:

```
<Connector port="8443" maxHttpHeaderSize="8192"
                   maxThreads="150" minSpareThreads="25"
maxSpareThreads="75"
                   enableLookups="false" disableUploadTimeout="true"
                   acceptCount="100" scheme="https" secure="true"
                   clientAuth="false" sslProtocol="TLS"
SSLEnabled="true"
                   URIEncoding="UTF-8"
keystorePass="<MY_CERTIFICATE_PASSWORD>"/>
```

3. Replace the text `<MY_CERTIFICATE_PASSWORD>` with the password you specified for your certificate.
4. Make sure that the attribute-value pair `SSLEnabled="true"` is part of the `Connector` element, as shown above. If this attribute is not present, attempts to access Confluence will time out.
5. Save the server configuration file.

Step 3. Specify the Location of your Certificate

By default, Tomcat expects the keystore file to be named `.keystore` and to be located in the user home directory under which Tomcat is running (which may or may not be the same as your own home directory). This means that, by default, Tomcat will look for your SSL certificates in the following location:

- On Windows: `C:\Documents and Settings\\#CURRENT_USER#\.keystore`
- On OS X and UNIX-based systems: `~/.keystore`

You may decide to move the certificate to a custom location. If your certificate is not in the default location, you will need to update your server configuration file as outlined below, so that Tomcat can find the certificate.

1. Edit the server configuration file at this location: `{CONFLUENCE-INSTALLATION}>/conf/server.xml`
2. Add the attribute `keystoreFile="<MY_CERTIFICATE_LOCATION>"` to the `Connector`element, so that the element looks like this:

```
<Connector port="8443" maxHttpHeaderSize="8192"
                   maxThreads="150" minSpareThreads="25"
maxSpareThreads="75"
                   enableLookups="false" disableUploadTimeout="true"
                   acceptCount="100" scheme="https" secure="true"
                   clientAuth="false" sslProtocol="TLS"
SSLEnabled="true"
                   URIEncoding="UTF-8"
keystorePass="<MY_CERTIFICATE_PASSWORD>"
                   keystoreFile="<MY_CERTIFICATE_LOCATION>"/>
```

3. Replace the text `<MY_CERTIFICATE_LOCATION>` with the path to your certificate, including the path and the name of the `.keystore` file.
4. Save the server configuration file.

Step 4. Change your Confluence Base URL to HTTPS

1. In your browser, go to the Confluence Administration Console.
2. Change the Server Base URL to HTTPS. See the documentation on configuring the server base URL.
3. Restart Tomcat and access Confluence on `https://<MY_BASE_URL>:8443/`.

Step 5. Add a Security Constraint to Cause Redirect of All URLs to HTTPS

Although HTTPS is now activated and available, the old HTTP URLs (http://localhost:8090) are still available. Now you need to redirect the URLs to their HTTPS equivalent. You will do this by adding a security constraint in `web.xml`. This will cause Tomcat to redirect requests that come in on a non-SSL port.

1. Check whether your Confluence site uses the **RSS macro**. If your site has the RSS macro enabled, you may need to configure the URL redirection with a firewall rule, rather than by editing the `web.xml` file. Skip the steps below and follow the steps on the RSS Feed Macro page instead.
2. Otherwise, Edit the file at `<CONFLUENCE_INSTALLATION>/confluence/WEB-INF/web.xml`.
3. Add the following declaration to the end of the file, **before** the `</web-app>`tag:

```
<security-constraint>
  <web-resource-collection>
    <web-resource-name>Restricted URLs</web-resource-name>
    <url-pattern>/</url-pattern>
  </web-resource-collection>
  <user-data-constraint>
    <transport-guarantee>CONFIDENTIAL</transport-guarantee>
  </user-data-constraint>
</security-constraint>
```

4. Restart Confluence and access http://localhost:8090. You should be redirected to https://localhost:8443/login.action.

ℹ Confluence has two web.xml files. The other one is at `<CONFLUENCE_INSTALLATION>/conf/web.xml`. Please only add the security constraints to `<CONFLUENCE_INSTALLATION>/confluence/WEB-INF/web.xml`, as described above.

Notes

- **Background information on generating a certificate:** The '`keytool -genkeypair`' command generates a key pair consisting of a public key and the associated private key, and stores them in a keystore. The command packages the public key into an X.509 v3 self-signed certificate, which is stored as a single-element certificate chain. This certificate chain and the private key are stored in a new keystore entry, identified by the `alias` that you specify in the command. The Java SE documentation has a good overview of the utility.

- **Custom SSL port:** If you have changed the port that the SSL connector is running on from the default value of 8443, you must update the `redirectPort` attribute of the standard HTTP connector to reflect the new SSL port. Tomcat needs this information to know which port to redirect to when an incoming request needs to be secure.

- **Protection for logins only or for individual spaces:** As of Confluence 3.0, Atlassian does not support HTTPS for logins only or for specific pages. We support only site-wide HTTPS. To see the reasoning behind this decision, please see CONF-18120 and CONF-4116.

Troubleshooting

- Check the Confluence knowledge base articles on troubleshooting SSL.

- If any of your users will access Confluence from **Internet Explorer 7 on Vista**, please note the following additional points when using Java's `keytool`utility:
  - Make sure that you specify the `-keyalg RSA` option, as shown in the example of the `keytool` command above. The default is the SHA1 algorithm, which results in an error 'Internet Explorer cannot display the webpage' on IE7 on Vista.
  - You may also need to specify the `-sigalg MD5withRSA` option. Otherwise, SHA1 will be used

even if you specify the `-keyalg RSA` option. See this Atlassian blogpost for more information.

- Problems with **Internet Explorer being unable to download attachments**: Applying SSL site wide can prevent IE from downloading attachments correctly. To fix this problem, edit `<CONFLUENCE_INSTALLATION>/conf/server.xml` and add the following line within the `<Context ... />`element:

```
<Valve
className="org.apache.catalina.authenticator.NonLoginAuthenticator"
       disableProxyCaching="true" securePagesWithPragma="false" />
```

Related Topics

- SSL Configuration HOW-TO in the Apache Tomcat 6.0 documentation
- SSL Configuration HOW-TO in the Apache Tomcat 5.5 documentation
- keytool - Key and Certificate Management Tool in the Java SE documentation
- Connecting to LDAP or JIRA or Other Services via SSL
- Supported Platforms

Connecting to LDAP or JIRA or Other Services via SSL

This page describes how to get Confluence connecting to external servers over SSL, via the various SSL-wrapped protocols.

Here are some examples of when you may need to connect to an external server over SSL/HTTPS:

- You need to connect to an LDAP server, such as Active Directory, if the LDAP server is running over SSL.
  For specific instructions for Active Directory, see Configuring an SSL Connection to Active Directory.
- You want to set up JIRA as a trusted application in Confluence, when JIRA is running over SSL.
- You want to refer to an https://... URL in a Confluence macro.

If you want to run Confluence itself over SSL, see Running Confluence Over SSL or HTTPS.

⚠ *The information on this page does not apply to Confluence OnDemand.*

✓ There's a Beta version of a Confluence SSL plugin that facilitates this process.

Importing SSL Certificates

The following commands apply to JDK 1.5. For commands/syntax relevant to JDK 1.6, please refer to this document from Oracle.

1. Add the root certificate to your default Java keystore with the following command. This is the certificate that was used to authorise the LDAP server's certificate. It will be either the one that was used for signing it, or will come from further up in the trust chain, possibly the root certificate. This is often a self-signed certificate, when both ends of the SSL connection are within the same network. Again, the exact alias is not important.

```
keytool -import -alias serverCert -file RootCert.crt -keystore
%JAVA_HOME%/jre/lib/security/cacerts (Windows)
keytool -import -alias serverCert -file RootCert.crt -keystore
$JAVA_HOME/jre/lib/security/cacerts (Linux/Unix/Mac)
```

2. Import your LDAP or JIRA server's public certificate into the JVM Keystore. This is the certificate that the LDAP server will use to set up the SSL encryption. You can use any alias of your choosing in place of "JIRAorLDAPServer.crt".

```
keytool -import -alias ldapCert -file JIRAorLDAPServer.crt -keystore
%JAVA_HOME%/jre/lib/security/cacerts (Windows)
keytool -import -alias ldapCert -file JIRAorLDAPServer.crt -keystore
$JAVA_HOME/jre/lib/security/cacerts (Linux/Unix/Mac)
```

3. Verify that the certificate has been added successfully by entering the following command:

```
keytool -list -keystore %JAVA_HOME%/jre/lib/security/cacerts (Windows)
keytool -list -keystore $JAVA_HOME/jre/lib/security/cacerts
(Unix/Linux)
keytool -list -keystore /Library/Java/Home/lib/security/cacerts (Mac)
```

4. Ensure that you have updated JAVA_OPTS to specify the path to the keystore, as specified in Connecting to SSL services, before restarting Tomcat/Confluence.
   There is no need to specify an alias for Confluence to use. On connecting to the LDAP server, it will search through the keystore to find a certificate to match the key being presented by the server.

Troubleshooting

Check the following knowledge base articles:

- Unable to Connect to SSL Services due to PKIX Path Building Failed sun.security.provider.certpath.SunCertPathBuilderException
- SSL troubleshooting articles

Related Topics

Configuring an SSL Connection to Active Directory
Configure Web Proxy Support for Confluence
Running Confluence Over SSL or HTTPS

Configuring RSS Feeds

A Confluence System Administrator can configure the following aspects of RSS feeds:

- The maximum number of items that Confluence returns to an RSS feed request.
- The maximum time period that Confluence allows to respond to an RSS feed request.

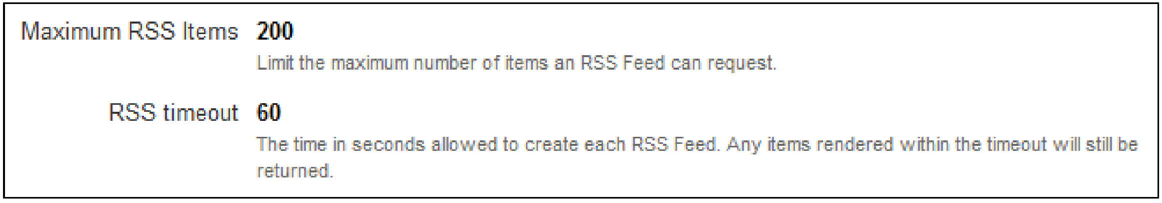
Both of these are set in the 'Edit Security Configuration' screen.

⚠ *The information on this page does not apply to Confluence OnDemand.*

To configure RSS feeds:

1. Choose **Browse** > **Confluence Admin**.
2. Click **Security Configuration** in the left panel. The 'Edit Security Configuration' screen will be displayed.
3. Click **Edit**.
4. Edit the value for **Maximum RSS Items**. The default value is 200.
5. Edit the value for **RSS timeout**.
6. Click **Save**.

Screenshot: Configuring RSS feeds



Maximum RSS Items **200**

Limit the maximum number of items an RSS Feed can request.

RSS timeout **60**

The time in seconds allowed to create each RSS Feed. Any items rendered within the timeout will still be returned.

Notes

- When using the RSS Feed Builder, a user could potentially enter such a large value for the number of feed items returned that Confluence would eventually run out of memory.
- When using the Feed Builder, if a users a value greater than this setting (or less than 0) they will get a validation error.
- If any pre-existing feeds are set to request more than the configured maximum, they will be supplied with only the configured maximum number of items. This is done silently - there is no logging and no message is returned to the RSS reader.
- If Confluence times out when responding to an RSS feed request, any items already rendered are returned.

Related Topics

Using the RSS Feed Builder

Design and Layout

- Choosing a Default Language
- Custom Decorator Templates
- Customising Look and Feel Overview
  - Customising Colour Schemes
  - Customising Site and Space Layouts
    - Adding a Navigation Sidebar
      - Adding an All Versions Section to your Navigation Bar
    - Upgrading Customised Site and Space Layouts
  - Global Templates
  - Importing Templates
  - Modify Confluence Interface Text
  - Working With Decorator Macros
  - Customising a Specific Page
  - Customising PDF or HTML Content
  - Customising the Dashboard
  - Customising the eMail Templates
  - Customising the Login Page
- Themes Overview
  - Applying a Theme to a Site
  - Customising the Left Navigation Theme

- Modifying Look and Feel (for themes)
    - Configuring the Theme Plugin
    - Including Cascading Stylesheets in Themes
- Creating a Theme

> ⚠ *Some functionality described on this page is restricted in **Confluence OnDemand**.*

RELATED TOPICS

Modifying Confluence Interface Text
Site Configuration

Choosing a Default Language

Administrators can define a default language to be applied to all spaces in your Confluence site. Note that individual users can select a language preference for their session.

> ⚠ *The information on this page does not apply to Confluence OnDemand.*

Setting the Default Language

To change the default language for the Confluence site:

1. Choose **Browse** > **Confluence Admin**.
2. Select '**Languages**' in the 'Configuration' section of the left-hand panel.
3. The '**Language Configuration**' screen will appear. Select the language that you want to use as the default language for your Confluence site.

Other Settings that Affect the Language

Individual users can choose the language that Confluence will use to display screen text and messages. Note that the list of supported languages depends on the language packs installed on your Confluence site.

The language used for your session will depend on the settings below, in the following order of priority from highest to lowest:

- The language preference defined in your user profile. Note that you need to be logged in for this setting to take effect.
- The language that you choose by clicking an option at the bottom of the Confluence login screen. Confluence stores this value in a cookie. When the cookie expires, the setting will expire too.
- The language set in your browser.
    - Note that your Confluence administrator can disable this option by setting a system property.
    - The browser sends a header with a prioritised list of languages. Confluence will use the first supported language in that list.
- The default language for your site, as defined by your Confluence site administrator.

Showing User Interface Key Names for Translation

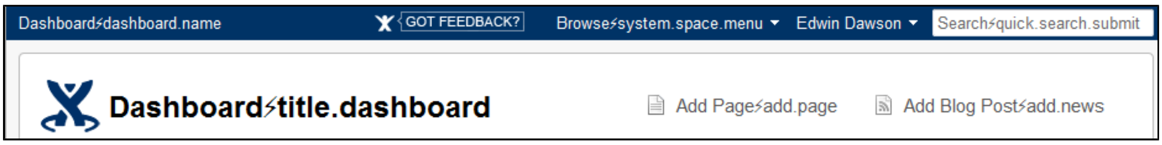
For those customers working on creating translations of the Confluence user interface, from 4.1 onwards there is a feature that will help. After opening the Confluence dashboard, you can simply add this text to the end of your Confluence URL, like so:

```
?i18ntranslate=on
```

Then press Enter.

This will then cause each element of the user interface to display its special **key name** while Confluence is still in an interactive mode. This makes it easier to find the essential context for each key, which can then be searched on http://translations.atlassian.com where you can enter an appropriate translation for your custom language pack.

The key names are displayed with a "lightning bolt" graphic between elements of the names. For example, the buttons will show up with elements shown like so:



For example, for the **Browse** button, the associated key **system.space.menu** can be found on http://translations.atlassian.com, allowing you to write a better translation for the term **Browse**, being able to see the full context of where the UI element belongs and what it means to the user.

To turn off the translation view, add this code to the end of the Confluence URL:

```
?i18ntranslate=off
```

RELATED TOPICS

Editing User Settings
Recognised System Properties
Configuring Indexing Language
Installing a Language Pack

Custom Decorator Templates

About Decorators

Confluence is built on top of the Open Source SiteMesh library, a web-page layout system that provides a consistent look and feel across a site. SiteMesh works through "decorators" that define a page's layout and structure, and into which the specific content of the page is placed. If you are interested, you can read more on the SiteMesh website.

What this means for Confluence is that you can customise the look and feel of almost all of your Confluence site through editing three decorators:

- The "Main" decorator defines the look and feel of most pages on the site
- The "Popup" decorator defines the look and feel of the popup windows such as the "Insert Link" and "History" pages.
- The "Printable" decorator defines the look and feel of the printable versions of pages (available through the 🖨 icon on each page)

You can view and edit these decorators from within Confluence: they are available from the "Layouts" option on the site's Administration menu. Changes to the decorators will affect all spaces hosted on that Confluence installation.

The decorator that is used to draw Confluence's administrative pages can not be edited from within Confluence. This means that if you make some editing mistake that renders the rest of the site unuseable, the administrative pages should still be available for you to fix the template.

⚠ *The information on this page does not apply to Confluence OnDemand.*

Browsing the Default Decorators

At any time, you can browse the default decorators that come packaged with Confluence by following the "View Default" links on the "Site Layouts" page. The template browser also allows you to view the "#parsed" templates that are included within the template when it is compiled. While you can't edit these included templates, you will probably have to copy some or all of them into your custom template as you do your customisation.

Editing Custom Decorators: Add a Logo

To edit Confluence decorators, you should have a good knowledge of HTML, and some understanding of the Velocity templating language.

The first thing you will see when you choose to create a custom "Main" decorator is... there's not much to edit. By default, most of the content of this decorator is included from other files:

```
<html>
<head>
     <title>$title - Confluence</title>

     #standardHeader()
</head>
<body onload="placeFocus()">

<div id="Content">
     <table border="0" cellpadding="0"
cellspacing="0" width="100%">
         <tr>
             <td width="60%" rowspan=2
class="logocell">#pagetitle("spacenametitl
e")</td>

             <td width="40%" align="right"
```

```
valign="top">#globalnavbar("table")</td>
         </tr>
         #if ($setup.isSetupComplete())
         <tr>
             <td align=right
valign="bottom">
                 #usernavbar()
                 #printableicon()
                 #helpicon()
             </td>
         </tr>
         #end
     </table>

     #breadcrumbsAndSearch()

     <table border="0" cellpadding="5"
cellspacing="0" width="100%"><tr><td>
<table border="0" cellpadding="0"
cellspacing="0" width="100%"><tr>

     <td valign="top" class="pagebody">
## The "toolbar-style" page operations
## #if
($page.getProperty("page.operations"))
## <table align="right"
class="toolbar"><tr><td>
## $page.getProperty("page.operations")
## </td></tr></table>
## #end

         #if
($page.getProperty("page.surtitle"))
```

```
$page.getProperty("page.surtitle")
         #end

         #if
(!$page.getProperty("page.no-page-header")
)
             <div class="pageheader">
                 <span
class="pagetitle">$title</span>
             </div>
         #end

         $body
     </td>
```

```
#parse
("/decorators/includes/complete_footer.vmd
")
```

We can add our logo, changing the "logocell" table cell:

```
<td width="60%" rowspan=2
class="logocell">
<img align="right"
src=http://www.atlassian.com/images/atlass
ian_logo.gif
width="203"
height="60">#pagetitle("spacenametitle")</
td>
```

When you insert this into the right section of the template and hit save, visitors to the site will see the logo at the top of each page. Note, the administrative pages will be unaffected: you will have to go to the dashboard or to a space to see the changes you have made.

Macros

Some parts of the page are drawn using Velocity macros, including the navigation bar. The macros you should know about when editing decorators are described in Working With Decorator Macros.

If Something Goes Terribly Wrong

From the "Site Layouts" page in Confluence's administrative menu, you can delete your custom templates. When you do this, the default template will be restored, fixing anything that may have been broken.

Alternatively, the custom templates are stored in the DECORATOR table in the database. If you have somehow managed to render Confluence completely unuseable through editing your templates, delete the relevant entries from the DECORATOR table.

For Advanced Users

The `velocity` directory is at the front of Confluence's velocity template search path. As such, you can override *any* of Confluence's velocity templates by placing an identically named file in the right place.

While we don't recommend you do this unless you know exactly what you're doing, it does give you complete control over the look of every aspect of Confluence. It also means that you can edit your templates in a text-editor if you wish, rather than through the web interface.

There are, however, two important caveats:

1. Velocity is configured to cache templates in memory. When you edit a page from within Confluence, it knows to reload that page from disk. If you are editing the pages on disk, you will either have to turn off

velocity's caching temporarily in `WEB-INF/classes/velocity.properties`, or restart the server to make your changes visible.

2. Because we only officially support the modification of the three global decorator files, other changes may interact unpredictably with future versions of Confluence. When upgrading, you should always test your custom modifications thoroughly before deploying them on a live site.

Customising Look and Feel Overview

You can customise the 'look and feel' of Confluence at both the global and space levels.

Any changes you make to the look and feel of the site at the global level will be applied as the default look and feel for all the spaces in the site. This means that any customisations will only be reflected in the "Default" theme. No other theme will have an impact from this change. An individual space can be configured to have its own look and feel through the space administration screens.

> ⚠ *Some functionality described on this page is restricted in **Confluence OnDemand**.*

Here's how you can customise the look and feel of your site:

- **Colour Scheme** : Change the colour scheme of the user interface.
- **Layouts** : Change the site layout, which determines how the controls are laid out in the site. This does not change the actual page layouts, but it does change the way the surrounding controls appear in the page.
- **Themes** : Use themes for advanced layout customisation.

RELATED TOPICS

No content found for label(s) customising-looknfeel.

Administrators Guide Home Confluence Documentation Home

Customising Colour Schemes

A Confluence administrator can configure a new colour scheme for the site dynamically from the **Administration Console**.

The default colour scheme for the site will also become the default for all spaces within it. However, it is possible for space administrators to configure a different colour scheme for spaces from the space administration screens.

> ⚠ *The information on this page does not apply to Atlassian OnDemand sites with multiple apps. If you are using Confluence-only OnDemand, the information does apply.*

To change the site's colour scheme:

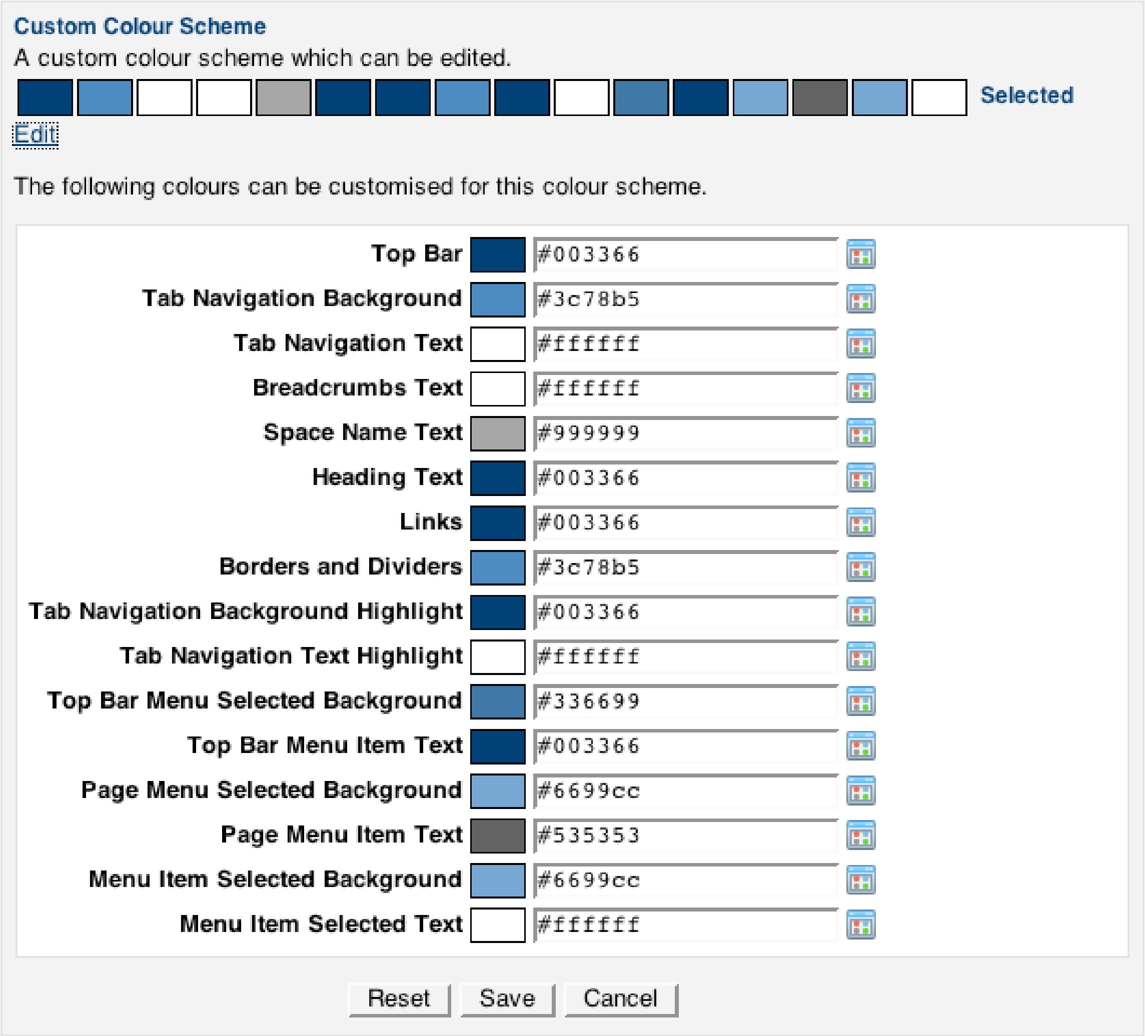
1. Choose **Browse** > **Confluence Admin**.
2. Select '**Colour Scheme**' in the left-hand panel.
   This will bring up a new screen. See screenshot below.
3. Click '**Edit**'. Enter standard HTML/CSS2 colour codes, or use the colour-picker to choose a new colour from the palette provided. Any changes you make will immediately be reflected across the Confluence installation.

The colour scheme applies to the following UI elements:

- **Top Bar -** the bar across the top of the page that contains the breadcrumbs
- **Tab Navigation Background -** the background colour of the tab navigation menus

- **Tab Navigation Text** - the text of the tab navigation menus
- **Breadcrumbs Text** - the breadcrumbs text in the top bar of the page
- **Space Name Text** - the text of the current space name located above the page title
- **Heading Text** - all heading tags throughout the space.
- **Links** - all links throughout the space.
- **Borders and Dividers** - table borders and dividing lines.
- **Tab Navigation Background Highlight** - the background colour of the tab navigation menu when highlighted
- **Tab Navigation Text Highlight** - the text of the tab navigation menu when highlighted
- **Top Bar Menu Selected Background** - the background colour of the top bar drop down menu when selected
- **Top Bar Menu Item** - the text colour of the menu items in the top bar drop down menu
- **Page Menu Selected Background** - the background colour of the drop down page menu when selected
- **Page Menu Item Text** - the text of the menu items in the drop down page menu
- **Menu Item Selected Background** - the background colour of the menu item when selected (applies to both the top bar and page drop down menus)
- **Menu Item Selected Text** - the text colour of the menu item when selected (applies to both the top bar and page drop down menus)

Please note that some UI elements are specific to the default theme and may not take effect for other themes.



Custom Colour Scheme

A custom colour scheme which can be edited.

The following colours can be customised for this colour scheme.

Top Bar	#003366
Tab Navigation Background	#3c78b5
Tab Navigation Text	#ffffff
Breadcrumbs Text	#ffffff
Space Name Text	#999999
Heading Text	#003366
Links	#003366
Borders and Dividers	#3c78b5
Tab Navigation Background Highlight	#003366
Tab Navigation Text Highlight	#ffffff
Top Bar Menu Selected Background	#336699
Top Bar Menu Item Text	#003366
Page Menu Selected Background	#6699cc
Page Menu Item Text	#535353
Menu Item Selected Background	#6699cc
Menu Item Selected Text	#ffffff

Screenshot above: Editing a site's colour scheme

Note

If you mess things up, just click the '**Reset**' button and then try again.

Related Topics

No content found for label(s) customising-looknfeel.

Administrators Guide Home Confluence Documentation Home

Customising Site and Space Layouts

You can modify Confluence's look and feel by editing the 'decorator' (layout) files. Modifying these files allows you to change the look and feel of:

- The Confluence site as a whole, which includes all spaces within the Confluence site.
- An individual space within the Confluence site.

This page tells you how to customise the layout files for your Confluence site as a whole. These customisations:

- Modify the default 'decorator' files of each space in your site.
- Are reflected in every space unless the space's own equivalent layout files have been customised.

You need System Administrator permissions to perform these customisations.

You can also customise the layout files for a given space. For more information, refer to Customising Space Layouts. Space layout customisations override the equivalent site customisations.

> ⚠ *The information on this page does not apply to Confluence OnDemand.*

> ⛔ If you modify the look and feel of Confluence by following these instructions, you will need to update your customisations when upgrading Confluence. The more dramatic the customisations are, the harder it will be to reapply your changes when upgrading. Please take this into account before proceeding with your customisation. For more information on updating your customisations, please refer to Upgrading Customised Site and Space Layouts
> .

Confluence is built on top of the open source SiteMesh library, a web-page layout system. Read more on the SiteMesh website. To edit the layout of Confluence, you will need to modify these decorator files. A decorator file is a .vmd file and is written in a very simple programming language called Velocity. You can learn more from the Velocity User Guide.

Once you are familiar with Velocity, you can edit the decorator files to personalise the appearance of Confluence.

The decorator files in Confluence are grouped into the following categories:

- **Site layouts**: These are used to define the controls that surround each page in the site. For example, the header and the footer.
- **Content layouts**: These control the appearance of content such as pages and blog posts. They do not change the way the pages themselves are displayed, but allow you to alter the way the surrounding comments or attachments are displayed.
- **Export layouts**: These control the appearance of spaces and pages when they are exported to HTML. If you are using Confluence to generate a static website, for example, you will need to modify these layouts.

Editing a site decorator file

1. Choose **Browse** > **Confluence Admin**.
2. Select **Layouts** under **Look and Feel**in the left-hand navigation panel.

    - Click **View Default** to view the .vmd file.
    - Click **Create Custom** to edit the default .vmd file. This will open up the .vmd file in edit mode.
3. Make changes and click **Update**.

If something goes wrong: Click **Reset Default** to revert to the original layouts.

Using Velocity macros

When editing Custom Decorator Templates, there are a number of macros available to define complex or variable parts of the page such as menus and breadcrumbs. You may insert these macros anywhere in your templates. More information on Working With Decorator Macros.

For advanced users

Overriding Velocity templates

The `velocity` directory is at the front of Confluence's Velocity template search path. As such, you can override *any* of Confluence's Velocity templates by placing an identically named file in the right place. While we don't recommend you do this unless you know exactly what you're doing, it does give you complete control over the look of every aspect of Confluence. It also means that you can edit your templates in a text-editor if you wish, rather than through the web interface.

Caching

Velocity is configured to cache templates in memory. When you edit a page from within Confluence, it knows to reload that page from disk. If you are editing the pages on disk, you will either have to turn off velocity's caching temporarily in `WEB-INF/classes/velocity.properties`, or restart the server to make your changes visible.

Location of Velocity files

In Confluence 2.6 and later, some Velocity files are located inside the Confluence JAR file that can be found at `confluence/WEB-INF/lib/confluence-x.x.x.jar`. To override files inside this JAR (which you can open with any ZIP tool like WinZip or 7-Zip), put your customised file in the same directory structure under `confluence/WEB-INF/classes/`.

For example, the file `templates/macros/alphaindex.vm` inside confluence.jar can be replace by putting your custom file in `WEB-INF/classes/templates/macros/alphaindex.vm`. You do not need to modify the file inside the JAR.

See also Editing Files within JAR Archives.

Finding the layout via the URL

If the layout has changed so extensively as to not be visible, you can browse to the URL directly:

```
http://<confluence base
url>/admin/resetdecorator.action?decoratorName=decorators/main.vmd
```

Substitute the base URL and the appropriate .vmd file.

RELATED TOPICS

No content found for label(s) customising-looknfeel.

Velocity Template Overview

Basic Introduction to Velocity

Administrators Guide Home Confluence Documentation Home

Adding a Navigation Sidebar

You can include a left-hand navigation sidebar (table of contents) in your Confluence space. There are two ways to do this:

- ☑ **Recommended: Use the Documentation Theme** – The Documentation theme provides the left-hand navigation sidebar that you see in this documentation. **Please go to the page that tells you how to configure the Documentation theme**.
- **Customise the Space Layouts** — This is an alternative method (documented below) that is more complex to set up than the Documentation theme and requires more maintenance with Confluence major release upgrades.

> ⚠ *The information on this page does not apply to Confluence OnDemand.*

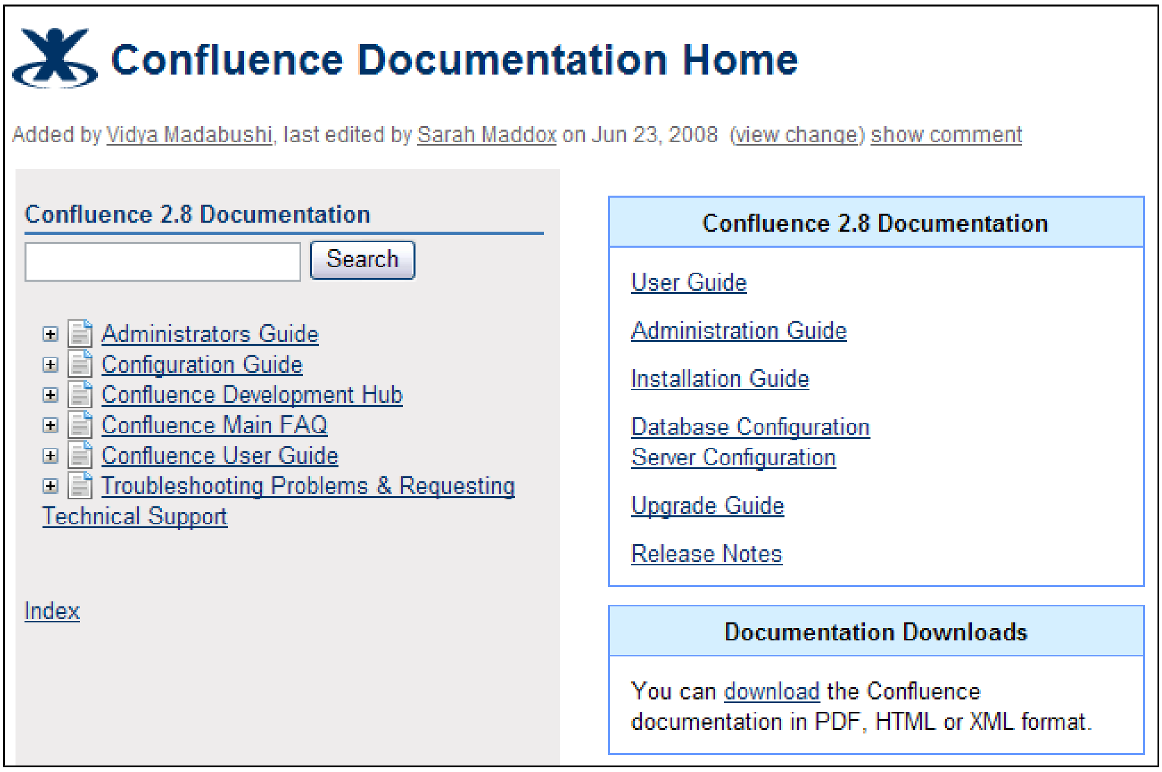
Notes to Read before you Start

Please take note of the following points before you use the method documented on this page:

- **Reapply customisation whenever you upgrade Confluence.** Every time you upgrade Confluence, you must reapply the layout customisations described on this page. When you upgrade to a new major Confluence version (such as moving from Confluence 2.9.x to Confluence 2.10.x or from Confluence 3.0.x to Confluence 3.1.x) you will need to reapply the layout customisation. See instructions below.
- **Check your wiki permissions.** To customise a space layout as described below, you must be a space administrator in the given space and you must be a system administrator on the Confluence site. See the overview of permissions and the glossary entries for space administrator and for Confluence administrator and system administrator.

Customising your Space Layouts to Add a Navigation Sidebar

Screenshot: A left-hand navigation bar resulting from customising the space layouts



Confluence Documentation Home

Added by Vidya Madabushi, last edited by Sarah Maddox on Jun 23, 2008 (view change) show comment

Confluence 2.8 Documentation

- Administrators Guide
- Configuration Guide
- Confluence Development Hub
- Confluence Main FAQ
- Confluence User Guide
- Troubleshooting Problems & Requesting Technical Support

Index

Confluence 2.8 Documentation

User Guide

Administration Guide

Installation Guide

Database Configuration
Server Configuration

Upgrade Guide

Release Notes

Documentation Downloads

You can download the Confluence documentation in PDF, HTML or XML format.

Follow the instructions below to add the navigation sidebar to your Confluence space.

Step 1. Create the TreeNavigation Page

First, you will create a Confluence page containing the `pagetree` macro. This is just a normal Confluence page. The only slight oddity is that it should reside at the root of your space, instead of under the space's home page.

Follow these instructions:

1. Go to the 'Space Pages' view for the current space. To do this:
    - Go to a page in the space and choose **Browse** > **Pages**.

   You are now at the 'root' level of your space. The 'root' level contains pages that are added above the space's home page, not as children of the home page.
2. At the root level of the space, create a page named 'TreeNavigation'.
3. On the page, insert the following text:

```
{pagetree}
```

4. Now decide if you want to add extra functionality to your page tree. By default, using the code above, the page tree will use the home page of the space as its root. You can choose to:
    - Specify a different root for your page tree.
    - Add a search box at the top of the tree.
    - Allow the viewers to expand and collapse the whole tree.
    - Control other aspects of the display.
      For more information, read about the Pagetree macro.

Step 2. Change the Space's Page Layout

Now you will change the space's page layout, to include the above page on the left of every web page displayed.

1. Choose **Browse** > **Space Admin**.
   ⓘ **Space Admin** is displayed only if you are a space administrator for that space or you are a

Confluence system administrator.

2. Make sure the Confluence Default theme is selected from the **Themes** menu.
3. Click **Layout** in the **Look and Feel** section.
   Note: The layout option is only displayed if you are a system administrator on the Confluence site.
4. Click **Create Custom** in the **Page Layout** section.
5. In the layout, locate the **VIEW** section, and find this code:

```
<div class="wiki-content">
$body
</div>
```

6. Replace the above code block with this code:

```
#if ($action.isPrintableVersion() == false)
<style>
.spacetree * ul{
padding-left:0px;
margin-left: 0px;
}
.spacetree * li{
margin-left: 5px;
padding-left:5px;
}

</style>

<table cellspacing="2" cellpadding="5">
<tr>
<td valign="top" align="left" width="22%" bgcolor="#F9F9F9"
class="noprint">
<div class="tabletitle">Table of Contents</div>
<div class="spacetree">
#includePage($helper.spaceKey "TreeNavigation")
</div>
</td>
<td valign="top" align="left" width="78%" class="pagecontent">
<div class="wiki-content">
$body
</div>
</td>
</tr>
</table>
#else
<div class="wiki-content">
    $body
</div>
#end
```

7. If you want to, you can change the table title in the above code from 'Table of Contents' to something else. For example, it might say 'Confluence Documentation'.
8. Save the updated layout.

Reapplying the Customisation on Upgrade

When you upgrade to a new major Confluence version (e.g. from Confluence 2.9.x to Confluence 2.10.x or from Confluence 3.0.x to Confluence 3.1.x), you will need to reapply this customisation.

Reason:
The new Confluence version may contain updates to the space layouts. Because you have customised the space layouts, Confluence will not overwrite your customisation. So your space will not get the latest updates until you set the layout to default and then reapply your changes.

Here's how to do it:

1. First make a copy of your customised code, if you have changed it from the code above:
   - Go to **Space Admin**, click **Layout** and edit the customised page layout (as created above).
   - Copy the section of code that inserts the customised left-hand navigation panel.
   - Close the page layout.
2. Click **Reset Default** next to **Page Layout**, to set the page layout back to default. This will bring in the new code for the upgraded version of Confluence.
3. Create a custom layout as described in step 2 above, and reinsert the custom left-hand navigation code.
4. Save the updated layout.

RELATED TOPICS

Configuring the Documentation Theme
Customising Site and Space Layouts
Upgrading Customised Site and Space Layouts
Example Confluence Designs

Adding an All Versions Section to your Navigation Bar

This page gives an example of how you might add an 'All Versions' section to your navigation side bar, as currently used in the Confluence documentation, Crowd documentation and the other Atlassian product documentation spaces.

If you are viewing this page online on the Atlassian documentation wiki, you will be able to see the 'All Versions' section at the top left of the navigation sidebar. Below is a screenshot.

A number of people have asked how we do it, so this page gives the answer. For details about creating the navigation side bar itself, please refer to Adding a Navigation Sidebar.

> ⚠ *The information on this page does not apply to Confluence OnDemand.*

Adding the Version Index to the Navigation Sidebar

This is how we added the 'All Versions' section to the sidebar:

- For each product (Confluence, Crowd, Bamboo, etc) there is a page in the Inclusions Library of the ALLDOC space. The page lists all the versions of that product's documentation, linking to the relevant spaces. For example, here is the page for Confluence and the page for Crowd.
  ℹ We put the 'all versions' page in ALLDOC because the page is used in a number of different spaces, via the {include} macro. For example, the 'all versions' page may be included:
  - In every documentation space (each version) for the product concerned, such as DOC, CONF29, CONF28, CROWD, CROWD013, CROWD012, etc.
  - In the Enterprise Hosting doc space.
  - As a panel on the documentation home page, as shown in the 'All Versions' panel of the above screenshot, as well as in the left-hand navigation bar.
  - Any other places where useful.
- In each documentation space, there is a page called 'TreeNavigationVersions' like this one or this one, which copies in the content of the above 'all versions' page.

- For each documentation space, the space's page layout now includes two pages instead of just one:
  - The 'TreeNavigation' page, as already described on the page above.
  - The new 'TreeNavigationVersions' page.

Here's the relevant section of our page layout as it is currently for the Confluence documentation (DOC) space:

```
#if ($action.isPrintableVersion() ==
false)
<style>
.spacetree * ul{
padding-left:0px;
margin-left: 0px;
}
.spacetree * li{
margin-left: 5px;
padding-left:5px;
}

</style>

<table cellspacing="2" cellpadding="5">
<tr>
<td valign="top" align="left" width="30%"
bgcolor="#eeecec" class="noprint">
<div class="tabletitle">All Versions</div>
<div class="spacetree">
#includePage($helper.spaceKey
"TreeNavigationVersions")
</div>
<div class="tabletitle">Confluence 2.10
Documentation</div>
<div class="spacetree">
#includePage($helper.spaceKey
"TreeNavigation")
</div>
```

```
</td>
<td valign="top" align="left" width="70%"
class="pagecontent">
<div class="wiki-content">
$body
</div>
</td>
</tr>
</table>
#else
<div class="wiki-content">
```

```
    $body
</div>
#end
```

Adding the Expand/Collapse Functionality to the Version Index

Another question we are asked is how we group the content of the included page under a collapsible control.

We use the Expand macro. The details are on the Expand macro's documentation page.

Related Topics

Adding a Navigation Sidebar

Upgrading Customised Site and Space Layouts

As Confluence evolves, so do the default site and space layouts that drive the rendering of every page. As new functionality is added or current functionally is changed, the default layouts are modified to support these changes.

> ⚠ If you are using custom layouts based on defaults from a previous Confluence version, you run the risk of **breaking functionality**, or worse, **missing out on great new features**!

Take care on each new release of Confluence to reapply your changes to the new default templates.

To reapply your custom layouts, you need to:

1. Obtain the source of your custom layouts from your current version of Confluence.
2. Reapply your customisations to the new default layouts.

> ⚠ *The information on this page does not apply to Confluence OnDemand.*

Step 1. Obtain your Custom Layouts

Ideally, you should keep a record of each customisation you have applied to each of your Confluence site or space layouts.

If not, you should be able to find your customisations using the following method. This method extracts all site- and space-level layouts from your Confluence site as a single output. From this output, you should be able to identify your customisations.

> ☑ This method is handy to use if you have:
>
> - Many spaces with space layout customisations, or
> - Do not have an independent record of your site or space layout customisations.

Custom layouts are stored in the `DECORATOR` table within your Confluence database. You can `SELECT` for the source of the layout using SQL like this:

```
mysql> select SPACEKEY,DECORATORNAME,BODY
from DECORATOR;
+----------+---------------------+------+
| SPACEKEY | DECORATORNAME       | BODY |
+----------+---------------------+------+
| NULL     | decorators/main.vmd | ...  |
+----------+---------------------+------+
1 row in set (0.03 sec)
```

*This example was tested on **MySQL**, but should be applicable to all SQL databases.*

Step 2. Reapply your Customisations

When you upgrade Confluence to another major release of Confluence, you will need to manually reapply any customisations you made to any site-wide or space-specific layouts. Unless otherwise stated, you should not need to reapply customisations after conducting a minor release upgrade of Confluence.

What are 'major' and 'minor' releases? Major release upgrades are ones where the 1st digit of Confluence's version number or the 1st digit after the 1st decimal place differ after the upgrade, for example, when upgrading from Confluence 3.0 to 3.1, or 2.8 to 3.0. Minor release upgrades are ones where the 1st digit of Confluence's version number and the 1st digit after the 1st decimal place remain the same after the upgrade, for example, when upgrading Confluence 3.0 to 3.0.1.

If you have made Confluence site-wide layout customisations:

1. Choose **Browse** > **Confluence Admin**.
2. Select **Layouts** under **Look and Fee**' in the left-hand navigation panel. The decorators are grouped under **Site**, **Content** and **Export** layouts.
3. Ensure you have all your customisations available (preferably in a form which can be copied and pasted).
4. Click **Reset Default** next to the layout whose customisations need to be reapplied.
5. Click **Create Custom** next to the same layout and reapply your customisations (by copying and pasting them) into the appropriate locations within the new default layout.
6. Click the **Save** button.
7. Repeat this procedure from step 4 for each layout whose customisations need to be reapplied.

If you have made space-specific layout customisations:

1. Visit any page in the relevant space.
2. Choose **Browse** > **Space Admin**.
   ℹ **Space Admin** is displayed only if you are a space administrator for that space or you are a Confluence system administrator.
3. Click **Layout** under **Look and Feel** in the left-hand navigation panel. The decorators are grouped under **Site**, **Content** and **Export** layouts.
4. Ensure you have all your customisations available (preferably in a form which can be copied and pasted).
5. Click **Reset Default** next to the layout whose customisations need to be reapplied.
6. Click **Create Custom** next to the same layout and reapply your customisations (by copying and pasting them) into the appropriate locations within the new default layout.
7. Click the **Save** button.
8. Repeat this procedure from step 5 for each layout whose customisations need to be reapplied.

Step 3. Test your Modifications Carefully

Changes may interact unpredictably with future versions of Confluence. When upgrading, you should always test your custom modifications thoroughly before deploying them on a live site. It's beyond the scope of Atlassian Support to test and deploy these changes.

Turning Off Caching

Velocity is configured to cache templates in memory. When you edit a page from within Confluence, it knows to reload that page from disk. If you are editing the pages on disk, you will either have to turn off Velocity's caching temporarily in `WEB-INF/classes/velocity.properties`, or restart the server to make your changes visible.

The `velocity.properties` file is available in the `confluence-x.x.x.jar` file, where `x.x.x` is the Confluence version number. The JAR file is located in the `WEB-INF/lib` directory. If you wish to make modification to the files in the JAR, we recommend the following steps:

1. Stop Confluence.
2. Make a backup copy of the JAR file.
3. Un-jar the file
4. Locate and edit the appropriate file that you wish to modify.
5. Re-jar the `confluence-x.x.x.jar` file.
6. Relocate the JAR file to the appropriate directory.
7. Restart Confluence.

RELATED TOPICS

Customising Site and Space Layouts

Global Templates

A template is a predefined page that can be used as a prototype when creating new pages. Templates are useful for giving pages a common style or format.

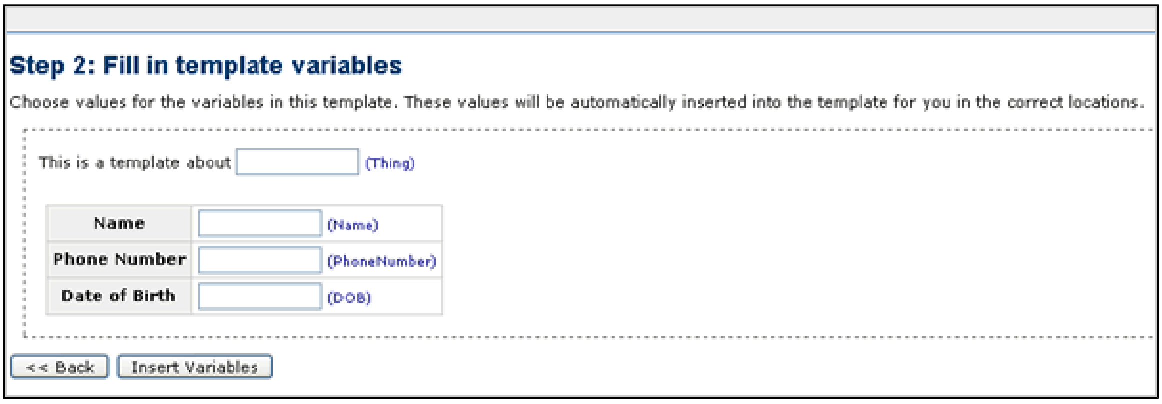
You can use regular Confluence markup to create the content of your template. You can also use special markup to define form fields that the author will fill in when creating the page.

Global templates are defined by Confluence administrators and are available in every space across the Confluence site.

To add a global template:

1. Go to the **Global Templates** option in the Confluence Administration Console, as follows:
   a. Choose **Browse** > **Confluence Admin**.
   b. Enter your password and click **Confirm**. You will be temporarily logged into a secure session to access the 'Administration Console'.
   c. Select **Global Templates** in the left-hand panel.
   d. Click **Add New Global Template**.
2. Click **Add New Global Template**.
3. Enter a name for your template in the **Name** box and an optional description in the **Description** box.
4. Using regular wiki markup and form field markup (if you are using forms), enter content in the text-entry box as you would in any other Confluence page.
5. Click **Edit** next to **Labels** if you want to use labels to categorise information. Add your labels. These labels will be included in all pages created using this template.
6. Preview and click **Save**.

Screenshot: A template as used to create a page



Step 2: Fill in template variables

Choose values for the variables in this template. These values will be automatically inserted into the template for you in the correct locations.

This is a template about (Thing)

Name	(Name)
Phone Number	(PhoneNumber)
Date of Birth	(DOB)

Related Topics

[Working with Templates](#)
[Editing a template](#)
[Removing a Template](#)
[Browsing a Space](#)
[Working with Pages](#)

Importing Templates

A template is a predefined page that can be used as a prototype when creating new pages. Templates are useful for giving pages a common style or format.
You can use regular Confluence markup to create the content of your template. You can also use special markup to define form fields that the author will fill in when creating the page.

Confluence ships with a number of templates, including the 'Charts', 'Document List' and 'Meeting Notes' templates. These templates are not available for use by default. However, if you have the appropriate permissions to access the Administration Console, you can import any of these templates to be used globally or within a specific space.

In addition, you can download additional template bundles from the Atlassian Plugin Exchange and then make them available by importing them.

On this page:

Quick guide to importing a template

1. Go to the 'Confluence Administration Console' and click **Import Templates**.
2. Select the templates that you want to import.
3. Choose which space to import the templates to, or whether to import them as global templates.
4. Click **Import**.

Step 1. Check the Templates Installed on your Confluence Site

To see the templates that are currently available for import on your Confluence site:

1. Log in to Confluence as a System Administrator or Confluence Administrator.
2. Choose **Browse** > **Confluence Admin**.
3. Select '**Import Templates**' in the left-hand panel. The '**Import Templates**' screen will appear, listing the

template packages installed on your Confluence instance (for example, 'Default Templates Package') and the templates included in each package.

Step 2. (Optional) Upload Additional Templates from the Atlassian Plugin Exchange

Additional templates are available as plugins, known as template packages. Follow the steps below if you want to add template packagess to your site that were not shipped with your Confluence installation.

Before installing a plugin into your Confluence site, please check the plugin's information page to see whether it is supported by Atlassian, by another vendor, or not at all. See our guidelines on plugin support.

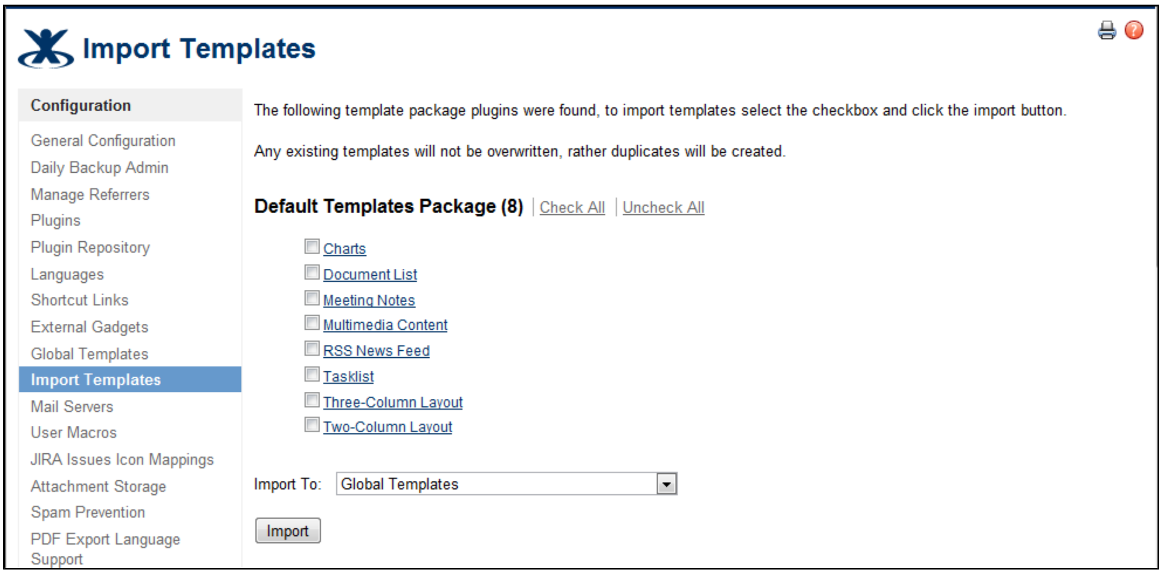
To upload more templates:

1. Go to the Atlassian Plugin Exchange and download the template bundle that you need.
2. Log in to Confluence as a System Administrator or Confluence Administrator.
3. Choose **Browse** > **Confluence Admin**.
4. Select '**Plugins**' in the left-hand panel.
5. The '**Plugins**' screen will appear. Select the '**Install**' tab.
6. Click '**Upload Plugin**', browse to find the template bundle file that you downloaded and upload it to Confluence.

Step 3. Import a Template to Make it Available to Users

To import a template:

1. Log in to Confluence as a System Administrator or Confluence Administrator.
2. Choose **Browse** > **Confluence Admin**.
3. Select '**Import Templates**' in the left-hand panel. The '**Import Templates**' screen will appear, listing the template packages installed on your Confluence instance (for example, 'Default Templates Package') and the templates included in each package.
4. Select the templates to be imported by ticking the checkboxes next to the relevant template names.
   ℹ *You can view a preview of the template by clicking the template name.*
5. Select the import destination for the templates in the '**Import To**' dropdown. If you want the templates to be available to only a specific space, select the name of the space, otherwise select '**Global Templates**' to make the templates available to all spaces.
6. Click the '**Import**' button to import the selected templates.



Import Templates

The following template package plugins were found, to import templates select the checkbox and click the import button.

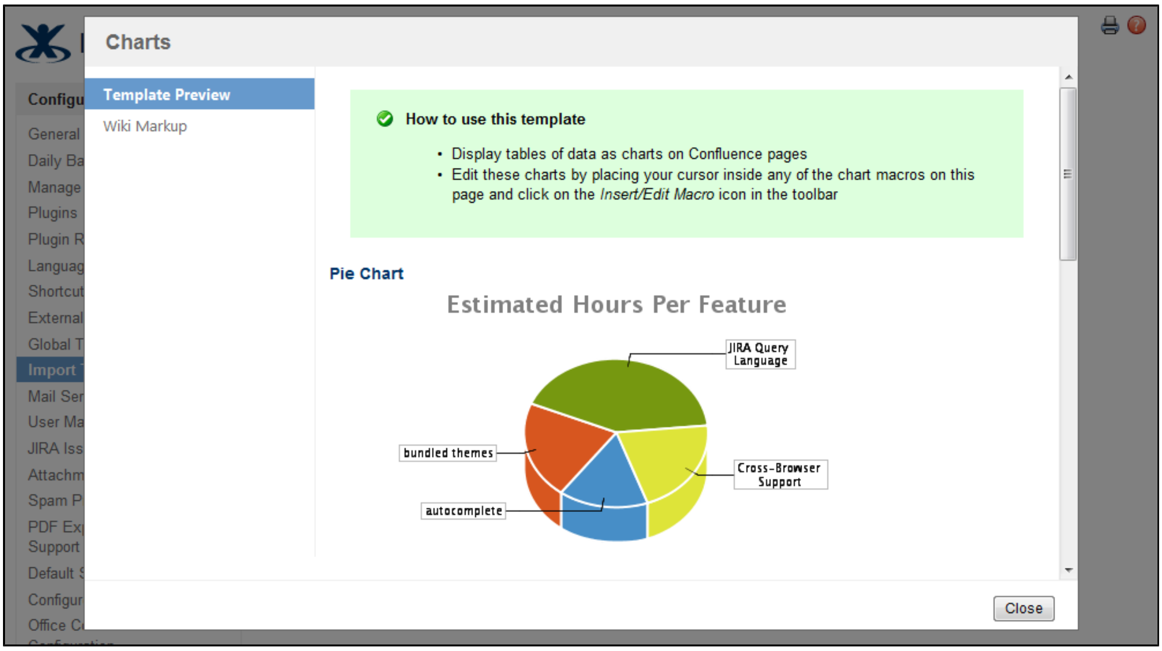
Any existing templates will not be overwritten, rather duplicates will be created.

Default Templates Package (8) | Check All | Uncheck All

□ Charts
□ Document List
□ Meeting Notes
□ Multimedia Content
□ RSS News Feed
□ Tasklist
□ Three-Column Layout
□ Two-Column Layout

Import To: Global Templates

Screenshot above: Importing a template



How to use this template

- Display tables of data as charts on Confluence pages
- Edit these charts by placing your cursor inside any of the chart macros on this page and click on the *Insert/Edit Macro* icon in the toolbar

Screenshot above: Previewing a template

Notes

- **Known issue importing templates from multiple template bundles.** There is a known issue preventing templates from being imported when multiple template bundles are available. Please read this KB article f or further information.
- **Building your own custom template bundles.** These are built as plugins and deployed to your Confluence instance. You can then import the templates from your custom template bundle, as described on this page. Read Creating A Template Bundle for instructions. Please note, you will need some programming knowledge to develop a custom template bundle.
- **Duplicate template names.** If a template with the same name already exists on import, a duplicate template of the same name will be created. You will need to check each template and rename manually.
- **Removing the template.** Removing the plugin that contains a template will not remove the template from your Confluence site if you have already imported it. You will need to remove it manually from the administration console or space.

RELATED TOPICS

Working with Templates
Editing a template
Removing a Template
Browsing a Space
Working with Pages

Modify Confluence Interface Text

All Confluence UI text is contained in a single Java properties file. This file can be modified to change the default text, and also to translate Confluence into other languages than English.

The UI text file is `ConfluenceActionSupport.properties`. From your Confluence install directory:

```
\confluence\WEB-INF\lib\confluence-3.x.jar

Within this File, the relevant file to edit is
:\com\atlassian\confluence\core\ConfluenceActionSupport.properties.
```

Refer to Editing jar files for reference.

> ⚠ *The information on this page does not apply to Confluence OnDemand.*

The file contains parameters with `name=value` pairs, in the format:

```
parameter.name=Parameter value
```

Parameter names are any text before the '=' character and should never be modified. Any text after the '=' character is the parameter value, which can be modified freely and can also contain variables. An example involving variables is:

```
popular.labels=The three most popular
labels are {0}, {1} and {2}.
```

For more information on replacing values, check out Translating ConfluenceActionSupport Content. Note that plugins store their text internally, so you must modify plugin text individually.

Steps For Modification

1. Stop Confluence
2. Under your install directory, open `\confluence\WEB-INF\lib\confluence-3.x.jar\com\atlassian\confluence\core\ConfluenceActionSupport.properties`
3. Search for the text you wish to modify, replace it and save the file in `<Confluence-Install>\confluence\WEB-INF\classes\com\atlassian\confluence\core`. Please create this folder structure, if it does not exist already.

   > ✓ If you re-bundle the JAR file, rather than re-deploy the class in the `WEB-INF\classes` directory, make sure to move the backup JAR file out of the /lib directory, or the backup may be deployed by mistake.

4. Restart Confluence

Common Modifications

- Rename 'Dashboard' by searching for `Dashboard`. To change "Dashboard" to "My Portal", change `dashboard.name=Dashboard` to `dashboard.name=My Portal`

Common Modifications

Task	Search For	Notes

Rename 'Dashboard'	Dashboard	The `dashboard.name` parameter has the name. To change 'Dashboard' to 'My Portal', change `dashboard.name=Dashboard` to `dashboard.name=My Portal` and update any other occurrences of the word 'Dashboard' in the instance
Modify login page text	login.	The `login.instructions` parameter has the "Enter your account details below to login to Confluence" text

Modify Keyboard Shortcuts

Confluence provides a set of keyboard shortcuts. You could customise the shortcuts by making modifications inside the `ConfluenceActionSupport.properties` file.

- To disable a particular shortcut, you can simply just comment out a respective line of code. One may like to disable the shortcut to one of the navigation links: *View, Edit, Attachments, Info* . For instance, to disable shortcut to *Attachments*one would comment out the following line:

```
#navlink.attachments.accesskey=a
```

- To modify an access key, one could simply just change the letter, bearing in mind the fact that the letter must be unique.

Working With Decorator Macros

Decorator Macros are Velocity macros which are used to draw complex or variable parts of the page such as menus and breadcrumbs when editing Custom decorators. Decorator macros can be inserted anywhere in your templates.

The macro is called by inserting a string of the form: #macroName("argument1" "argument2" "argument3").There are no commas between the arguments. Unless otherwise noted, these macros take no arguments.

NOTE: These macros will only work reliably when customising `main.vmd`. They may not work in other Velocity decorators. Decorator macros will not work inside normal confluence pages.

⚠ *The information on this page does not apply to Confluence OnDemand.*

Macro	Usage
`#breadcrumbs()`	Draws the "You are here" breadcrumbs list, like the one found above the page name in the default template.

`#includePage(pageTitle)`	Includes a confluence page with the specified title. If you have 2 or more pages with the same title across multiple spaces, this macro will include the page belonging to the space you are currently viewing.
`#searchbox()`	Inserts a search box into the page, like the one to the far right of the breadcrumbs in the default template.
`#globalnavbar(type)`	Draws the global navigation bar, as found in the top right-hand corner of the default template. The navigation bar can be displayed in two modes:
`#globalnavbar("table")`	Displays the navigation bar in its default mode: drawn as a table of links with coloured backgrounds and mouse-over effects.
`#globalnavbar("text")`	Displays the navigation bar as series of text links separated by | characters.
`#usernavbar()`	Draws the user-specific navigation-bar. This bar contains the links to the user's profile and history, or to the login and signup pages if the user is not logged in.
`#helpicon()`	Draws the ❓ help icon, and link to the Confluence help page.
`#printableicon()`	On pages where a printable version is available, draws the 🖨 printable page icon, linking to the printable version of the page. Otherwise, draws nothing
`#pagetitle(class)`	When you are viewing a page in a Confluence space, draws the name of the space that page is in. Otherwise, writes the word "CONFLUENCE".The "class" argument is the CSS class that the title should be drawn in. Unless you have customised your Confluence installation's CSS file, you should call this with "spacenametitle" as the class: `#pagetitle("spacenametitle")`
`#poweredby()`	Writes out the "Powered by Confluence" and Confluence version-number boilerplate found at the bottom of the default template.
`#bottomshadow()`	Draws the fading shadow-effect found at the bottom of the content area in the default template.
`#dashboardlink()`	Inserts a link to the dashboard page.

RELATED TOPICS

No content found for label(s) admin-macros.

Customising a Specific Page

If you'd like to change the appearance of a specific page, you can modify the corresponding Velocity template. Here's how to find out which one:

1. Access the page. Note the name of the action. For example, the "Contact Administrators" page is `<baseUrl>/administrators.action`.
2. Browse to <confluence-install>/confluence/WEB-INF/lib/confluence-x.y.jar. Copy the file.
3. Unzip or unjar the file using a standard unzipper or the java jar utility.
4. Open xwork.xml. Search the file for the name of the action corresponding to the page you'd like to modify. You'll see an entry like:

```
<action name="administrators"
class="com.atlassian.confluence.user.actions.AdministratorsAction">
            <interceptor-ref name="defaultStack"/>
            <result name="success"
type="velocity">/administrators.vm</result>
        </action>
```

5. The file to look for is the vm or vmd file. In the above example, it's administrators.vmd. Because there is no context path (just a / before the name of the file), its in the root of the Confluence webapp. For the stand-alone, that's <confluence-install>/confluence folder.
6. Modify the file.

For details on how to configure the file, check the Velocity Template Overview.

> ⚠ *The information on this page does not apply to Confluence OnDemand.*

RELATED CONTENT

No content found for label(s) customising-looknfeel.

Customising PDF or HTML Content

To customise Confluence's PDF output, you can edit the CSS stylesheets used by the PDF exporter. See Customising Exports to PDF.

To customise the HTML output, you will need to modify the file `confluence-x.y.z-jar/com/atlassian/confluence/pages/Page.htmlexport.vm`. See Editing Files within JAR Archives to learn how to repackage this file.

Customising the Dashboard

If you are a Confluence Administrator, you can customise the global dashboard, affecting the way all users will see the dashboard.

Confluence users can customise their own view of the dashboard too. See the user's guide.

Sending users to a space home page instead of the dashboard

See Configuring the Site Home Page.

Editing the top left-hand section of the dashboard

See Editing the Site Welcome Message.

Disabling the 'Popular' tab on the dashboard

In some environments, you may prefer not to display the new 'Popular' tab on the dashboard. For example, if your wiki allows only a small group of people to log in and contribute content or comments. then the tab may not be relevant to you.

To prevent the tab from appearing, you can disable the relevant plugin module. You need System Administrator permissions to do this. Go to the **Dashboard Macros** plugin (See Configuring a Plugin), click **Manage plugin modules** and disable the **Popular Tab** module.

On this page:

Related pages:

- Customising your Personal Dashboard
- Customising Look and Feel Overview

⚠ *The information on this page does not apply to Confluence OnDemand.*

Advanced customisations

These configurations require knowledge of plugin development and/or the Velocity template language. See our guide to the Atlassian Plugin SDK and our introduction to Velocity.

Editing the bottom left-hand section of the dashboard

This section can be updated using Confluence web panels. You can add items to the dashboard by including a web panel with the key `atl.dashboard.left`:

```
<web-panel key="{key}"
location="atl.dashboard.left">
                    <resource name="view"
type="velocity" location="{location}"/>
                </web-panel>
```

You can remove the existing entities panel by disabling the global-entities-panel plugin from the dashboard macros plugin.

Editing the top right-hand action bar

You can add more links to the top right navigation bar by adding web items to `system.dashboard.button`:

```
<web-item key="{key}" name="{name}"
section="system.dashboard.button">
                    <label key="{label}"/>
                    <link/>
                    <styleClass/>
                </web-item>
```

Modifying the global template or layout

You can also modify files to add content to the global dashboard.

To make modifications to the dashboard, modify the global template `/confluence/decorators/global.vmd` or the layout at **Administration** > **Layouts** > **Global Layout**.

For example, search the global layout for these macros:

```
$helper.renderConfluenceMacro("{recently-updated-dashboard:dashboard|showProfilePic=true}")
```

To modify the bundled plugin macros used in the Confluence dashboard:

1. Modify the `atlassian-bundled-plugins.zip` file located at `<Confluence install>/confluence/WEB-INF/classes/com/atlassian/confluence/setup`.
2. Update the `confluence-dashboard-macros-x.x.jar` file, rezip it and then put it back to `<Confluence install>/confluence/WEB-INF/classes/com/atlassian/confluence/setup`. Refer to Editing Files within JAR Archives.
3. Delete the JAR from `<confluence-home>/bundled-plugins`.
4. Restart Confluence.

To customise the space list, you can work with `spacelist.vm`.

Customising the eMail Templates

> ⛔ Customisations to the Confluence email templates will need to be reapplied when you upgrade Confluence. Consider this before making drastic changes to the layout, and be sure to keep a list of what you have changed for your upgrade process later.

Only administrators with access to the server where Confluence is running can modify the Confluence email templates.

⚠ *The information on this page does not apply to Confluence OnDemand.*

Process to change the email templates

1. Shut down your test instance of Confluence.
2. In the Confluence web application folder, find the file `/confluence/WEB-INF/lib/confluence-2.x.jar`.
3. Make a copy of this file as a backup.
4. Learn how to edit files within .jar archives.
5. Within the jar file, find the `/templates/email` folder. Find the appropriate file(s) within that folder.
6. Edit the file with a text editor to make the required changes. The content is mostly HTML, but has some Velocity template variables in it. See Velocity Template Overview for more information about how these work.
7. Again using the guide on editing files within .jar archives, either rejar the set of folders or drop the new files into the identical folder structure in the `WEB-INF/classes` directory.
8. Start Confluence up again and test your changes.
9. Apply the changes to your production Confluence instance.

The same process can be applied to modify most of the templates in the Confluence web application. For velocity files that are not in a jar file, you need not shut down and restart Confluence. Be careful to test your changes before applying them to a live site. The templates contain code that is vital for Confluence to function, and it is easy to accidentally make a change that prevents use of your site.

RELATED TOPICS

- Velocity Template Overview
- Customising Site and Space Layouts
- Customising Look and Feel Overview
- Modify Confluence Interface Text

Customising the Login Page

This page gets you started on customising the Confluence login page, to add your own logo or custom text. This will not customise the login *process*, just what users sees when they log in.

Notes:

- Customisations to the Confluence login page will need to be reapplied when you upgrade Confluence. Consider this before making drastic changes to the layout, and be sure to keep a list of what you have changed for your upgrade process later.
- Please test your changes on a **test** Confluence site first.

Only administrators with access to the server where Confluence is running can modify the Confluence login page.

Related pages:

- Editing the Global Logo
- Velocity Template Overview
- Customising Site and Space Layouts
- Customising Look and Feel Overview
- Modify Confluence Interface Text

⚠ *The information on this page does not apply to Confluence OnDemand.*

To change the login page:

1. Shut down your Confluence server.
2. In the Confluence installation directory, find the file `confluence/login.vm`.
3. Make a copy of this file as a backup.
4. Edit the file with a text editor to make the required changes. The content contains a mixture of HTML and Velocity. See Velocity Template Overview (in our developer documentation).
5. Start Confluence and test your changes.

The same process can be applied to modify most of the templates in the Confluence web application. Be careful to test your changes before applying them to a live site. The templates contain code that is vital for Confluence to function, and it is easy to accidentally make a change that prevents use of your site.

Themes Overview

Themes are pre-defined style sets that can be applied to alter the appearance of your site. Themes allow you to personalise the 'look and feel' of Confluence. You can apply a theme to your entire Confluence site and to individual spaces. Choose a specific theme if you want to add new functionality or significantly alter the appearance of Confluence.

Confluence comes with a selection of themes. In addition, a site administrator can install new themes as plugins via the Confluence Administration Console. Provided that the theme is installed into your Confluence site, any space administrator can apply a theme to a space.

By default when you create a new space, the space will have the Confluence default theme.

To look at the themes installed:

1. Choose **Browse** > **Confluence Admin**.
2. Select '**Themes**' under 'Look and Feel' in the left-hand panel.
3. You will see a list of all installed themes.

Useful Plugins

Before installing a plugin into your Confluence site, please check the plugin's information page to see whether it is supported by Atlassian, by another vendor, or not at all. See our guidelines on plugin support.

- Adaptavist's Theme Builder Plugin for Confluence allows you to customise your Confluence site by adding layouts, logo banners, menu-driven navigation, style sheets, footers and more.

Related Topics

No content found for label(s) themes-configuration.

Administrators Guide Home Confluence Documentation Home

Applying a Theme to a Site

Themes allow you to personalise the 'look and feel' of Confluence. You can apply a theme to your entire Confluence site and to individual spaces. Choose a specific theme if you want to add new functionality or significantly alter the appearance of Confluence.

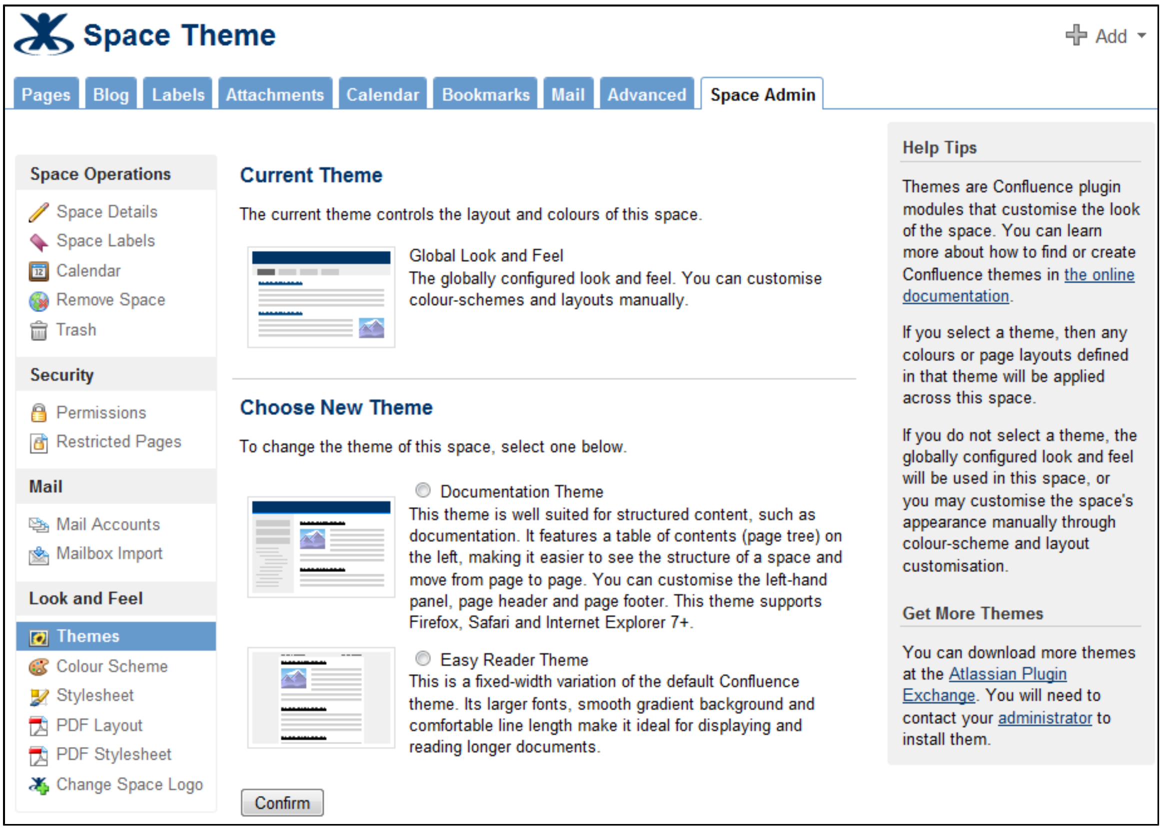
Confluence comes with a selection of themes. In addition, a site administrator can install new themes as plugins via the Confluence Administration Console. Provided that the theme is installed into your Confluence site, any space administrator can apply a theme to a space.

By default when you create a new space, the space will have the Confluence default theme.

To apply a theme across the site,

1. Ensure that the theme you wish to apply has been installed as a plugin.
2. Choose **Browse** > **Confluence Admin**.
3. Select '**Themes**' under '**Look and Feel**' in the left-hand panel.
4. The screen will display all available themes. Click a radio button to select a theme.
5. Click '**Confirm**'.

Screenshot : Applying a theme



Current Theme

The current theme controls the layout and colours of this space.

Global Look and Feel
The globally configured look and feel. You can customise colour-schemes and layouts manually.

Choose New Theme

To change the theme of this space, select one below.

○ Documentation Theme
This theme is well suited for structured content, such as documentation. It features a table of contents (page tree) on the left, making it easier to see the structure of a space and move from page to page. You can customise the left-hand panel, page header and page footer. This theme supports Firefox, Safari and Internet Explorer 7+.

○ Easy Reader Theme
This is a fixed-width variation of the default Confluence theme. Its larger fonts, smooth gradient background and comfortable line length make it ideal for displaying and reading longer documents.

Confirm

Help Tips

Themes are Confluence plugin modules that customise the look of the space. You can learn more about how to find or create Confluence themes in the online documentation.

If you select a theme, then any colours or page layouts defined in that theme will be applied across this space.

If you do not select a theme, the globally configured look and feel will be used in this space, or you may customise the space's appearance manually through colour-scheme and layout customisation.

Get More Themes

You can download more themes at the Atlassian Plugin Exchange. You will need to contact your administrator to install them.

RELATED TOPICS

No content found for label(s) themes-configuration.

Administrators Guide Home Confluence Documentation Home

Customising the Left Navigation Theme

The Left Navigation theme is no longer part of Confluence

This theme is no longer part of Confluence and is not supported from Confluence 3.4 onwards. We suggest the Documentation theme, as it provides a customisable left-hand navigation panel and additional configurable features. If you are using an earlier version of Confluence, please refer to the documentation for your version. For example, go to the documentation for Confluence 3.3.

Modifying Look and Feel (for themes)

Here's how you can define a new look and feel for Confluence in your theme:

1. **Layout** : Edit Confluence's layout by modifying the decorator files that are used to define it.
   - Working with Decorators
   - Velocity Template Overview

    - Configuring the atlassian.plugin.xml file to reference the decorators
2. **Colour schemes** : Configure a new colour scheme for your theme. **Optional**
    - Configuring a new colour scheme
    - Configuring the atlassian.plugin.xml file to include the new colour scheme
3. **Stylesheet** : Include a stylesheet to define your theme. **Optional**

ℹ Note that for every component you edit, you will need to configure the `atlassian-plugin.xml` which is the central configuration file for the plugin to override the default files with the new files you've created.

⚠ *The information on this page does not apply to Confluence OnDemand.*

Layout: Working with decorators

What are decorators?

Confluence is built on top of the Open Source SiteMesh library, a web-page layout system. To edit the layout of Confluence, you will need to modify these decorator files. A decorator file is a '.vmd' file and is written in a very simple programming language called **Velocity**. Learn more about Velocity.

Confluence comes bundled with a set of decorator or VMD files that you can customize. Broadly these are categorised into **Site**, **Content** and **Export** decorators. These are further grouped into categories called *contexts* and under each context has various *modes* (ways of viewing the context).

To make editing easier, layout for similar screens (example: view and edit page screens) is configured through the same VMD file. So, if you want to customize how the Confluence **View Page Screen** or **Edit Page Screen** lo oks, you can make **both** of these changes inside one decorator file: **page.vmd**.

Decorator	Context	Mode	Comment
page.vmd	page	'view', 'edit', 'edit-preview', 'view-information', and 'view-attachments'	
blogpost.vmd	blogpost (news)	'view', 'edit', 'edit-preview', and 'remove'	We prefer to use 'news' as an end-user term; all templates and classes use 'blogpost' to indicate RSS related content
mail.vmd	mail	'view', 'view-thread' and 'remove'	

space.vmd	space-pages, space-mails, space-blogposts, space-templates, space-operations, space-administration	CONTEXT: "space-pages". MODES: "list-alphabetically", "list-recently-updated", "list-content-tree", "create-page". CONTEXT: "space-mail". MODES: "view-mail-archive". CONTEXT: "space-blogposts". MODES: "view-blogposts", "create-blogpost". CONTEXT: "space-templates". MODES: "view-templates". CONTEXT: "space-operations". MODES: "view-space-operations". CONTEXT: "space-administration". MODES: "view-space-administration", "list-permission-pages".	space.vmd handles a wide range of options, this context is accessed by clicking on 'browse space' in the default theme of Confluence (tabbed theme)
global.vmd	global	'dashboard', 'view-profile', 'edit-profile', 'change-password-profile', 'edit-notifications-profile'	
main.vmd	n/a (header and footer formatting)		main.vmd is used to control the header and footer of each page, not the page specific presentation logic

For example, if you wanted to remove the 'Attachments' tab on the view page screen, you would make this layout change in the page.vmd file - where the 'view' mode is handled (as shown below).

```
#*
     Display page based on mode: currently
'view', 'edit', 'preview-edit', 'info' and
'attachments.
     See the individual page templates
(viewpage.vm, editpage.vm, etc.) for the
setting of the mode parameter.
   *#
   ## VIEW
   #if ($mode == "view")

       <make layout modifications here>

   #elseif ...
```

Step One: Copying the decorators

The easiest way to begin configuring a new layout is by copying the default decorator files and editing them to suit your theme.

1. Choose **Browse** > **Confluence Admin**.
2. Select **Layouts** in the left panel. This will display options to view and edit the default decorators.
3. Copy the files that you intend to modify and place them in a directory structure that makes sense to you. See example below.

Step Two: Creating a directory structure for the decorators:

You should place your decorators in a directory hierarchy which makes sense to you. We recommend that you place the atlassian-plugin.xml file at the top level of the directory structure, and then place the decorators in directories which make a meaningful division of what they do.

Here is an example:

```
atlassian-plugin.xml
com/atlassian/confluence/themes/mytheme/
com/atlassian/confluence/themes/mytheme/global.vmd
com/atlassian/confluence/themes/mytheme/space.vmd
com/atlassian/confluence/themes/mytheme/mail.vmd
com/atlassian/confluence/themes/mytheme/blogpost.vmd
com/atlassian/confluence/themes/mytheme/main.vmd
com/atlassian/confluence/themes/mytheme/page.vmd
```

Step Three: Editing the decorators

To edit the decorators, you will require knowledge of a very simple programming language called **Velocity**. Learn more about Velocity.

Decorator Macros

When editing the decorators, you will need to use **Decorator Macros** to draw complex or variable parts of the page such as menus and breadcrumbs. See Working With Decorator Macros

Theme Helper Object

When editing decorator files you will also come across a variable called **$helper** - this is the **theme helper object**.

The following table summarises what this object can do:

Behaviour	Explanation
$helper.domainName	displays the base URL of your Confluence instance on your page. This is useful for constructing links to your own Confluence pages.
$helper.spaceKey	returns the current space key or null if in a global context.

$helper.spaceName	returns the name of the current space
$helper.renderConfluenceMacro("{create-space-button}")	renders a call to a Confluence Macro for the velocity context
$helper.getText("key.key1")	looks up a key in a properties file matching `key.key1=A piece of text` and returns the matching value ("A piece of text")
$helper.action	returns the XWork action which processed the request for the current page.

If you are on a page or space screen you also have access to the actual page and space object by using `$helper.page` and `$helper.space` respectively.

If you want to deliver more into what other methods are available in this object, please see our API's for ThemeHelper.

Step Four: Configuring the central configuration file to reference the new decorators

How to do this is explained in Configuring the Theme Plugin

Working with colour schemes for themes

Configuring the colour scheme

The easiest way to configure a colour scheme is to do it dynamically from the **Administration Console** (as you would normally when you want to change the site's colour scheme online), and then express it as an xml file. This method makes it possible for you to experiment with different colours and test them out before including the colour scheme in your theme.

1. Choose **Browse** > **Confluence Admin**.
2. Select '**Colour scheme**' in the left panel.
3. Use the colour picker to define the colours for the following UI elements:

- **Top Bar** - the bar across the top of the page that contains the breadcrumbs.
- **Space Name Text** - the text of the current space name located above the page title.
- **Heading Text** - all heading tags throughout the space.
- **Links** - all links throughout the space.
- **Borders and Dividers** - table borders and dividing lines.
- **Menu Bar Background** - background of top navigational buttons
- **Menu Bar Text** - text that appears on the menu bar
- **Menu Bar Background Highlight** - background colour of menu bar when highlighted.
- **Menu Bar Text Highlight** - menu bar text when highlighted

More information on customising colour schemes

Expressing the colour scheme as XML

Once, you have decided on the colours for the different UI elements, you will need to configure the atlassian.plugin.xml to include the new colour scheme. How to do this is explained in detail in Configuring the Theme Plugin.

RELATED TOPICS

No content found for label(s) themes-configuration.

Administrators Guide Home Confluence Documentation Home

Configuring the Theme Plugin

Each plugin is described in its own `atlassian-plugin.xml` file, which specifies attributes of the plugin, including a description of each module it contains. Once you have modified the different components to define a new look and feel for your theme, you will need to configure this file so Confluence knows where to look when overriding the default files.

The easiest way to begin is by copying the `atlassian-plugin.xml` from one of the default themes bundled with Confluence and modifying it for your theme.

⚠ *The information on this page does not apply to Confluence OnDemand.*

The structure of an `atlassian-plugin.xml` file is fairly self-explanatory:

```
<atlassian-plugin key="com.atlassian.confluence.themes.tabless" name="Plain Theme">
   <plugin-info>
       <description>This theme demonstrates a plain look and feel for Confluence. It is useful as a building block for your own themes.</description>
       <version>1.0</version>
       <vendor name="Atlassian Software Systems Pty Ltd" url="http://www.atlassian.com/"/>
   </plugin-info>

    <theme key="tabless" name="Tabless Theme" class="com.atlassian.confluence.themes.Bas
```

```
icTheme">
        <description>plain Confluence
theme.</description>
        <layout
key="com.atlassian.confluence.themes.table
ss:main"/>
        <layout
key="com.atlassian.confluence.themes.table
ss:global"/>
        <layout
key="com.atlassian.confluence.themes.table
ss:space"/>
        <layout
key="com.atlassian.confluence.themes.table
ss:page"/>
        <layout
key="com.atlassian.confluence.themes.table
ss:blogpost"/>
        <layout
key="com.atlassian.confluence.themes.table
ss:mail"/>
        <colour-scheme
key="com.atlassian.confluence.themes.table
ss:earth-colours"/>
    </theme>

    <layout key="main" name="Main
Decorator"
class="com.atlassian.confluence.themes.Vel
ocityDecorator"

overrides="/decorators/main.vmd">
        <resource type="velocity"
```

```
name="decorator"

location="com/atlassian/confluence/themes/
tabless/main.vmd"/>
    </layout>

    <layout key="global" name="Global
Decorator"
class="com.atlassian.confluence.themes.Vel
ocityDecorator"

overrides="/decorators/global.vmd">
        <resource type="velocity"
name="decorator"

location="com/atlassian/confluence/themes/
tabless/global.vmd"/>
    </layout>

    <layout key="space" name="Space
Decorator"
class="com.atlassian.confluence.themes.Vel
ocityDecorator"

overrides="/decorators/space.vmd">
        <resource type="velocity"
name="decorator"

location="com/atlassian/confluence/themes/
tabless/space.vmd"/>
    </layout>

    <layout key="page" name="Page
```

```
Decorator"
class="com.atlassian.confluence.themes.Vel
ocityDecorator"

overrides="/decorators/page.vmd">
        <resource type="velocity"
name="decorator"

location="com/atlassian/confluence/themes/
tabless/page.vmd"/>
    </layout>

    <layout key="blogpost" name="Blogpost
Decorator"
class="com.atlassian.confluence.themes.Vel
ocityDecorator"

overrides="/decorators/blogpost.vmd">
        <resource type="velocity"
name="decorator"

location="com/atlassian/confluence/themes/
tabless/blogpost.vmd"/>
    </layout>

    <layout key="mail" name="Mail
Decorator"
class="com.atlassian.confluence.themes.Vel
ocityDecorator"

overrides="/decorators/mail.vmd">
        <resource type="velocity"
name="decorator"
```

```
location="com/atlassian/confluence/themes/
tabless/mail.vmd"/>
    </layout>


    <colour-scheme key="earth-colours"
name="Brown and Red Earth Colours"

class="com.atlassian.confluence.themes.Bas
eColourScheme">
         <colour key="topbar"
value="#440000"/>
         <colour key="spacename"
value="#999999"/>
         <colour key="headingtext"
value="#663300"/>
         <colour key="link"
value="#663300"/>
         <colour key="border"
value="#440000"/>
         <colour key="navbg"
value="#663300"/>
         <colour key="navtext"
value="#ffffff"/>
         <colour key="navselectedbg"
value="#440000"/>
         <colour key="navselectedtext"
value="#ffffff"/>
```

```
    </colour-scheme>

</atlassian-plugin>
```

Modifying the `atlassian-plugin.xml` file

We will configure this file section by section.

Plugin information

```
<atlassian-plugin key="com.atlassian.confluence.themes.tabless" name="Plain Theme">
   <plugin-info>
       <description>This theme demonstrates a plain look and feel for Confluence. It is useful as a building block for your own themes.</description>
       <version>1.0</version>
       <vendor name="Atlassian Software Systems Pty Ltd" url="http://www.atlassian.com/"/>
   </plugin-info>
```

plugin key : Specify a key that uniquely identifies the plugin, eg. com.example.themes.dinosaur

name : Give the plugin a name.

description : Provide a short description of the plugin.

vendor : Replace the text with your information.

Theme information

```
<theme key="dinosaurs" name="Dinosaur Theme"

class="com.atlassian.confluence.themes.BasicTheme">
    <description>A nice theme for the kids</description>
    <colour-scheme key="com.example.themes.dinosaur:earth-colours"/>
    <layout key="com.example.themes.dinosaur:main"/>
    <layout key="com.example.themes.dinosaur:mail-template"/>
</theme>
```

theme key : Specify a key that uniquely identifies the theme.

class : The class of a theme must implement `com.atlassian.confluence.themes.Theme`. The `com.atlassian.confluence.themes.BasicTheme` class provided with Confluence gathers together all the resources listed within the module definition into a theme.

name : Give the theme a name. Make sure that you replace all instances of the theme name with this name.

description : Provide a short description of your theme

colour-scheme key : A theme can contain an optional `colour-scheme` element that defines which colour-scheme module this theme will use. If you are using a new colour scheme, enter its key.

layout key : A theme can contain any number of `layout` elements that define which layouts should be applied in this theme. Refer to these modules by their **complete module key** as shown above.

Referencing the decorators

You will need to add a layout entity as shown below for each of the decorators you are using. See working with decorators

```
<layout key="page" name="Page Decorator"
class="com.atlassian.confluence.themes.Vel
ocityDecorator"

overrides="/decorators/page.vmd">
        <resource type="velocity"
name="decorator"

location="com/atlassian/confluence/themes/
tabless/page.vmd"/>
</layout>
```

class : The class which each decorator, or layout, is mapped to must implement `com.atlassian.confluence.themes.VelocityDecorator`.

overrides : The layout entry must provide an `overrides` attribute which defines which decorator within Confluence is being overrridden by the theme.

Location : Specify the location of the new decorator file, so Confluence know where to look when overriding the default decorator.

ℹ It is possible for a theme to use modules that aren't in the same plugin as the theme. Just keep in mind that your theme will be messed up if the plugin that the theme depends on is removed.

Including the colour scheme

Colour schemes can be pre-configured for your theme dynamically from the **Administration Console**. See configuring colour schemes

To transport them within a theme however, they need to be expressed in the `atlassian-plugin.xml` file as shown above.

```
<colour-scheme key="earth-colours"
name="Brown and Red Earth Colours"

class="com.atlassian.confluence.themes.BaseColourScheme">
     <colour key="topbar"
value="#440000"/>
     <colour key="spacename"
value="#999999"/>
     <colour key="headingtext"
value="#663300"/>
     <colour key="link" value="#663300"/>
     <colour key="border"
value="#440000"/>
     <colour key="navbg" value="#663300"/>
     <colour key="navtext"
value="#ffffff"/>
     <colour key="navselectedbg"
value="#440000"/>
     <colour key="navselectedtext"
value="#ffffff"/>
</colour-scheme>
```

colour-scheme key : Specify a key that uniquely identifies the colour scheme.

name : Give a name to the colour scheme.

class : The class of the colour scheme must implement `com.atlassian.confluence.themes.ColourScheme`. The `com.atlassian.confluence.themes.BaseColourScheme` class provided with Confluence sets the colours based on the module's configuration.

colour key: For each UI element, you will need to add its name and value.

See configuring colour scheme

RELATED TOPICS

No content found for label(s) themes-configuration.

Administrators Guide Home Confluence Documentation Home

Including Cascading Stylesheets in Themes

Confluence allows you to integrate your own stylesheets within the theme plugin so you can have greater control over the appearance of your site. Confluence's main stylesheet is a useful reference when overriding styles and can be found in the Confluence install directory under `...confluence/styles/site-css.vm`.

> ⚠ *The information on this page does not apply to Confluence OnDemand.*

Step One: Defining the stylesheet in the atlassian-plugin.xml

To make a stylesheet available to a decorator, you will need to reference it as a resource from within the central configuration file - `atlassian-plugin.xml`.

Here is an example where a stylesheet is being used to define the 'leftnavigation' theme:

```
<layout key="main" name="Main Decorator"
class="com.atlassian.confluence.themes.VelocityDecorator"
overrides="/decorators/main.vmd">
<resource type="velocity" name="decorator"
location="templates/leftnavigation/main.vmd"/>
<resource type="stylesheet"
name="leftnav.css"
location="templates/leftnavigation/leftnav-css.vm">
</resource>
</layout>
```

The resource parameter takes three arguments:

- **Type**: The type of resource-in this instance, 'stylesheet'.
- **Name**: The name of the stylesheet.
- **Location**: The location of the file represented in the jar archive you will use to bundle your theme.

Step Two: Using the stylesheet in the decorator

To reference the stylesheet in the decorator, you will need to use the #pluginStylesheet velocity macro.

For example, here's how you reference the leftnav.css file defined in the layout entry above:

```
#pluginStylesheet("com.atlassian.confluence.themes.leftnavigation:main" "leftnav.css")
```

The macro takes two arguments:

- **completePluginKey**: The complete plugin key which is constructed from the pluginkey and the layout key like this: {**pluginKey**}:{**layoutKey**}
  In the above example, `com.atlassian.confluence.themes.leftnavigation` is the key of the plugin, and `main` is the key of the layout.
- **stylesheetName**: the name of the stylesheet

If you place your stylesheet **after** the `#standardHeader` macro in the decorator, the contents of your custom stylesheet will override those in Confluence's default stylesheet.

If your stylesheet needs to reference the colour scheme, you need to use the space stylesheet macro instead:

```
#pluginSpaceStylesheet("com.atlassian.confluence.themes.leftnavigation:main" "leftnav.css" $spaceKey)
```

You can then use colour scheme references in your stylesheet, similar to Confluence's stylesheets, and they will be replaced with the appropriate global or space-specific colour scheme:

```
.navItemOver {
    color: $action.navSelectedTextColor;
}
```

RELATED TOPICS

No content found for label(s) themes-configuration.

Administrators Guide Home Confluence Documentation Home

Creating a Theme

Unsure what a theme is? See the overview of themes.

If you want to create your own theme, you will need to write a Confluence plugin. Please refer to the following pages:

- Get started with plugin development.
- Create a theme using the theme plugin module.

⚠ *The information on this page does not apply to Confluence OnDemand.*

RELATED TOPICS

No content found for label(s) themes-configuration.

Administrators Guide Home Confluence Documentation Home

Importing Data

- Importing Content from Another Wiki
- Universal Wiki Converter
- Importing Content Into Confluence

⚠ *The information on this page does not apply to Confluence OnDemand.*

Importing Content from Another Wiki

The Universal Wiki Converter (UWC) allows you to import content from other wikis into Confluence. The Confluence Administration Console offers a link to the Universal Wiki Converter documentation and download sites.

ℹ **You need to install and run the UWC separately from Confluence.**

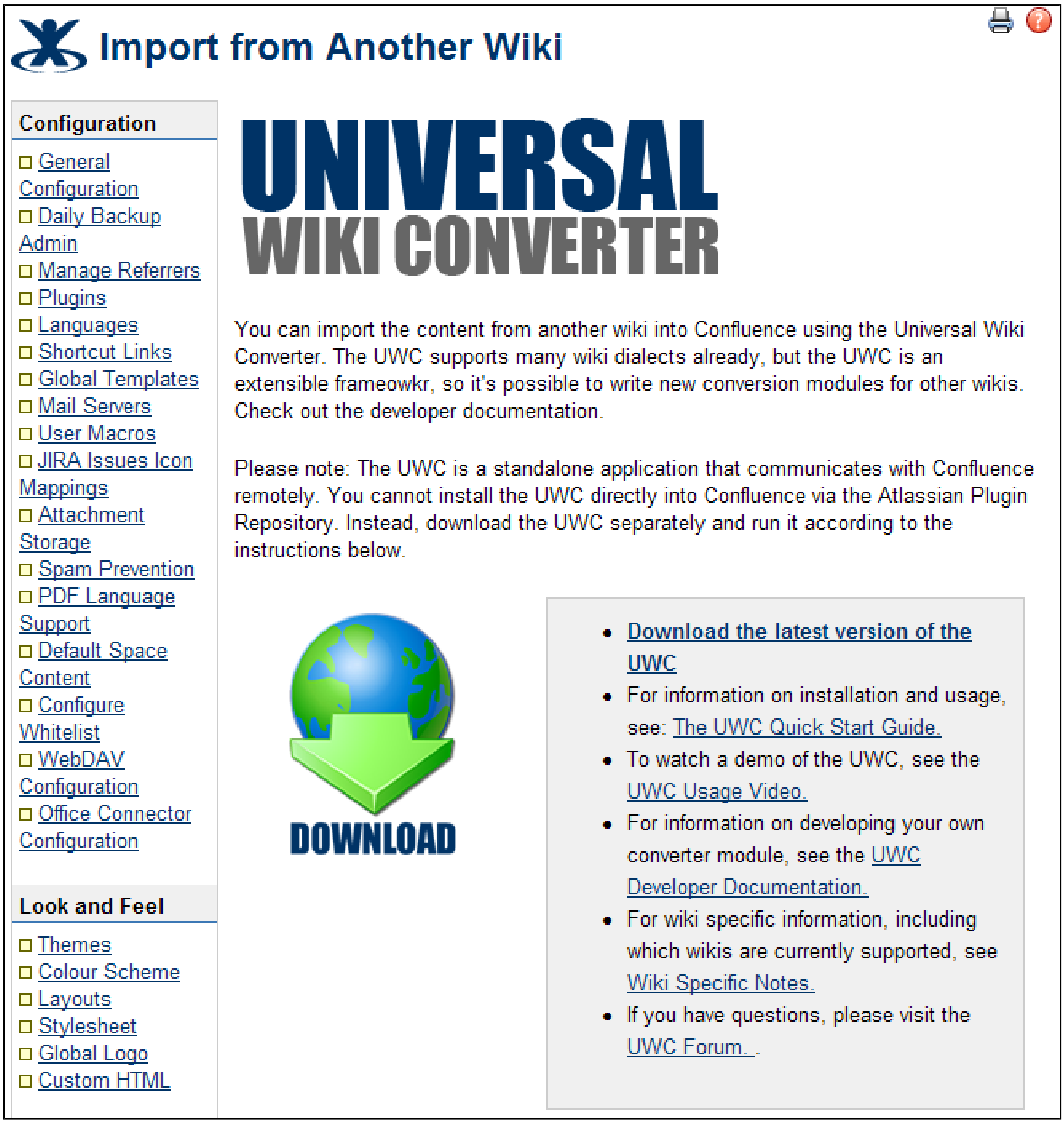
The UWC is a standalone application that communicates with Confluence remotely. You cannot install the UWC directly into Confluence. Instead, download the UWC separately and run it according to the instructions below.

⚠ *The information on this page does not apply to Confluence OnDemand.*

The UWC supports many wiki dialects. In addition, the UWC is an extensible framework, which means that developers can continue writing new conversion modules for other wikis. To see the latest list of conversions available, please refer to the UWC documentation.

- Download the latest version of the UWC.
- For information on installation and usage, see the UWC Quick Start Guide.
- For information on developing your own converter module, see the UWC Developer Documentation.
- For information about a specific wiki, including a list of currently supported wikis, see the UWC documentation.
- To ask a question, see the UWC discussions on Atlassian Answers.

Screenshot: Links from the Confluence Administration Console to the UWC



You can import the content from another wiki into Confluence using the Universal Wiki Converter. The UWC supports many wiki dialects already, but the UWC is an extensible frameowkr, so it's possible to write new conversion modules for other wikis. Check out the developer documentation.

Please note: The UWC is a standalone application that communicates with Confluence remotely. You cannot install the UWC directly into Confluence via the Atlassian Plugin Repository. Instead, download the UWC separately and run it according to the instructions below.

- **Download the latest version of the UWC**
- For information on installation and usage, see: The UWC Quick Start Guide.
- To watch a demo of the UWC, see the UWC Usage Video.
- For information on developing your own converter module, see the UWC Developer Documentation.
- For wiki specific information, including which wikis are currently supported, see Wiki Specific Notes.
- If you have questions, please visit the UWC Forum. .

RELATED TOPICS

- Importing Content Into Confluence
- Importing Data

Installing Plugins and Macros

A **plugin** is an add-on to the core Confluence code, which can extend the Confluence functionality. Some plugins are shipped with Confluence, others are available for you to install yourself.

A **macro** allows a developer to perform programmatic functions within a page, and gives the Confluence user access to more complex content structures. Many macros are made available by plugins.

You need System Administrator permissions in order to install and configure plugins.

Installing and configuring plugins and macros

- Installing and Configuring Plugins using the Universal Plugin Manager
  - Checking Plugin Compatibility for Confluence Upgrades
  - Configuring a Plugin
  - Disabling or Enabling a Plugin
  - Installing a Plugin

Installing and Configuring Plugins using the Universal Plugin Manager

This page provides information about the Universal Plugin Manager (UPM) in Confluence and links to topics on how to install and configure plugins using the UPM. You need System Administrator permissions in order to install and configure plugins.

A note about plugin safety: Plugins are very powerful: they can change the behaviour of almost any part of the Confluence server. It is **very important** that you trust a plugin before you install it. Always be aware of where (and who) a plugin comes from.

Overview of the Universal Plugin Manager

The Universal Plugin Manager (UPM) provides a set of functions for managing your plugins. The UPM is itself a system plugin. It allows you to perform common tasks such as:

- Enabling and disabling plugins and their plugin modules.
- Installing new plugins.
- Configuring advanced plugin options.
- Finding out-of-date plugins and updating them.
- Checking the compatibility of your installed plugins against newer versions of the application.

Through the UPM you can interact with the Atlassian Plugin Exchange. You can use the UPM to browse available plugins for your application, and try or buy any of these plugins without ever leaving your application.

Related pages:

- Confluence Plugin Guide for Developers
- Adding, Editing and Removing User Macros

⚠ *Some functionality described on this page is restricted in* ***Confluence OnDemand****.*

Managing your plugins

- Checking Plugin Compatibility for Confluence Upgrades
- Configuring a Plugin
- Disabling or Enabling a Plugin

- Installing a Plugin
- Uninstalling a Plugin
- Upgrading your Existing Plugins
- Viewing the Plugin Audit Log
- Viewing your Installed Plugins

Notes

Having problems with the Universal Plugin Manager? Try the Universal Plugin Manager FAQ. (This will redirect you to the Universal Plugin Manager documentation. Use the back button on your browser to return the Confluence documentation.)

Checking Plugin Compatibility for Confluence Upgrades

The **Application Upgrade Check** in the Universal Plugin Manager (UPM) helps you to check whether your plugins will still work with Confluence after a Confluence upgrade.

For example, if you were thinking of upgrading from Confluence 4.1 to Confluence 4.2, the Application Upgrade Check can tell you the following:

- Installed plugins that are compatible with Confluence 4.1 and Confluence 4.2.
- Installed plugins that are not compatible with Confluence 4.2, but will be compatible with Confluence 4.2 if you upgrade them.
- Installed plugins that are not compatible with Confluence 4.2, even if you upgrade them to their latest version.

> ⚠ *The information on this page does not apply to Confluence OnDemand.*

To access the Universal Plugin Manager in Confluence:

1. Choose **Browse** > **Confluence Admin**.
2. Click the **Plugins** link in the **Configuration** section of the left-hand menu. The Universal Plugin Manager will appear.

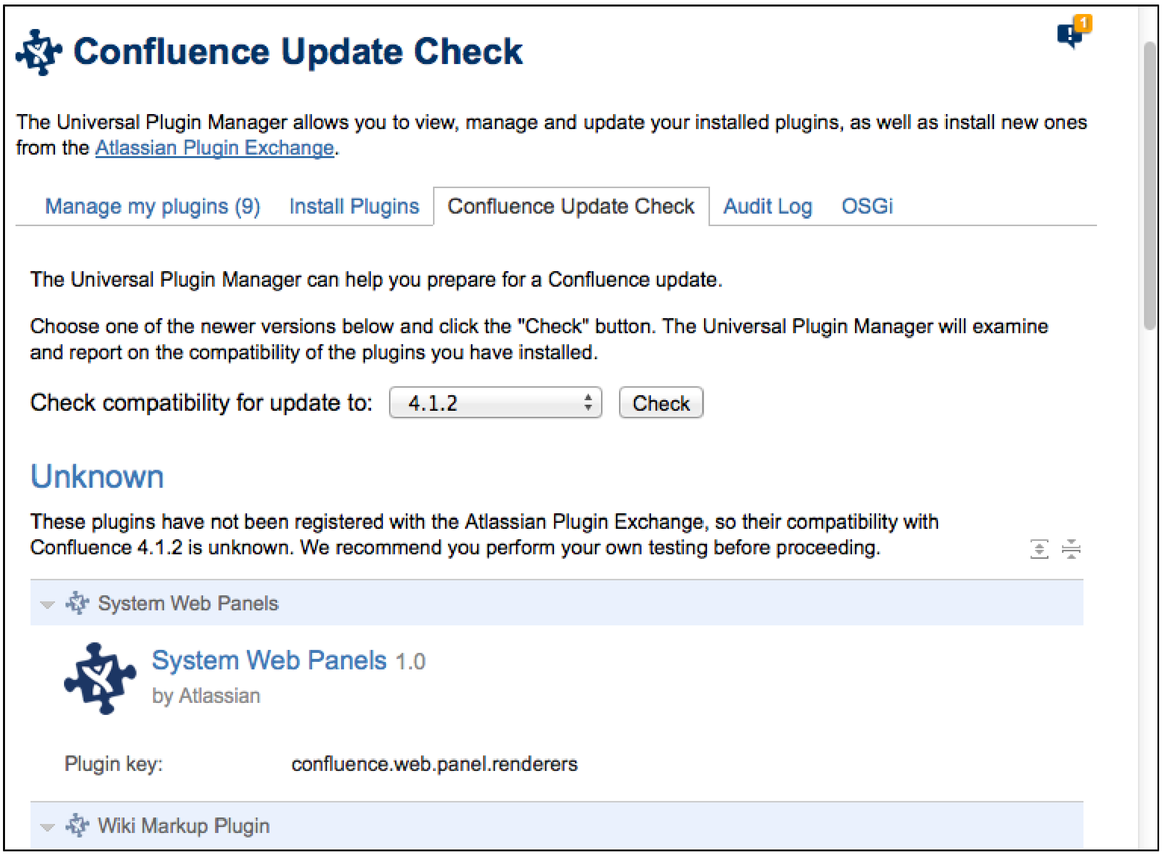
To check compatibility of your plugins against different Confluence versions:

1. Click the **Upgrade Check** tab.
2. In the **Check compatibility for** dropdown menu, select the version of your application to check the plugins against.
3. Click the **Check** button.
4. The page display any of your installed plugins that are not compatible with the selected application version. The compatibility checker will also check the compatibility of the latest available version of each plugin (if not already upgraded). You can click on the name of any of the plugins to view more information about the plugin.

   The plugins are grouped into sections under the following headings:
   - **Incompatible** – The installed versions of these plugins are not compatible with the selected application version. There are currently no plugin upgrades available that are compatible with the selected application version.
   - **Compatible, if upgraded** – The installed versions of these plugins are not compatible with the selected application version. However, the plugins will be compatible if you upgrade them. There are buttons allowing you to upgrade these plugins.
   - **Compatible if both <the application> and the plugin are upgraded** – The installed versions of these plugins are not compatible with the selected application version. There is a plugin compatible

with the newer application version, but it is not compatible with the application version you are currently running. You must upgrade the application and *then* upgrade the plugin. There are buttons allowing you to disable these plugins before proceeding with the upgrade.
- **Compatible** – The currently installed versions of these plugins are compatible with the selected application version.
- **Unknown** – These plugins may or may not be compatible with the selected application version. If a plugin is not registered with the Atlassian Plugin Exchange, the Universal Plugin Manager cannot check its compatibility with different application versions.

Screenshot: Checking plugin compatibility against different Confluence versions



Confluence Update Check

The Universal Plugin Manager allows you to view, manage and update your installed plugins, as well as install new ones from the Atlassian Plugin Exchange.

The Universal Plugin Manager can help you prepare for a Confluence update.

Choose one of the newer versions below and click the "Check" button. The Universal Plugin Manager will examine and report on the compatibility of the plugins you have installed.

Check compatibility for update to: 4.1.2 Check

Unknown

These plugins have not been registered with the Atlassian Plugin Exchange, so their compatibility with Confluence 4.1.2 is unknown. We recommend you perform your own testing before proceeding.

System Web Panels

System Web Panels 1.0
by Atlassian

Plugin key: confluence.web.panel.renderers

Wiki Markup Plugin

Configuring a Plugin

A number of Confluence plugins have advanced configuration options. If you have one of these plugins installed on your Confluence site, you can view and update these configuration options via the Universal Plugin Manager (UPM).

If you would like to disable or enable a plugin, please refer to **Disabling or Enabling a Plugin**.

To access the Universal Plugin Manager in Confluence:

1. Choose **Browse** > **Confluence Admin**.
2. Click the **Plugins** link in the **Configuration** section of the left-hand menu. The Universal Plugin Manager will appear.

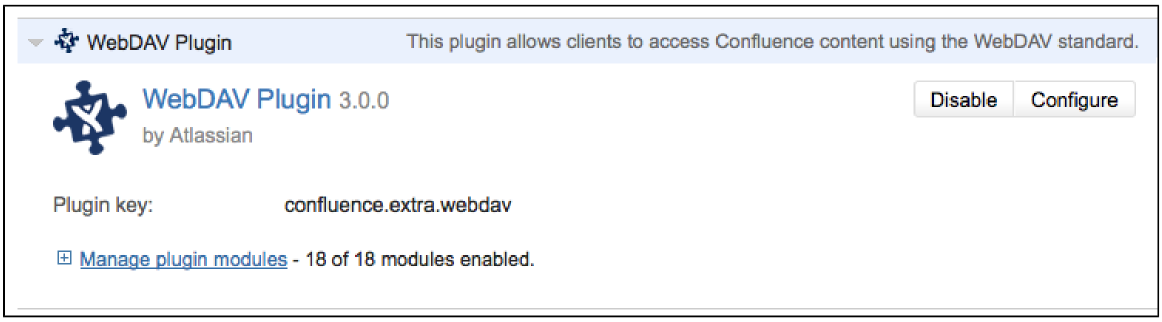
To configure a plugin in Confluence:

1. Click the **Manage Existing** tab.
2. Locate the plugin that you want to configure and click its title.
   The plugin details section expands.
3. Click the **Configure** button for that plugin.
   The advanced configuration options appear.

> ⚠ If the plugin is disabled, you cannot configure it and so the Configure **button** does not appear. If there are no advanced configuration options for the plugin, there is no **Configure** button.

4. Update the configuration settings as desired and save your changes.
   Note: The plugin itself provides advanced configuration options. If you encounter any problems after you click the **Configure** button, the plugin is responsible for the issue, not the UPM.

Screenshot: Configuring a plugin



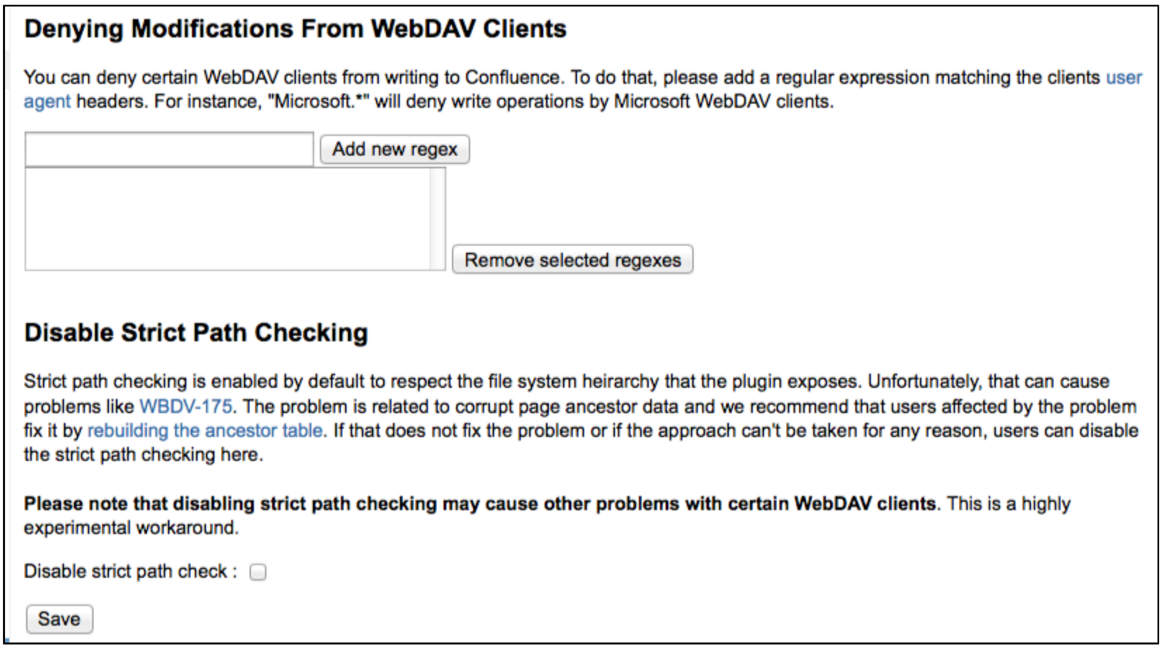
WebDAV Plugin — This plugin allows clients to access Confluence content using the WebDAV standard.

WebDAV Plugin 3.0.0
by Atlassian

Plugin key: confluence.extra.webdav

⊞ Manage plugin modules - 18 of 18 modules enabled.

Screenshot: Example of plugin configuration options – WebDAV configuration



Denying Modifications From WebDAV Clients

You can deny certain WebDAV clients from writing to Confluence. To do that, please add a regular expression matching the clients user agent headers. For instance, "Microsoft.*" will deny write operations by Microsoft WebDAV clients.

Disable Strict Path Checking

Strict path checking is enabled by default to respect the file system heirarchy that the plugin exposes. Unfortunately, that can cause problems like WBDV-175. The problem is related to corrupt page ancestor data and we recommend that users affected by the problem fix it by rebuilding the ancestor table. If that does not fix the problem or if the approach can't be taken for any reason, users can disable the strict path checking here.

Please note that disabling strict path checking may cause other problems with certain WebDAV clients. This is a highly experimental workaround.

Disable strict path check : □

Disabling or Enabling a Plugin

The **Universal Plugin Manager (UPM)** allows you to disable a plugin on your Confluence site without permanently removing the plugin. You can also enable any plugins that have been previously disabled. If you want to add or remove a plugin from your Confluence site, please refer to Installing a Plugin or Uninstalling a Plugin respectively.

You can also disable all user installed plugins in your application, by enabling **safe mode**. This may help you to diagnose a plugin-related problem more easily.

On this page:

Disabling a plugin

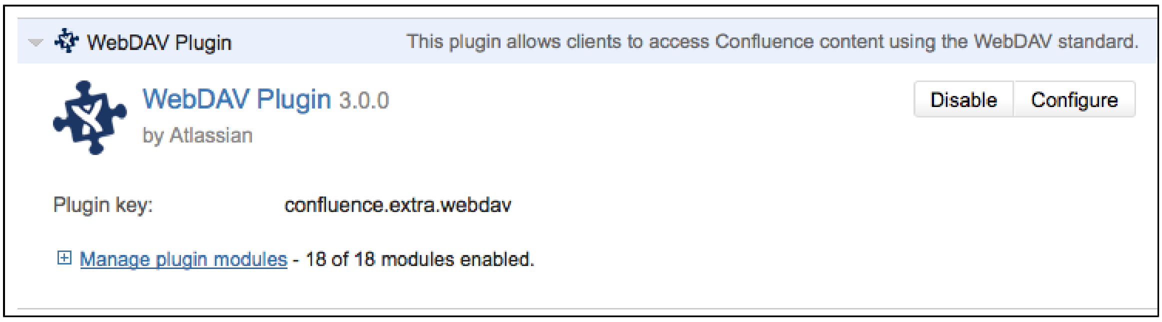
To access the Universal Plugin Manager in Confluence:

1. Choose **Browse** > **Confluence Admin**.
2. Click the **Plugins** link in the **Configuration** section of the left-hand menu. The Universal Plugin Manager will appear.

To disable a plugin:

1. Click the **Manage Existing** tab. You will see a list of the plugins installed in your application. Enabled plugins will have this icon:
2. Locate the plugin that you want to disable and click the title to expand the plugin details section.
3. Click the **Disable** button.
4. Once a plugin has been disabled, you *may* need to restart your application for your change to take effect. If so, you will see a message for the plugin, **Disabled, requires restart**.
   Once the plugin is fully disabled, you will see an **Enable** link for the plugin.

Screenshot: Disabling a plugin



This plugin allows clients to access Confluence content using the WebDAV standard.

Plugin key: confluence.extra.webdav

Manage plugin modules - 18 of 18 modules enabled.

Enabling a plugin

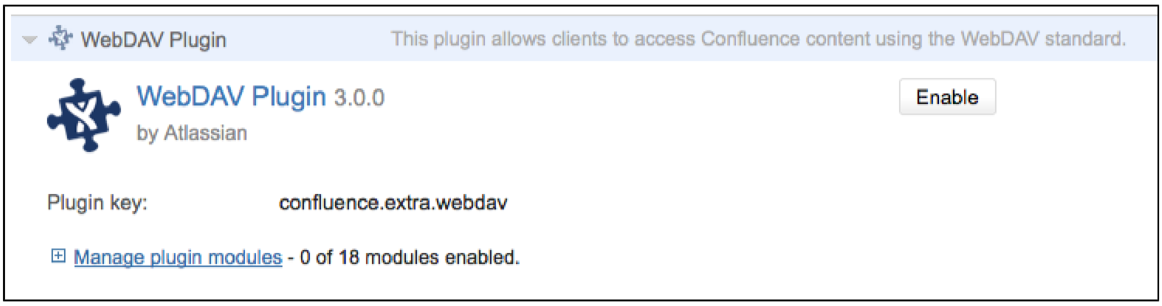
To access the Universal Plugin Manager in Confluence:

1. Choose **Browse** > **Confluence Admin**.
2. Click the **Plugins** link in the **Configuration** section of the left-hand menu. The Universal Plugin Manager will appear.

To enable a plugin:

1. Click the **Manage Existing** tab. You will see a list of the plugins installed in your application. Disabled plugins will have this icon:
2. Locate the plugin that you want to enable and click the title to expand the plugin details section.
3. Click the **Enable** button.
4. Once a plugin has been enabled, you *may* need to restart your application for your change to take effect. If so, you will see a message for the plugin, **Enabled, requires restart**.
   Once the plugin is fully disabled, you will see a **Disable** link for the plugin.

Screenshot: Enabling a plugin



This plugin allows clients to access Confluence content using the WebDAV standard.

Plugin key: confluence.extra.webdav

Manage plugin modules - 0 of 18 modules enabled.

Disabling/Enabling all user-installed plugins (safe mode)

Running your application in safe mode disables all user installed plugins at once. All plugins that were disabled when you entered safe mode will be re-enabled when you exit safe mode.

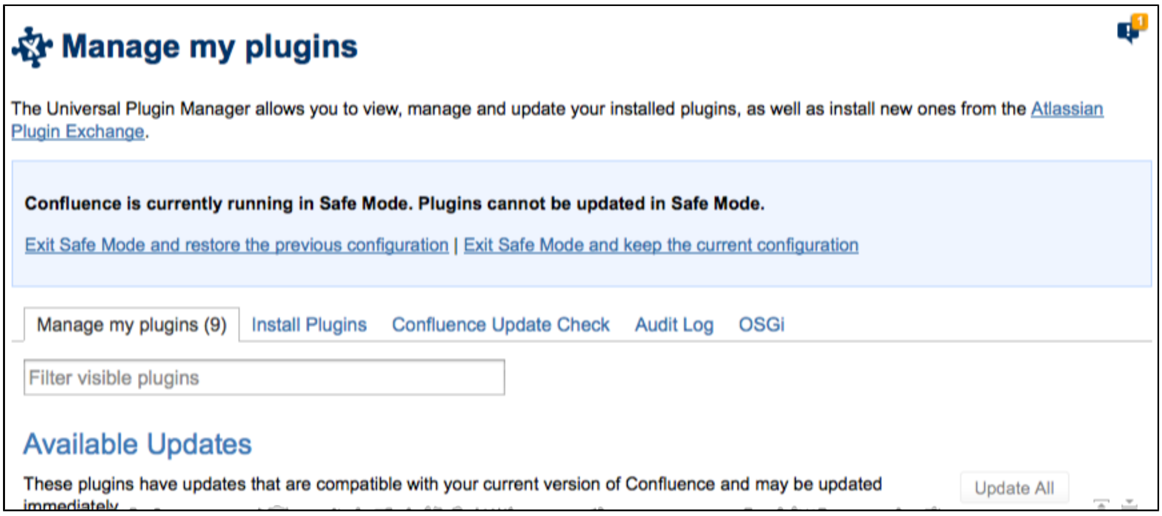
To access the Universal Plugin Manager in Confluence:

1. Choose **Browse** > **Confluence Admin**.
2. Click the **Plugins** link in the **Configuration** section of the left-hand menu. The Universal Plugin Manager will appear.

To enable safe mode:

1. Click the **Manage Existing** tab.
   The system displays a list the installed plugins.
2. Click the **Enable Safe Mode** link.
3. Click the **Continue** button in the confirmation window.
   All user installed plugins will be disabled and your application will now be running in safe mode.
4. Make changes to your installed plugins as desired.
   For example, you may want to enable/disable specific plugins or plugin modules.
5. Exit safe mode by clicking one of the links in the Safe Mode banner:
   - Click **Exit Safe Mode and restore the previous configuration** to restore your plugin configuration to its state before you entered Safe Mode.
   - Click **Exit Safe Mode and keep the current configuration** to keep all changes made to your plugin configuration during Safe Mode.

Screenshot: Running Confluence in safe mode



Manage my plugins

The Universal Plugin Manager allows you to view, manage and update your installed plugins, as well as install new ones from the Atlassian Plugin Exchange.

Confluence is currently running in Safe Mode. Plugins cannot be updated in Safe Mode.

Exit Safe Mode and restore the previous configuration | Exit Safe Mode and keep the current configuration

Available Updates

These plugins have updates that are compatible with your current version of Confluence and may be updated immediately.

Installing a Plugin

This page describes how to install a plugin into Confluence using the Universal Plugin Manager (UPM). Plugins can be used to customise and extend the functionality available in Confluence.

You can search for plugins in the UPM, or upload your own. The UPM searches the plugins in the Atlassian Plugin Exchange.

On this page:

The information on this page does not apply to Confluence OnDemand.

Adding a plugin from the Atlassian Plugin Exchange

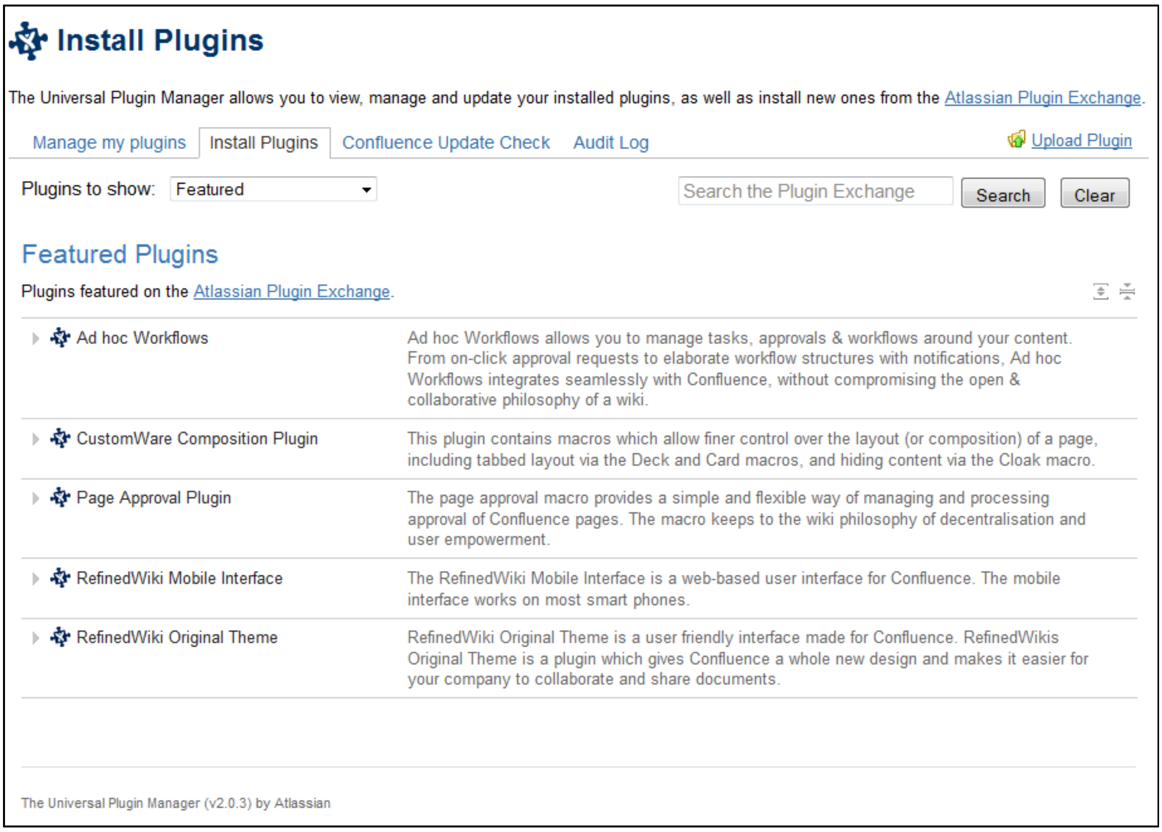
To access the Universal Plugin Manager in Confluence:

1. Choose **Browse** > **Confluence Admin**.
2. Click the **Plugins** link in the **Configuration** section of the left-hand menu. The Universal Plugin Manager will appear.

To find and add a plugin from the Atlassian Plugin Exchange:

1. Click the **Install** tab in the UPM. You will see a list of featured plugins.
2. Search for your plugin as follows:
    - Enter some keywords that describe the plugin in the **Search the Plugin Exchange** search box and press Enter.
    - Alternatively, browse to the desired plugin in the list. You can choose **Featured**, **Popular**, **Supported** *(by Atlassian)* or **All available** from the **Plugins to show** dropdown to see a different list of plugins.
3. Click the **Install** button for the desired plugin to add it to your application. A confirmation message and the plugin details will appear when the plugin is installed successfully.
   Note: You may need to restart your application for your change to take effect. The Universal Plugin Manager will inform you if this is the case.
   Note: Not all plugins can be automatically installed. Some required manual installation. These plugins will have a **Download** button instead of an **Install** button. In these cases, you should read and follow the plugin's installation instructions.

Screenshot: Finding a new plugin from the Atlassian Plugin Exchange



Install Plugins

The Universal Plugin Manager allows you to view, manage and update your installed plugins, as well as install new ones from the Atlassian Plugin Exchange.

Plugins to show: Featured

Search the Plugin Exchange

Featured Plugins

Plugins featured on the Atlassian Plugin Exchange.

Ad hoc Workflows	Ad hoc Workflows allows you to manage tasks, approvals & workflows around your content. From on-click approval requests to elaborate workflow structures with notifications, Ad hoc Workflows integrates seamlessly with Confluence, without compromising the open & collaborative philosophy of a wiki.
CustomWare Composition Plugin	This plugin contains macros which allow finer control over the layout (or composition) of a page, including tabbed layout via the Deck and Card macros, and hiding content via the Cloak macro.
Page Approval Plugin	The page approval macro provides a simple and flexible way of managing and processing approval of Confluence pages. The macro keeps to the wiki philosophy of decentralisation and user empowerment.
RefinedWiki Mobile Interface	The RefinedWiki Mobile Interface is a web-based user interface for Confluence. The mobile interface works on most smart phones.
RefinedWiki Original Theme	RefinedWiki Original Theme is a user friendly interface made for Confluence. RefinedWikis Original Theme is a plugin which gives Confluence a whole new design and makes it easier for your company to collaborate and share documents.

The Universal Plugin Manager (v2.0.3) by Atlassian

Uploading your own plugin

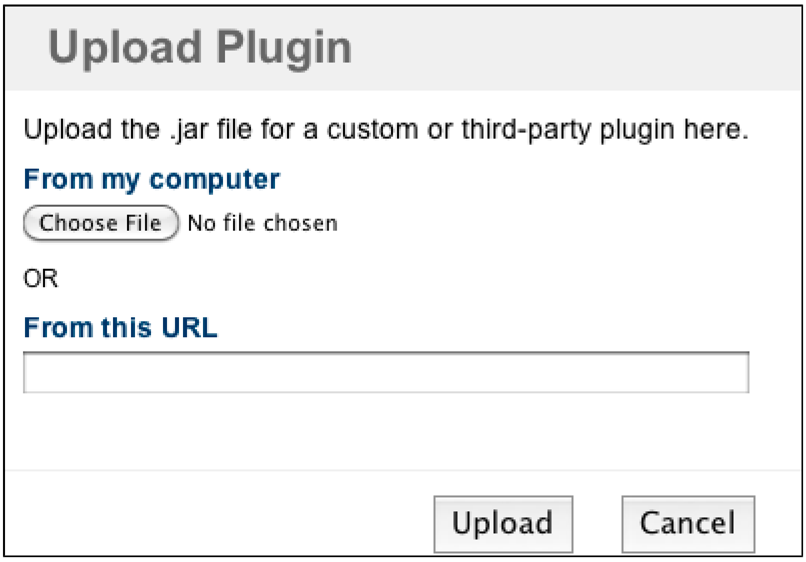
To access the Universal Plugin Manager in Confluence:

1. Choose **Browse** > **Confluence Admin**.
2. Click the **Plugins** link in the **Configuration** section of the left-hand menu. The Universal Plugin Manager will appear.

To upload your own plugin to Confluence:

1. Click the **Install** tab in the UPM.
   The system displays a list of featured plugins.
2. Click the **Upload Plugin** link.
   The system displays the **Upload Plugin** window.
3. Specify the location of your plugin:
   - If the plugin you want to install is on your computer, use the **Browse** dialogue to choose the plugin JAR file.
   - If you want to install a plugin from a remote location, enter the URL of the plugin JAR file in the **Fro m this URL** text box.
4. Click the **Upload** button to upload and enable your plugin. A confirmation message will appear when the plugin is successfully installed.
   Note: You may need to restart your application for your change to take effect. The Universal Plugin Manager will inform you if this is the case.

Screenshot: Uploading a new plugin



Upload Plugin

Upload the .jar file for a custom or third-party plugin here.

From my computer

From this URL

Notes

- In **Confluence**, you can install and uninstall both version 1 and version 2 plugins using the Universal Plugin Manager.
- Some entries that you find listed in the Universal Plugin Manager **are not actually plugins**. These entries will show a 'Download' button which allows you to download the application to your desktop and run it following the instructions given by that application.

Uninstalling a Plugin

If you wish to remove a plugin from Confluence altogether, you can uninstall it via the Universal Plugin Manager (UPM). If you only want to temporarily remove it, you may wish to disable your plugin instead.

To access the Universal Plugin Manager in Confluence:

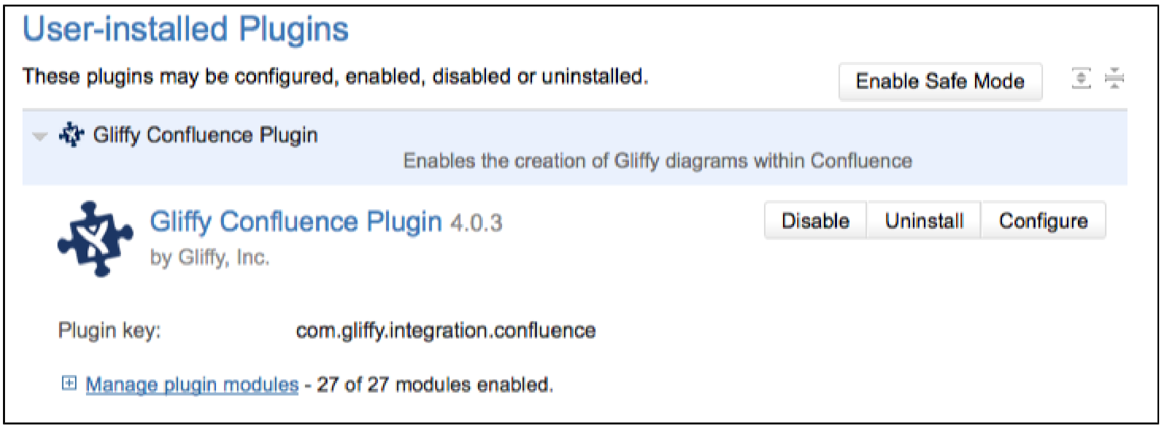
1. Choose **Browse** > **Confluence Admin**.
2. Click the **Plugins** link in the **Configuration** section of the left-hand menu. The Universal Plugin Manager will appear.

To uninstall a plugin from Confluence:

1. Click the **Manage Existing** tab.
   The systems lists the plugins installed in your application.
2. Click the name of the plugin that you wish to uninstall.
   The system displays the plugin details.
3. Click the **Uninstall** button.
   The information summary displays an **Uninstalling** message and uninstalls the plugin from your application.

> ⚠ *The information on this page does not apply to Confluence OnDemand.*

Screenshot: Uninstalling a plugin



User-installed Plugins

These plugins may be configured, enabled, disabled or uninstalled.

Gliffy Confluence Plugin

Enables the creation of Gliffy diagrams within Confluence

Gliffy Confluence Plugin 4.0.3

by Gliffy, Inc.

Plugin key: com.gliffy.integration.confluence

⊞ Manage plugin modules - 27 of 27 modules enabled.

Upgrading your Existing Plugins

Plugins are often developed separately from Confluence. You may wish to upgrade your plugins to more recent versions to allow them to work with your Confluence version or simply to take advantage of new features in a plugin version. The Universal Plugin Manager (UPM) provides you with a list of plugins that have available upgrades and allows you to upgrade each plugin individually or in bulk.

Tip: If you are considering upgrading Confluence, you can use the Universal Plugin Manager to check the compatibility of your plugins with your desired Confluence version. See Checking Plugin Compatibility for Confluence Upgrades.

On this page:

> ⚠ *The information on this page does not apply to Confluence OnDemand.*

Upgrading a plugin

To access the Universal Plugin Manager in Confluence:

1. Choose **Browse** > **Confluence Admin**.
2. Click the **Plugins** link in the **Configuration** section of the left-hand menu. The Universal Plugin Manager will appear.

To upgrade a plugin in Confluence:

1. Click the **Manage my plugins** tab. You will see a list of plugins that are available for upgrading, under the heading 'Available Updates'.
   - If there is a later version of a plugin that you have already installed, this page will show the latest **c**

ompatible version of the plugin.
   - You can click the plugin name to expand the row and see more information about the plugin.
   - You can filter your list by entering keywords in the **Filter visible plugins** text box.
2. Click the name of the plugin that you want to upgrade, to see more information about the plugin.
3. Click the **Update** button next to the plugin to update it to the version shown.

Upgrading all plugins

To access the Universal Plugin Manager in Confluence:

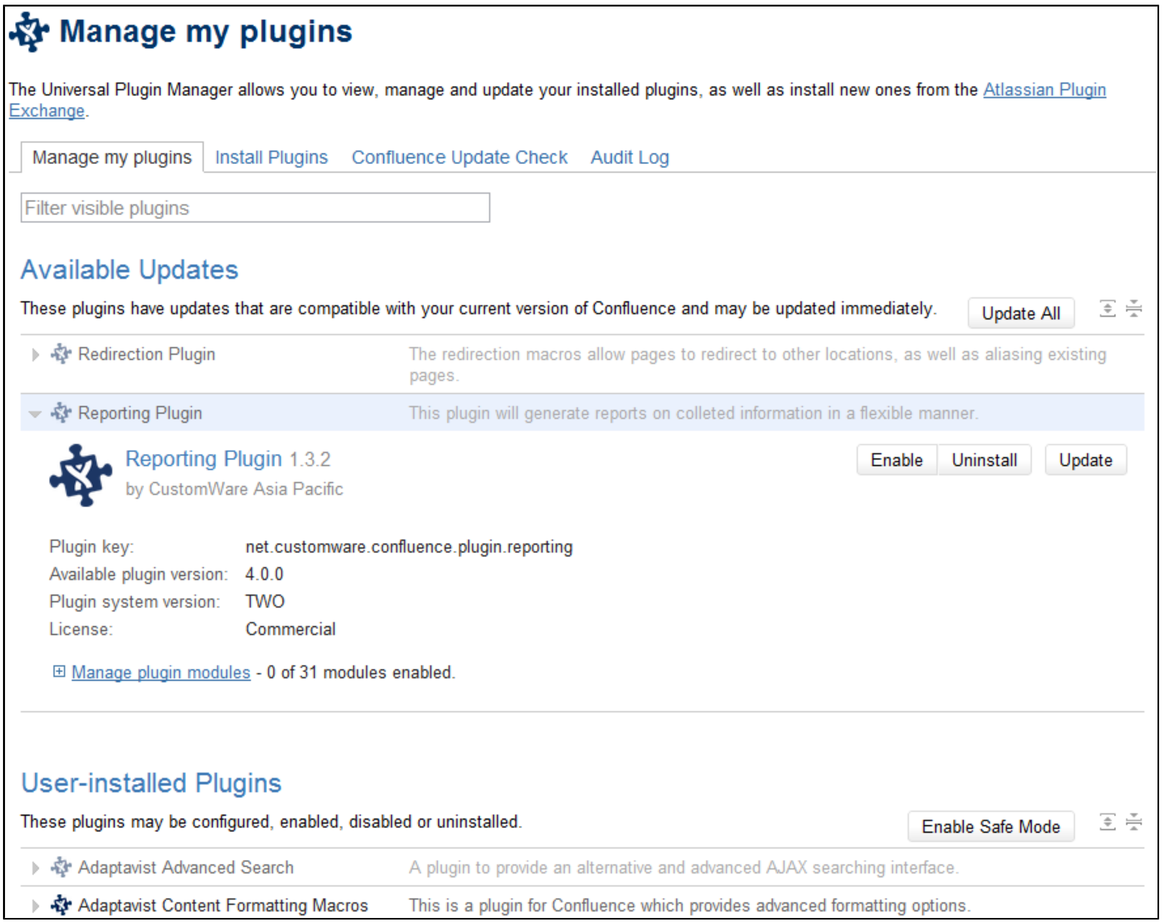
1. Choose **Browse** > **Confluence Admin**.
2. Click the **Plugins** link in the **Configuration** section of the left-hand menu. The Universal Plugin Manager will appear.

To upgrade all available plugins in Confluence:

1. Click the **Manage my plugins** tab. You will see a list of plugins that are available for upgrading, under the heading 'Available Updates'.
   - If there is a later version of a plugin that you have already installed, this page will show the latest **c ompatible** version of the plugin.
   - You can click the plugin name to expand the row and see more information about the plugin.
   - You can filter your list by entering keywords in the **Filter visible plugins** text box.
2. Click the **Update All** button to upgrade every plugin to the plugin versions shown.

   Note: Not all plugins can be installed or upgraded via the Universal Plugin Manager. There are some plugins that you must manually install and upgrade.

Screenshot: Upgrading plugins



Manage my plugins

The Universal Plugin Manager allows you to view, manage and update your installed plugins, as well as install new ones from the Atlassian Plugin Exchange.

Available Updates

These plugins have updates that are compatible with your current version of Confluence and may be updated immediately.

Redirection Plugin — The redirection macros allow pages to redirect to other locations, as well as aliasing existing pages.

Reporting Plugin — This plugin will generate reports on colleted information in a flexible manner.

Reporting Plugin 1.3.2
by CustomWare Asia Pacific

Plugin key: net.customware.confluence.plugin.reporting
Available plugin version: 4.0.0
Plugin system version: TWO
License: Commercial

Manage plugin modules - 0 of 31 modules enabled.

User-installed Plugins

These plugins may be configured, enabled, disabled or uninstalled.

Adaptavist Advanced Search — A plugin to provide an alternative and advanced AJAX searching interface.

Adaptavist Content Formatting Macros — This is a plugin for Confluence which provides advanced formatting options.

Viewing the Plugin Audit Log

The Universal Plugin Manager (UPM) keeps a log of all plugin activity in your Confluence instance. For example, adding plugins, and enabling plugins. You can configure the audit log to adjust the period of time for which log entries should be kept.

Viewing the plugin audit log

To access the Universal Plugin Manager in Confluence:

1. Choose **Browse** > **Confluence Admin**.
2. Click the **Plugins** link in the **Configuration** section of the left-hand menu. The Universal Plugin Manager will appear.

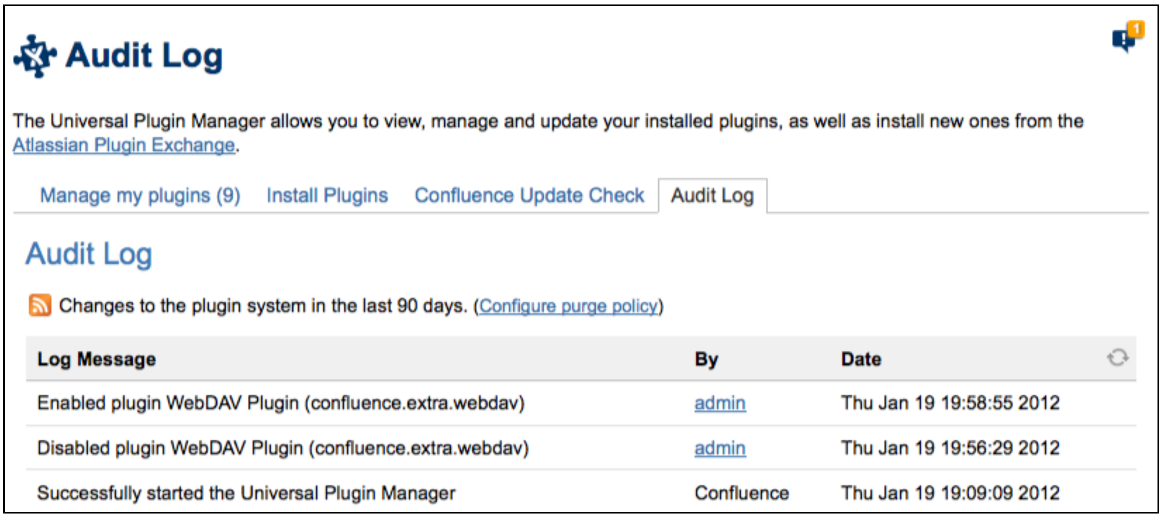
To view the plugin audit log:

1. Click the **Audit Log** tab.
   The plugin audit log appears with a list of the 25 most recent entries.
2. Use the arrows if you want to view older entries.
3. Click the orange RSS icon if you want to receive the audit log activity in an RSS feed.

On this page:

- Viewing the plugin audit log
- Configuring the plugin audit log

Screenshot: Viewing the plugin audit log



Audit Log

The Universal Plugin Manager allows you to view, manage and update your installed plugins, as well as install new ones from the Atlassian Plugin Exchange.

Audit Log

Changes to the plugin system in the last 90 days. (Configure purge policy)

Log Message	By	Date
Enabled plugin WebDAV Plugin (confluence.extra.webdav)	admin	Thu Jan 19 19:58:55 2012
Disabled plugin WebDAV Plugin (confluence.extra.webdav)	admin	Thu Jan 19 19:56:29 2012
Successfully started the Universal Plugin Manager	Confluence	Thu Jan 19 19:09:09 2012

Configuring the plugin audit log

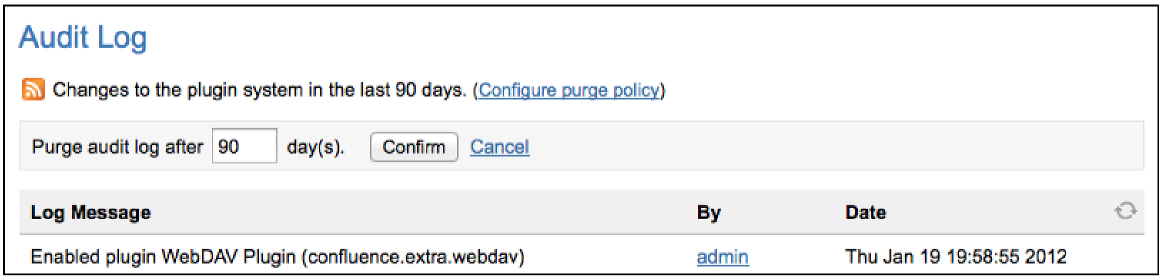
To access the Universal Plugin Manager in Confluence:

1. Choose **Browse** > **Confluence Admin**.
2. Click the **Plugins** link in the **Configuration** section of the left-hand menu. The Universal Plugin Manager will appear.

To configure the amount of time log entries are kept:

1. Click the **Audit Log** tab.
   The plugin audit log appears.
2. Click the **Configure purge policy** link.
3. Specify how many days to keep the logs before purging in the **Purge audit log after** field.
4. Click the **Confirm** button.

Screenshot: Configuring the audit log's purge policy



Audit Log

Changes to the plugin system in the last 90 days. (Configure purge policy)

Purge audit log after 90 day(s). Confirm Cancel

Log Message	By	Date
Enabled plugin WebDAV Plugin (confluence.extra.webdav)	admin	Thu Jan 19 19:58:55 2012

Viewing your Installed Plugins

The **Universal Plugin Manager (UPM)** allows you to easily view the plugins installed on your Confluence instance. This includes plugins that are bundled with Confluence as well as any third party plugins that you have installed. Both enabled and disabled plugins are displayed.

On this page:

Viewing your Installed Plugins

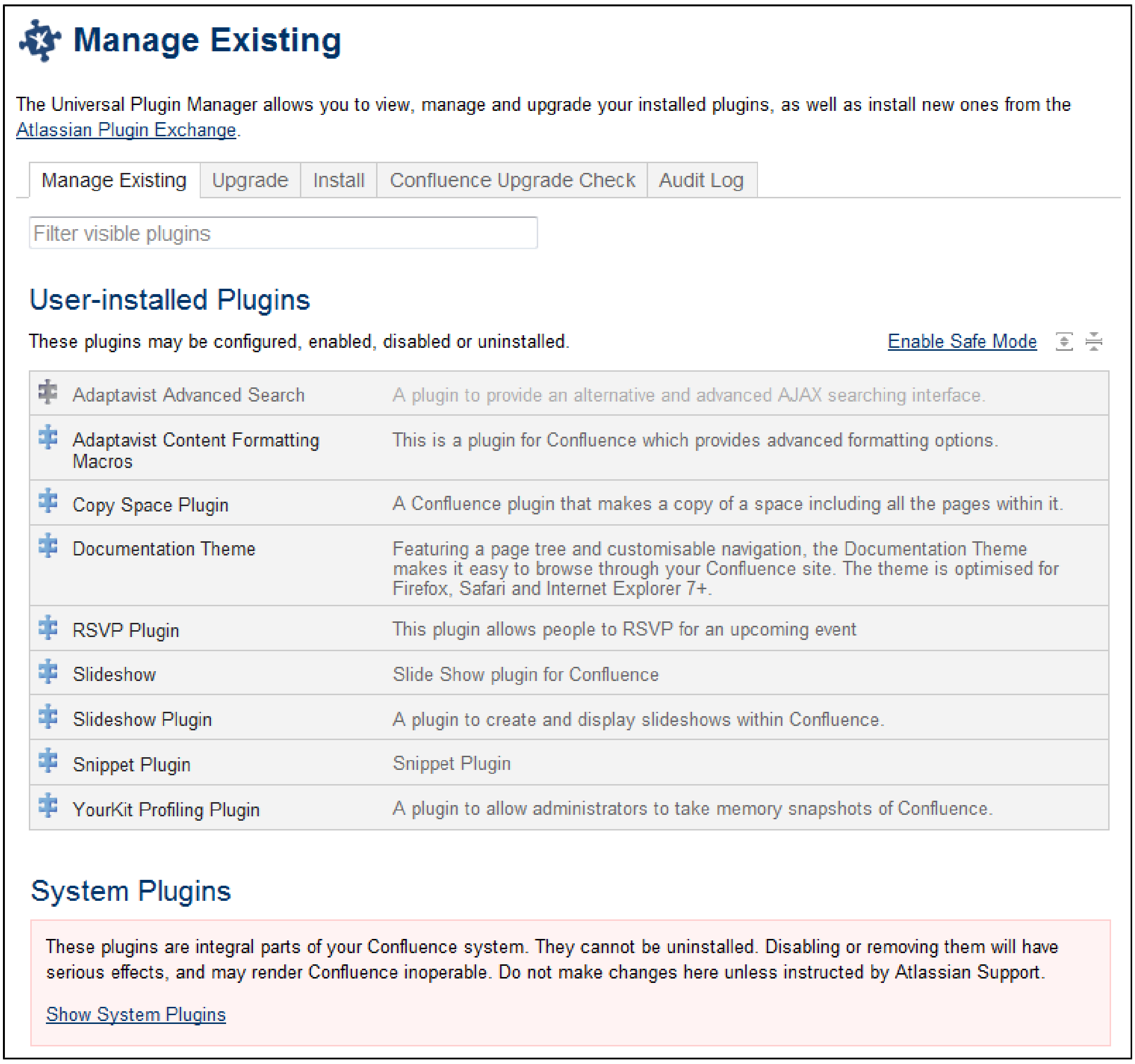
To view your installed plugins,

1. Click the '**Manage Existing**' tab. The plugins installed on your application will be displayed.
   - The plugins will be grouped into 'User-installed Plugins' and 'System Plugins'.
   - You can filter your list by entering keywords in the 'Filter visible plugins' text box.
   - The list of 'System Plugins' will be hidden by default. Click the '**Show System Plugins**' link, if you want to view them.
   - Enabled plugins will be listed with an 🧩 icon. Disabled plugins will be listed with an 🧩 icon.
   - Click the name of a plugin to view the plugin's details.
   - Click '**Enable Safe Mode**' to run your application in safe mode. Read 'Disabling or Enabling a Plugin' (see Related Topics below) for more information on Safe Mode.

What is the difference between a 'System Plugin' and a 'User Installed Plugin'?

- **System plugins** are those that shipped with the product when you downloaded it from Atlassian. These plugins are integral to the functioning of the system, and although you can disable some of them, you should not do so unless instructed by an Atlassian Support engineer. Note, not every system plugin can be disabled and you will not be able to uninstall any system plugins at all.
- **User-installed plugins** are those which have been installed in the product after it was set up: either by uploading a plugin jar file, or by placing it in the applications plugin directories. These plugins *can* be uninstalled.

Screenshot: Viewing Installed Plugins (Confluence)



Manage Existing

The Universal Plugin Manager allows you to view, manage and upgrade your installed plugins, as well as install new ones from the Atlassian Plugin Exchange.

User-installed Plugins

These plugins may be configured, enabled, disabled or uninstalled.

Adaptavist Advanced Search	A plugin to provide an alternative and advanced AJAX searching interface.
Adaptavist Content Formatting Macros	This is a plugin for Confluence which provides advanced formatting options.
Copy Space Plugin	A Confluence plugin that makes a copy of a space including all the pages within it.
Documentation Theme	Featuring a page tree and customisable navigation, the Documentation Theme makes it easy to browse through your Confluence site. The theme is optimised for Firefox, Safari and Internet Explorer 7+.
RSVP Plugin	This plugin allows people to RSVP for an upcoming event
Slideshow	Slide Show plugin for Confluence
Slideshow Plugin	A plugin to create and display slideshows within Confluence.
Snippet Plugin	Snippet Plugin
YourKit Profiling Plugin	A plugin to allow administrators to take memory snapshots of Confluence.

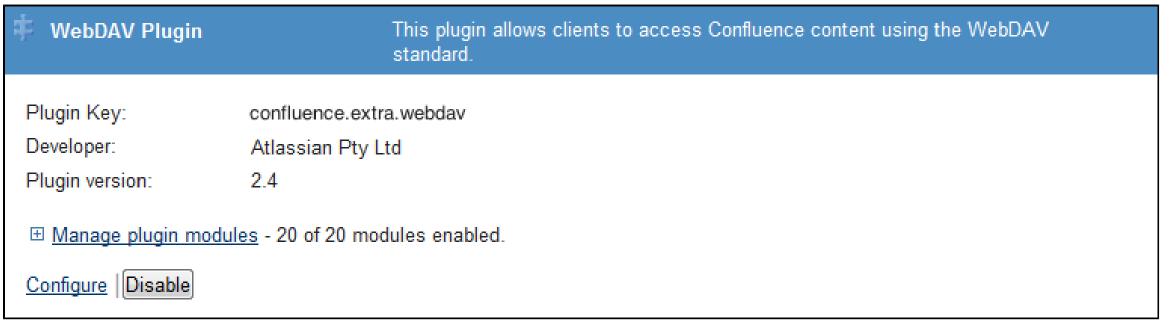
System Plugins

These plugins are integral parts of your Confluence system. They cannot be uninstalled. Disabling or removing them will have serious effects, and may render Confluence inoperable. Do not make changes here unless instructed by Atlassian Support.

Viewing a Plugin's Details

You can view the details for a plugin when you click the name of a plugin in the installed plugins list (as described above). The summary contains a short description of the plugin as well as buttons/links for plugin operations and related information.

Screenshot: Viewing a Plugin's Details (Confluence)



WebDAV Plugin — This plugin allows clients to access Confluence content using the WebDAV standard.

Plugin Key:	confluence.extra.webdav
Developer:	Atlassian Pty Ltd
Plugin version:	2.4

⊞ Manage plugin modules - 20 of 20 modules enabled.

- **Plugin key** — This field shows the unique key the identifies each plugin in the system.
- **Developer** — This field lists the name of the plugin developer and a link to the developer's homepage, if provided by the plugin developer.
- **Plugin version** — This field lists the version of the plugin currently installed.
- **Manage plugin modules** — Click this link to display the modules below the plugin summary. This link will only display if the plugin has modules, e.g. the Confluence Advanced Macros plugin. If you want to enable

or disable a plugin module, hover your mouse over the module and click the '**Enable**'/'**Disable**' button that displays.

- **Configure** — Click this link to display the configuration settings for the plugin in the Universal Plugin Manager. This link will be disabled if the plugin is disabled. Please note that not all plugins have settings that can be configured through the Universal Plugin Manager. Refer to 'Configuring a Plugin' (see Related Topics below) for more information.
- **Disable** — Click this button to disable the plugin in your application. This button will only display if the plugin is enabled. Refer to 'Disabling or Enabling a Plugin' (see Related Topics below) for more information.
- **Enable** — Click this button to enable the plugin in your application. This button will only display if the plugin is disabled.
- **Uninstall** — Click this button to uninstall the plugin from your application. This button will only display if the plugin is a user-installed plugin. Refer to 'Uninstalling a Plugin' (see Related Topics below) for more information.

Related Topics

Configuring a Plugin
Disabling or Enabling a Plugin
Uninstalling a Plugin

Plugin loading strategies in Confluence

The categories

Confluence plugins have different behaviour based on how they are loaded by Confluence. The plugins themselves are the same, but based on how they are loaded, they may or may not be upgraded, or may not be disabled, or may not be uninstalled. This chart should explain how plugins can be loaded by Confluence, and the ramifications for each choice.

The category any *particular* plugin is in can vary with Confluence version or circumstance. The examples mentioned here describe the way particular plugins are loaded by default in Confluence 2.8.

⚠ *The information on this page does not apply to Confluence OnDemand.*

Category	Description	Example
Static	**cannot be installed or upgraded without a Confluence restart**	

Core	Included with Confluence and cannot be uninstalled. The classes and plugin.xml are not bundled into plugin jars, but mixed in with Confluence source on the main classpath. Additionally, the plugin.xml definitions are not called "atlassian-plugin.xml" as they are everywhere else, but are named for the plugin e.g., "basic-macros.xml". We would like to separate some of them out and turn them into *Bundled* plugins.	Admin Sections
WEB-INF/lib	Confluence also places some plugin jars inside **WEB-INF/lib**. They are inserted during the build process by Maven. These plugins, likewise, cannot be uninstalled. In ancient times, this was the only way to install plugins, so users are also free to install plugins here. We try to discourage them from doing so, however. As of version 3.0, most of the JAR files in this directory are library dependencies, not plugins.	
Dynamic	**the opposite of static, these can be installed/upgraded while Confluence is running**	

Bundled	Bundled plugins can be administered from the Plugins console from Administration >> Plugins. You can upload or disable them there. *Bundled* plugins are included in a zip of jars called **atlassian-bundled-plugins.zip** which is on the main Confluence classpath, in a resources directory - `<confluence-install>/confluence/WEB-INF/classes/com/atlassian/confluence/setup`. At Confluence startup, they are extracted and copied into the **$CONFLUENCE_HOME/bundled-plugins** directory, from whence they are loaded. To remove a bundled plugin (you shouldn't normally have to do this), remove the plugin from the atlassian-bundled-plugins.zip file and the bundled-plugins directory, otherwise Confluence will just put it back in place on the next startup. In versions later than 2.6, you'll have to recreate the .jar file (if the jar file is from the lib folder) or recreate the zip folder(if its in the classes folder). Bundled plugins can be upgraded or disabled.	Office Connector
Uploaded	Installed by the user via the plugin repository or the Plugin Manager page. These plugins are stored in the database and then copied to the **$CONFLUENCE_HOME/plugins-cache** folder on each Confluence node.	could be anything

To summarise the relationships of categories in the table, all plugins are either *Static* or *Dynamic*. *Static* plugins can be further categorised into *Core* or *WEB-INF/lib*. *Dynamic* plugins are divided into *Bundled* and *Uploaded*.

Use of the categories in Confluence

Within Confluence, the *Core* and *WEB-INF/lib* categories are not actually named as such, and they don't map neatly to other names (though they do map, as will be explained). They are used here because of the logical distinction they provide.

In Confluence, some of the *Core* plugins are called "System". Plugins can be designated as "System" by adding a flag to the plugin manifest file. To do this, `system=true` should be added to the top-level `atlassian-plugin` element of the manifest file. The manifest file is generally called `atlassian-plugin.xml`, but it could have another name; the *Core* plugins' files do.

All of the *Core* plugins once were labeled as "System", but it seems the practice has faded over time. If a plugin is designated as "System", then it will not show up in the Plugin Manager page in Confluence and thus cannot be enabled/disabled. However, it *will* show up in the Plugin Repository Client, where it can be disabled; allowing disabling there is probably incorrect behavior.

Static plugins that are not marked as "System" (any remaining *Core* and *WEB-INF/lib* plugins), are simply called *Static* in Confluence. There is no way to tell the *WEB-INF/lib* and *Core* plugins apart from within Confluence. You just have to figure out where the classes are.

Members of the other specific categories - *Bundled* and *Uploaded* - can be determined. We can tell which plugins are *Bundled* and which plugins are *Uploaded*, so we know which plugins are *Uploaded* though this specific term is never used in the Confluence UI. Instead, they are called *Dynamic*.

Upgrading plugins

- *Core* plugins cannot be upgraded.
- *WEB-INF/lib* plugins can be upgraded by replacing the JAR in WEB-INF/lib and restarting Confluence.
- *Bundled* plugins can be upgraded using the Plugin Manager or the Plugin Repository Client. A new plugin jar is uploaded and stored as an *Uploaded* plugin. Confluence compares the version number with the *Bundled* plugin and uses the newer.
- *Uploaded* plugins are upgradable using the Plugin Manager or the Plugin Repository Client. When a new plugin jar is uploaded, the previous version is discarded from the database and the `$CONFLUENCE_HOME/plugin-cache`.

RELATED TOPICS

Removing Malfunctioning Plugins

Removing Malfunctioning Plugins

Confluence goes to some lengths to prevent itself being unusable due to a problematic plugin. However, sometimes a plugin will manage to do this anyway. This page describes what to do if a plugin cannot be disabled or deleted from the Administration console (from `Administration >> Plugins`).

> *The information on this page does not apply to Confluence OnDemand.*

Plugin Loading Strategies

1. Read through Plugin loading strategies in Confluence.
2. Determine where your plugin is loaded. The usual options are:
   a. The PLUGINDATA table on the database
   b. The <confluence-home>/bundled-plugins folder
   c. The <confluence-home>/plugin-cache folder
   d. The <confluence-home>/plugins-osgi-cache folder
   e. The <confluence-home>/plugins-temp folder
   f. The <confluence-install>/confluence/WEB-INF/lib folder (deprecated approach)

Check these locations when troubleshooting plugin loading issues.

> Check the How to display classpath utility for tips on what's loading, and the Knowledge Base Article on plugin malfunctioning.

Deleting a plugin from the Database

To remove a plugin from Confluence when Confluence is not running,

1. Connect to the Confluence database.
2. Run the following SQL statement in your database:

   ```
   select plugindataid, pluginkey, filename, lastmoddate from
   plugindata;
   ```

3. After you have found the plugindataid for the offending plugin, please run the following:

   ```
   delete from plugindata where plugindataid='XXXXXX';
   ```

   where XXXXXX is the plugindataid value.

4. Restart Confluence.

Disabling a plugin from the database

To disable in the database,

Run the following query on your Confluence database:

```
select BANDANAVALUE from BANDANA where
BANDANAKEY = 'plugin.manager.state.Map'
```

This will return a value like:

```
<map>
  <entry>

<string>com.atlassian.confluence.ext.us
age</string>
    <boolean>true</boolean>
  </entry>
</map>
```

Edit the value `boolean` to have **false**:

```
<map>
  <entry>

<string>com.atlassian.confluence.ext.us
age</string>
    <boolean>false</boolean>
  </entry>
</map>
```

Deleting a Bundled Plugin

Bundled plugins can be administered from the Plugins console from Administration >> Plugins. You can upload or disable them there.

Bundled plugins are included in a zip of jars called **atlassian-bundled-plugins.zip** which is on the main Confluence classpath, in a resources directory - `<confluence-install>/confluence/WEB-INF/classes/com/atlassian/confluence/setup`. At Confluence startup, they are extracted and copied into the **$CONFLUENCE_HOME/bundled-plugins** directory, from whence they are loaded. To remove a bundled plugin (you shouldn't normally have to do this), remove the plugin from the atlassian-bundled-plugins.zip file and the bundled-plugins directory, otherwise Confluence will just put it back in place on the next startup. In versions later than 2.6, you'll have to recreate the .jar file (if the jar file is from the lib folder) or recreate the zip folder(if its in the classes folder). Bundled plugins can be upgraded or disabled.

If you need to remove a bundled plugin, check to see if you have duplicates in the `<confluence-home>/bundled-plugins` or `<confluence-home>/plugin-cache` directory.

Usually, the problem is that an old plugin is getting loaded along with the properly bundled one, but if you need to remove a bundled plugin, check Plugin loading strategies in Confluence.

Enabling and Configuring Macros

Macros allow you to perform programmatic functions within a page, and can be used for generating more complex content structures.

Generally speaking, a macro is simply a command wrapped inside curly braces {...}. To learn how to write your own macro, or use macros written by other people, read the Confluence Plugin Guide.

⚠ *The information on this page does not apply to Confluence OnDemand.*

RELATED TOPICS:

- Configuring a URL Whitelist for Macros
- Configuring the User List Macro
- Enabling HTML macros
    - Enabling the html-include Macro
- Troubleshooting the Gallery Macro

Configuring a URL Whitelist for Macros

This page tells you how to restrict some Confluence macros so that they can get information from authorised sources (URLs) only.

Whitelisting URLs for the RSS and HTML Include macros

The RSS and HTML Include macros are used to include content dynamically from other websites onto a Confluence page. The included content may possibly be malicious or harmful to your Confluence instance.

Confluence administrators can set up a list of trusted URLs, thus limiting the locations from which the RSS macro and the HTML Include macro can draw their content.

The form below allows you to define specific URLs and/or URL patterns which are trusted, or to allow inclusion from all URLs without restriction.

To configure the URL whitelist:

1. Choose **Browse** > **Confluence Admin**.
2. Select **Configure Whitelist** in the left-hand panel. The 'Configure Whitelist' screen will appear, as shown in the screenshot below.
3. Select one of the options as follows:
    - **Allow all domains** — There will be no restrictions to the content which can be included onto your Confluence pages.
    - **Restrict to listed domains** — Confluence will allow content from trusted URLs only. When you select this option, a textbox will open allowing you to enter specific URLs and/or URL patterns. Enter one or more URLs, each on its own line. You can enter the full URL, or use the pattern

matching rules described below.

4. Click **Save**.

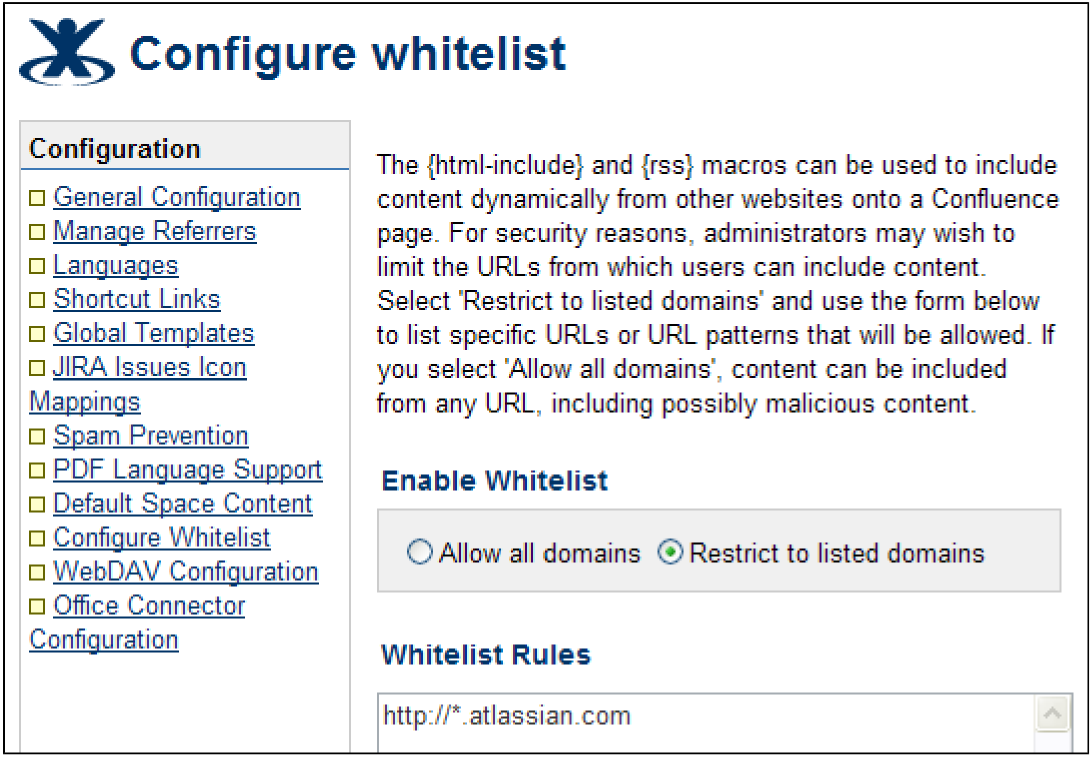
On this page:

Related pages:

- Enabling HTML macros
- RSS Feed Macro
- HTML Include Macro
- Configuring a URL Whitelist for Gadgets
- Confluence Administrator's Guide

⚠ *The information on this page does not apply to Confluence OnDemand.*

Screenshot: Configuring a URL whitelist for RSS and HTML Include macros



The {html-include} and {rss} macros can be used to include content dynamically from other websites onto a Confluence page. For security reasons, administrators may wish to limit the URLs from which users can include content. Select 'Restrict to listed domains' and use the form below to list specific URLs or URL patterns that will be allowed. If you select 'Allow all domains', content can be included from any URL, including possibly malicious content.

Enable Whitelist

○ Allow all domains ● Restrict to listed domains

Whitelist Rules

```
http://*.atlassian.com
```

URL Pattern-Matching Rules

Enter one URL or URL pattern per line. You can enter a full URL or use pattern-matching as described below:

- If the rule starts with an equals sign (=), only the exact URL following the '=' will be allowed.
- If the rule starts with a slash (/) then the whole rule will be treated as a regular expression.
- Otherwise, any asterisk (*) will be treated as a wildcard to match one or more characters.

Notes

Some things to be aware of:

- By default, the RSS and HTML Include macros are disabled in Confluence. A System Administrator can

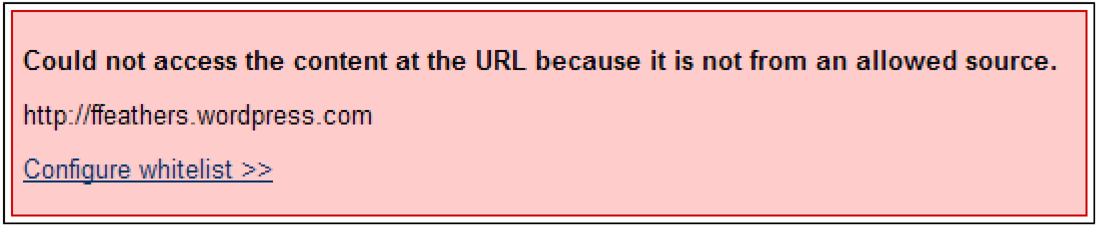
enable them on the 'Plugins' screen of the Confluence Administration Console.
- A user who has the 'Confluence Administrator' permission, but not necessarily the 'System Administrator' permission, can configure the URL whitelist for the HTML Include and RSS macros.

What Happens to a Page Containing a Disallowed URL?

A user can add the RSS Feed macro or the HTML-include macro to a Confluence page. The macro code includes a URL from which the content is drawn. When the page is displayed, Confluence will check the URL against the whitelist. If the URL is not allowed, Confluence will display an error message on the page.

The error message says that Confluence "could not access the content at the URL because it is not from an allowed source" and displays the offending URL. If the person viewing the page is a Confluence Administrator, they will also see a link to the Administration page where they can configure the URL whitelist.

Here is an example of the error message, including the link shown only to Confluence Administrators:

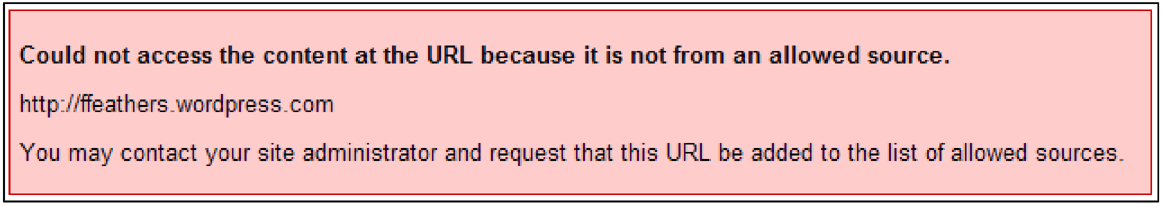


Could not access the content at the URL because it is not from an allowed source.

http://ffeathers.wordpress.com

Configure whitelist >>

Here is an example of the error message, but without the link.



Could not access the content at the URL because it is not from an allowed source.

http://ffeathers.wordpress.com

You may contact your site administrator and request that this URL be added to the list of allowed sources.

Configuring the User List Macro

The User List macro has an optional **Display Online** parameter. If the User Listener plugin is configured to allow this feature, then the page author can select **Display Online** to show a list of all online users.

You need to have System Administrator permissions in order to perform this function.

To enable the Display Online filter in the User List macro:

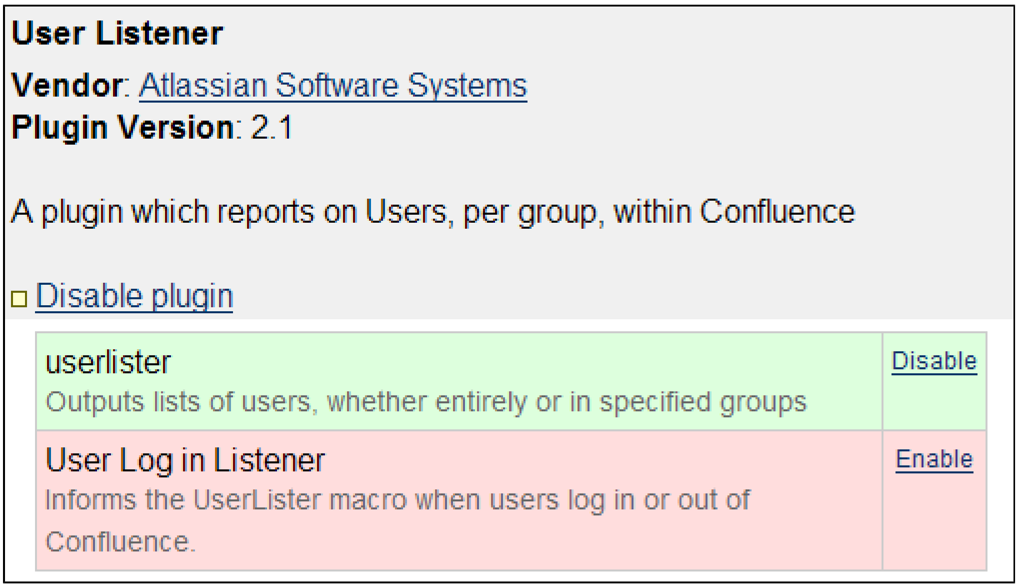
1. Choose **Browse** > **Confluence Admin**.
2. Select **Plugins** in the left-hand panel. This will list the currently installed plugins.
3. Scroll down and click **User Listener**. The User Listener plugin panel will appear at the top of the screen.
4. Enable the User Log In Listener module by clicking **Enable** on its right.
5. Restart Confluence.

The information on this page does not apply to Confluence OnDemand.

List of online users can be misleading

When the **Display Online** parameter is used, Confluence uses a context listener to generate the list of online users. A context listener is a J2EE term for something that listens for events in the application server. We listen for session open and close events, so a user is 'online' if they have a session on the application server. Some application servers don't correctly despatch close events for sessions – in these cases, the list of online users may be misleading.

Screenshot: Enabling the User Log In Listener



User Listener

Vendor: Atlassian Software Systems
Plugin Version: 2.1

A plugin which reports on Users, per group, within Confluence

□ Disable plugin

userlister Outputs lists of users, whether entirely or in specified groups	Disable
User Log in Listener Informs the UserLister macro when users log in or out of Confluence.	Enable

Related Topics

User List Macro
Enabling and Configuring Macros

Enabling HTML macros

The `{html}` macro allows you to use HTML code within a Confluence page.

The `{html-include}` macro allows you to include the contents of an HTML file in a Confluence page.

CAUTION: Including unknown HTML inside a webpage is dangerous. Because HTML can contain active scripting components, it would be possible for a malicious attacker to present a user of your site with script that their web browser would believe came from you. Such code could be used, for example, to steal a user's authentication cookie and give the attacker their Confluence login password.
By default, the HTML macros are disabled. You should only turn on these macros if you trust all your users not to attempt to exploit them.

You need to have System Administrator permissions in order to perform this function.

The information on this page does not apply to Confluence OnDemand.

To enable the HTML macros,

1. Choose **Browse** > **Confluence Admin**.
2. Select '**Plugins**' in the left-hand panel. This will display the installed plugins active for this Confluence installation. Click on 'Show System Plugins' to display bundled plugins.
3. Click' '**HTML macros**', then click '**Enable Plugin**'
4. Ensure that '**html (html)**' module is enabled

RELATED TOPICS

No content found for label(s) admin-macros.

Administrators Guide Home Confluence Documentation Home

Enabling the html-include Macro

The `{html-include}` macro allows you to include the content of an HTML file in a Confluence page. This page tells you how to enable the macro, so that it is available on your Confluence site. For help on using the macro, see HTML Include Macro.

> **CAUTION: Including unknown HTML inside a web page is dangerous.**
>
> Because HTML can contain active scripting components, it would be possible for a malicious attacker to present a user of your site with script that their web browser would believe came from you. Such code could be used, for example, to steal a user's authentication cookie and give the attacker their Confluence login password.

> ⚠ *The information on this page does not apply to Confluence OnDemand.*

Enabling the HTML Macros

By default, the HTML macros are disabled. You should only turn on these macros if you trust all your users not to attempt to exploit them.

ⓘ You need to have System Administrator permissions in order to perform this function.

To enable the HTML macros,

1. Choose **Browse** > **Confluence Admin**.
2. Select '**Plugins**' in the left-hand panel. This will display the installed plugins active for this Confluence installation.
3. Click' '**HTML macros**', then click '**Enable Plugin**'.

To embed an external page,

Use the following syntax:

```
{html-include:url=http://www.example.com}
```

To include HTML inline,

Use the following syntax:

```
{html}
<b>I like cheese</b>
{html}
```

RELATED TOPICS

HTML Include Macro

No content found for label(s) admin-macros.

Administrators Guide Home Confluence Documentation Home

Troubleshooting the Gallery Macro

Gallery Macro

The page _Gallery Macro Parameters does not exist.

For more information, refer to Gallery Macro.

⚠ *The information on this page does not apply to Confluence OnDemand.*

Troubleshooting

If you encounter the following error message: `System does not support thumbnails: no JDK image support` then ensure that you have following system property available for your JVM:

```
JAVA_OPTS=-Djava.awt.headless=true
```

Also see CONF-1737

⚠ Please note that gallery-ext.jar is available at CONF-6620

Adding, Editing and Removing User Macros

User macros are short pieces of code that perform an often-used function or add some custom formatting to a page. People can call the macro into action by adding the macro keyword to their Confluence pages. You can write a 'user macro' by adding code on a screen in the Confluence Administration Console.

Notes:

- You need System Administrator permissions in order to perform this function.
- See Shared User Macros for a list of community-donated macros.

⚠ Be careful when installing user macros from unknown authors.

- If you remove a user macro that is in use on Confluence pages, you will need to remove the macro from the pages manually. When you remove the user macro, the usage of the macro on the page will become invalid. *Hint:* Use the Confluence search to find all occurrences of the macro on pages and blog posts.

> ⚠ *The information on this page does not apply to Confluence OnDemand.*

To add a user macro:

1. Choose **Browse** > **Confluence Admin**.
2. Click **User Macros** in the left-hand panel.
3. Click **Create a User Macro** at the top of the list of macros.
4. Enter the macro details as explained in the guide to writing user macros.
5. Click **Add**.

To edit a user macro:

1. Choose **Browse** > **Confluence Admin**.
2. Select **User Macros** in the left-hand panel. This will list the currently configured user macros.
3. Click **Edit** next to the relevant macro.
4. Update the macro details as explained in the guide to writing user macros.
5. Click **Save**.

To remove a user macro:

1. Choose **Browse** > **Confluence Admin**.
2. Select **User Macros** in the left-hand panel. This will list the currently configured user macros.
3. Click **Remove** next to the relevant macro.

Related Topics

Best Practices for Writing User Macros

Examples of User Macros

Administrators Guide Home Confluence Documentation Home

Writing User Macros

User macros are short pieces of code that perform an often-used function or add some custom formatting to a page. People can add the macro to a page by choosing it from the Macro Browser when editing a Confluence page. The macro is run when the page is loaded by the browser. You can write a user macro by adding code on a screen in the Confluence Administration Console.

You need to have System Administrator permissions in order to create user macros.

> ⓘ **Do you need a plugin instead?**
>
> If you want to distribute your user macro as a plugin, please refer to the developer's guide to the User Macro plugin module. If you want to create more complex, programmatic macros in Confluence, you may need to write a Macro plugin.

On this page:

⚠ *The information on this page does not apply to Confluence OnDemand.*

Creating a User Macro

To create a user macro:

1. Go to the **Confluence Administration Console** and click **User Macros** in the left-hand panel.
2. Click **Create a User Macro**.
3. Supply the information in the input fields as explained below, then click **Add**.

The sections below tell you about each of the input fields.

Macro Name

Enter the text that people will see when looking for the macro in the Macro Browser.

Visibility

Set the visibility options to specify who can see this macro when they are searching using the Macro Browser or Autocomplete.

ℹ User macros must have parameters defined in order to appear in the Confluence 4.0 Macro Browser.

The options are as follows:

Visibility Option	Meaning
Visible to all users	All users will see this macro when searching for a macro using the Macro Browser or Autocomplete.

Visible only to system administrators	Choose this option if you want the macro to be 'hidden' from most users when the users are looking for a macro to add to a page. Note that this does not completely hide the macro. Instead, it is useful if you want to avoid cluttering the Macro Browser and Autocomplete with unnecessary macros. Specifically, if you are: • **Editing a page and inserting a macro using the Macro Browser:** Only system administrators will see this macro in the Macro Browser. For other users, the macro will not show up in the Macro Browser when the user searches for a macro to add to a page. • **Editing a page and inserting a macro using Autocomplete:** Only system administrators will see this macro in Autocomplete. For other users, the macro will not show up in the Autocomplete list when the user searches for a macro to add to a page. • **Viewing the page:** The macro output will be visible to all users who have permission to see the page. • **Editing a page that already contains the macro:** Provided a user has permission to edit the page, the macro will be visible to all users when editing the page, and all users who have permission to edit the page will also be able to edit or remove the macro. Please note that all the macro information will also be discoverable, including the macro title, description, parameter names and other metadata. Do not include confidential data anywhere in the definition of a user macro, even if it is marked as visible only to system administrators.

Macro Title

Enter the text that should appear in the Macro Browser and in Autocomplete, to identify this macro when people are looking for it to insert onto a page.

Description

Enter the text that should appear in the Macro Browser describing this macro. Note that the Macro Browser's search will pick up matches in the description as well as in the title.

Categories

Select one or more categories for your macro. To select more than one category, hold down the 'Ctrl' key while selecting. These are the categories that appear in the Macro Browser, helping users to choose a macro from a logical set.

Icon URL

If you would like the Macro Browser to display an icon for your macro, enter the URL here. You can enter an absolute URL or a path relative to the Confluence base URL. For example:

- Absolute URL:

```
http://mysite.com/mypath/status.png
```

- Relative URL:

```
/images/icons/macrobrowser/status.png
```

Documentation URL

Enter the URL pointing to the online help or other documentation for your macro.

Macro Body Processing

Specify how you want Confluence to process the body of your macro before passing it to your macro. Below is an explanation of the macro body and the options available.

What is the macro body?

The macro body is the content that is displayed on the wiki page. If the macro allows a body, users will be able to enter body content when configuring the macro in the Macro Browser.

How can I use the macro body?

If you specify that your macro has a body, you will be able to pass text to the macro when you invoke it from within a page.

If your macro has a body, any body content that the user enters will be available to the macro in the `$body` variable. See the section about the template below. In addition, the options below allow you to tell Confluence to pre-process the body before it is placed in the macro output.

What are the options for macro body?

Body Processing Option	Meaning
No macro body	Select this option if your macro does not need a body.

Escaped	If your macro has a body, and you make use of the body as `$body` in your template, Confluence will add escape characters to the HTML markup in the macro body. You could use this if you want to show the HTML markup in the rendered page. For example, if the body is:
	`<b>Hello World</b>`
	Then value of $body will be:
	`&lt;b&gt;Hello World&lt;/b&gt;`
	This will render as:
	`<b>Hello World</b>`

Unrendered	If your macro has a body, and you make use of the body as `$body` in your template, HTML in the body will be processed within the template before being output. Ensure that HTML is ultimately output by the template.
Rendered	If your macro has a body, and you make use of the body as `$body` in your template, Confluence will recognise HTML in the macro body. For example, if the body is: `<b>Hello World</b>` Then value of $body will be: `<b>Hello World</b>` This will render as: **Hello World**

Template

Enter XHTML code to specify what the macro will do.

For example, to add a macro inside the macro you are writing, you would write:

```
<ac:macro ac:name="someOtherMacro" />
```

Quick guide

- Use XHTML in the macro template. Details of Confluence's XHTML format are in Confluence Storage Format.
- You can use the Velocity templating language. Here is more information on the Velocity project.
- If your macro has a body, your template can refer to the macro body text by specifying '`$body`'.
- Each parameter variable you use must have a matching metadata definition. Use `@param` to define metadata for your macro parameters.
- When using the information passed using parameters, refer to your parameters as $paramXXX where 'XXX' is the parameter name that you specifed in the `@param` metadata definition.
- Use `@noparams` if your macro does not accept parameters. ⓘ Note that this will prevent your macro appearing in the macro browser.

See our detailed guide to writing a user macro template.

Examples and Best Practices

See:

- Examples of User Macros
- Best Practices for Writing User Macros

Related Topics

Developer documentation:

- User Macro Module
- Macro Module
- Confluence Plugin Guide

Library of user-contributed user macros

- Shared User Macros

> ⓘ Be careful when installing user macros. Ideally use only macros from authors and sources that are well known to you.

Best Practices for Writing User Macros

This section contains tips and suggestions for best practice in macro coding. To see how to write a user macro and add it to your Confluence site, take a look at our guide to writing user macros.

> ⚠ *The information on this page does not apply to Confluence OnDemand.*

Add a Descriptive Header to your Macro Template

We recommend that you include a short description of your macro via comments at the top of the **Template** field as shown below. You can see an excellent example in the 'Image rollover' user macro.

```
## Macro title: My macro name
## Macro has a body: Y or N
## Body processing: Selected body
processing option
## Output: Selected output option
##
## Developed by: My Name
## Date created: dd/mm/yyyy
## Installed by: My Name

## Short description of what the macro
does
```

Expose your Parameters in the Macro Browser

Confluence offers great options for making your macro look good in the macro browser. You can specify the macro category, link to an icon, define the parameters that the macro browser will use to prompt the user for information, and more.

In particular, read the documentation on defining the macro parameters to be displayed in the macro browser.

Supply Default Values for Macro Parameters

You cannot guarantee that a user will supply parameters, so one of the first things to do in the macro is check that you have received some value if you expect to rely on it later on in the macro code.

In the example below, the macro expects three parameters. It substitutes sensible defaults if they are not supplied:

```
#set($spacekey= $paramspacekey)
#set($numthreads= $paramnumthreads)
#set($numchars= $paramnumchars)

## Check for valid space key, otherwise use current
#if (!$spacekey)
  #set ($spacekey=$space.key)
#end

## Check for valid number of threads, otherwise use default of 5
#if (!$numthreads)
  #set ($numthreads=5)
#end

## Check for valid excerpt size, otherwise use default of 35
#if (!$numchars)
  #set ($numchars=35)
#end
```

Related Topics

Writing User Macros

Examples of User Macros

Below are some sample user macros. To see how to write a user macro and add it to your Confluence site, take a look at our guide to writing user macros.

On this page:

- Simple Examples of User Macros
- User-Contributed User Macros

⚠ *The information on this page does not apply to Confluence OnDemand.*

Simple Examples of User Macros

We provide these user macros as simple examples just to get you started. You would not want to install these user macros onto your Confluence site.

Example 1: User Macro to Display 'Hello World'

Take a look at an example of a 'Hello World' macro.

Example 2: The 'Error' User Macro to Create a Red Box

Let's write a simple macro that creates a red box (using an existing Confluence style) around some text. This may be useful for writing about error conditions, for example. That is why we give this macro the name 'error'.

To create the 'Error' user macro:

1. Go to the 'Confluence Administration Console' and click **User Macros** in the left-hand panel.
2. Click **Create a User Macro** at the top of the list of macros.
3. Enter the macro attributes as follows:
   - Macro Name: `error`
   - Visibility: `Visible to all users in the Macro Browser`
   - Macro Title: `Error`
   - Description: `Displays a red box around some text`
   - Categories: `Confluence Content`
   - Icon URL: You can leave this field empty.
   - Documentation URL: You can leave this field empty.
   - Macro Body Processing: `Rendered`
   - Template:

     ```
     <div class="error">$body</div>
     ```
4. Click **Add**.

To use the macro within a page, use the Macro Browser. Your page will display an error box, like this:

> This is bad

Example 3: User Macro to Demonstrate the Use of Parameters

This example demonstrates how you can pass parameters into your macro. Let's say you want to write your own font colour macro:

```
<span style="color: $param0">$body</span>
```

The usage of this macro will be:

```
{colour:green}Some example text{colour}
```

The output will be:
Some example text

If your macro requires more than one parameter, you can use variables $param0 to $param9 to represent them. To specify multiple parameters, use:

```
{colour:red|blue|green}
```

Where red, blue and green are the 1st, 2nd and 3rd parameters respectively.

Alternatively, you can also use explicitly named parameters in your macro. These macro parameters will appear as variables with the name $param<x> where <x> is the name of your parameter. To specify named parameters, use:

```
{style:colour=red}
```

In your user macro you can then use `$paramcolour` which will have the value `red` in this case.

User-Contributed User Macros

You may want to take a look at the library of user-contributed user macros.
⚠ Be careful when installing user macros from unknown authors.

Hello World Example of User Macro

This page tells you how to create a user macro that displays the text 'Hello World!' and any variable text you place between the macro tags. (For full details about creating a user macro, see the guide to writing user macros .)

> ⚠ *The information on this page does not apply to Confluence OnDemand.*

Defining the 'Hello World' User Macro

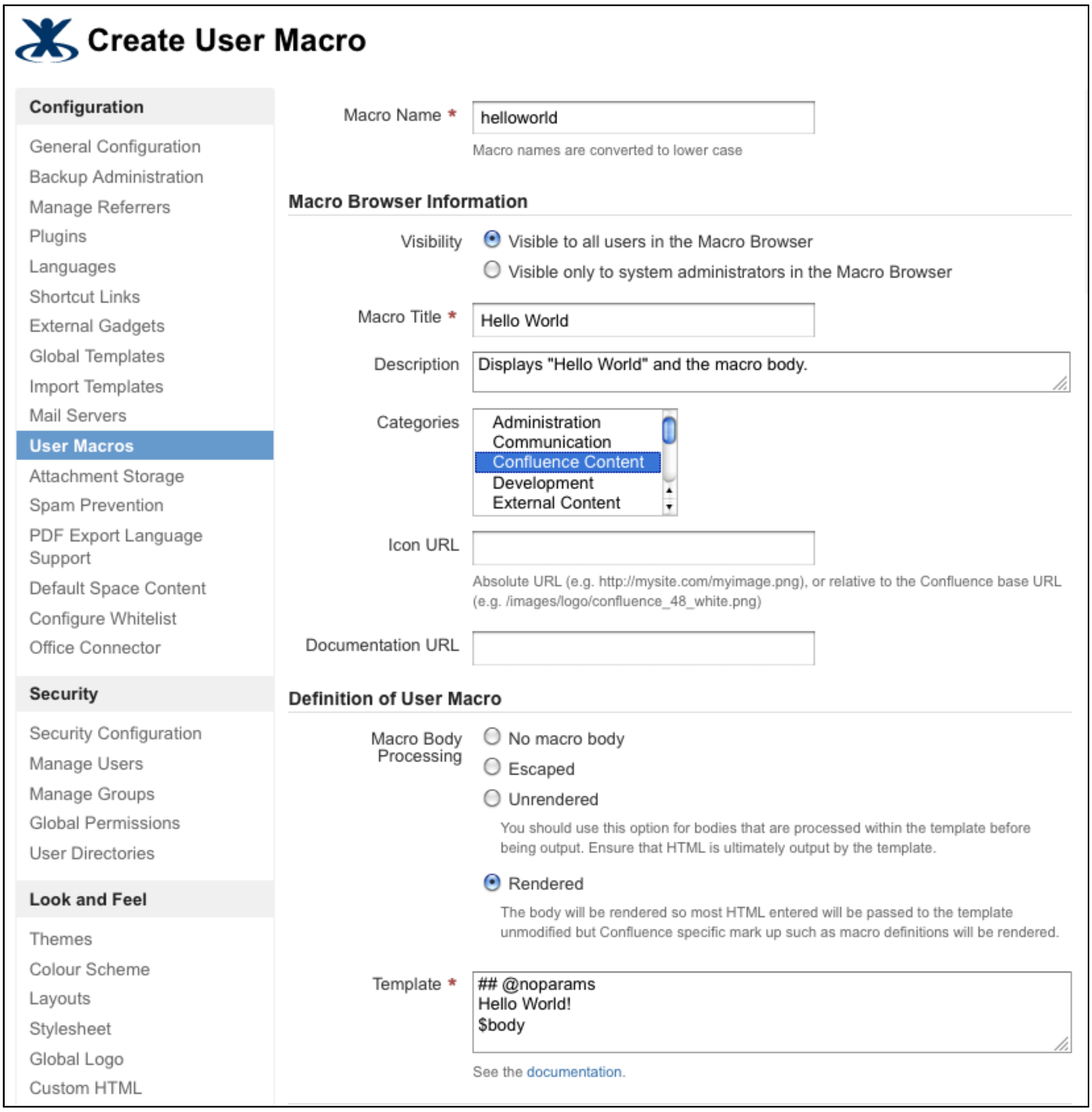
To create the 'Hello World' user macro:

1. Go to the 'Confluence Administration Console' and click **User Macros** in the left-hand panel.
2. Click **Create a User Macro** at the top of the list of macros.
3. Enter the macro attributes as follows:
    - Macro Name: `helloworld`
    - Visibility: `Visible to all users in the Macro Browser`
    - Macro Title: `Hello World`
    - Description: `Displays "Hello World" and the macro body.`
    - Categories: `Confluence Content`
    - Icon URL: You can leave this field empty.
    - Documentation URL: You can leave this field empty.
    - Macro Body Processing: `Rendered`
    - Template:

```
## @noparams
Hello World!
$body
```

4. Click **Add**.

Screenshot: Definition of the 'Hello World' user macro



Create User Macro

Macro Name * helloworld

Macro names are converted to lower case

Macro Browser Information

Visibility
● Visible to all users in the Macro Browser
○ Visible only to system administrators in the Macro Browser

Macro Title * Hello World

Description: Displays "Hello World" and the macro body.

Categories: Administration, Communication, Confluence Content (selected), Development, External Content

Icon URL

Absolute URL (e.g. http://mysite.com/myimage.png), or relative to the Confluence base URL (e.g. /images/logo/confluence_48_white.png)

Documentation URL

Definition of User Macro

Macro Body Processing
○ No macro body
○ Escaped
○ Unrendered

You should use this option for bodies that are processed within the template before being output. Ensure that HTML is ultimately output by the template.

● Rendered

The body will be rendered so most HTML entered will be passed to the template unmodified but Confluence specific mark up such as macro definitions will be rendered.

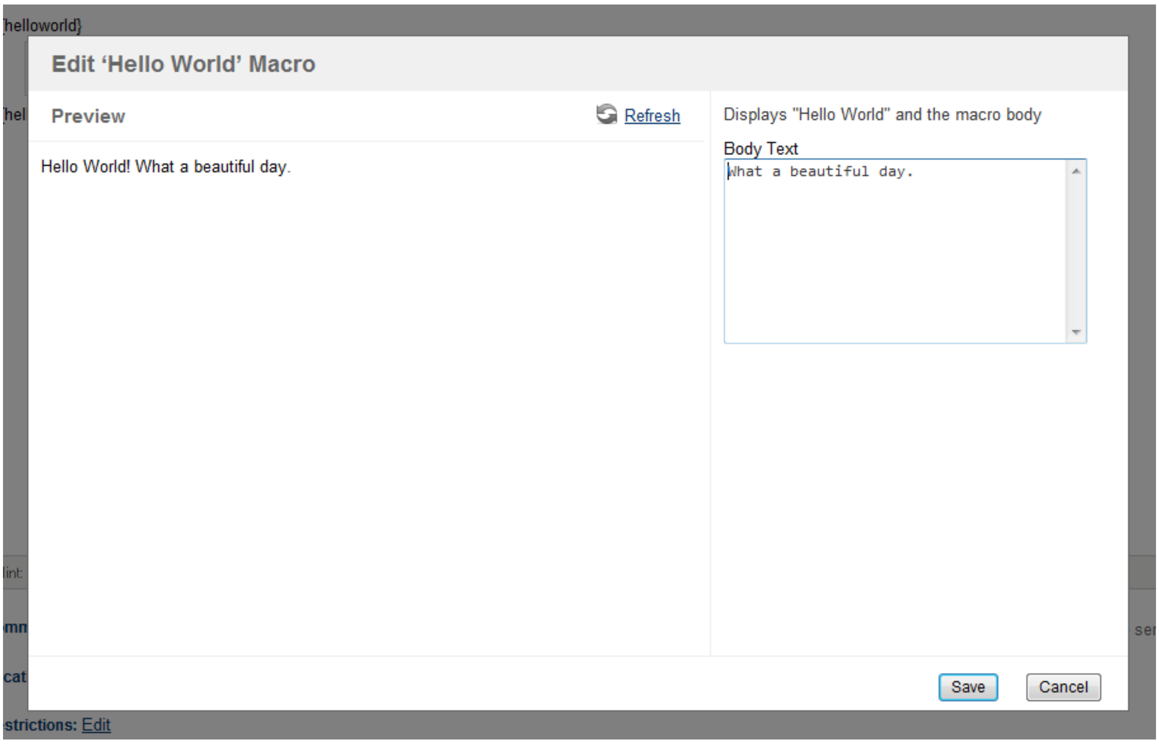
Template *

```
## @noparams
Hello World!
$body
```

See the documentation.

Using the 'Hello World' Macro on a Page

Now you can add the macro to your Confluence page using the Macro Browser:



Edit 'Hello World' Macro

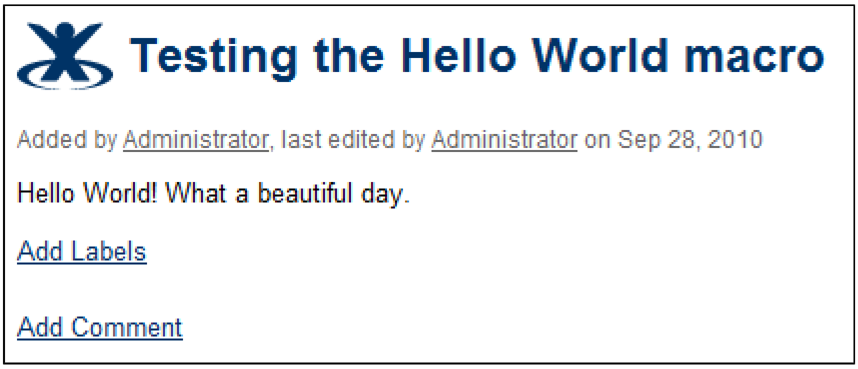
Preview

Hello World! What a beautiful day.

Displays "Hello World" and the macro body

Body Text: What a beautiful day.

The result is:



Testing the Hello World macro

Added by Administrator, last edited by Administrator on Sep 28, 2010

Hello World! What a beautiful day.

Related Topics

Writing User Macros

NoPrint Example of a User Macro

This page gives an example of a user macro, the 'NoPrint' macro, that you can use to prevent text from being printed. (For full details about creating a user macro, see the guide to writing user macros.)

> ⚠ *The information on this page does not apply to Confluence OnDemand.*

Defining the 'NoPrint' User Macro

To create the 'NoPrint' user macro:

1. Go to the 'Confluence Administration Console' and click **User Macros** in the left-hand panel.
2. Click **Create a User Macro** at the top of the list of macros.
3. Enter the macro attributes as follows:
    - Macro Name: `noprint`
    - Visibility: `Visible to all users in the Macro Browser`
    - Macro Title: `NoPrint`
    - Description: `Hides text from printed output.`
    - Categories: `Confluence Content`

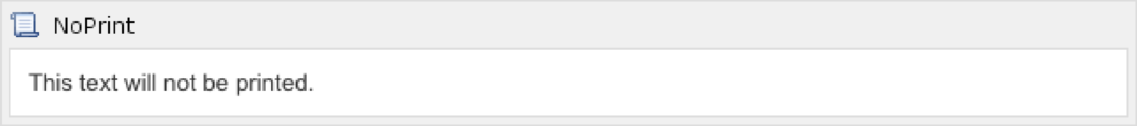
- Icon URL: You can leave this field empty.
- Documentation URL: You can leave this field empty.
- Macro Body Processing: `Rendered`
- Template:

```
## @noparams
<div class="noprint">$body</div>
```

4. Click **Add**.

Using the 'NoPrint' Macro on a Page

Now you can add the macro to your Confluence page using the Macro Browser. Text entered into the body of the macro placeholder will not be printed.



NoPrint

This text will not be printed.

Making PDF Export Recognise the NoPrint Macro

See Advanced PDF Export Customisations#noprint.

Related Topics

Writing User Macros

Guide to User Macro Templates

You write a user macro in a screen in the Confluence Administration Console. The 'template' is one of the fields that you define when writing a user macro. (See the rest of the guide to writing user macros.) This page gives you guidelines about the code you can enter in a user macro template.

Quick guide to user macro tempates:

- Use XHTML in the macro template. Details of Confluence's XHTML format are in Confluence Storage Format.
- You can use the Velocity templating language. Here is more information on the Velocity project.
- If your macro has a body, your template can refer to the macro body text by specifying '`$body`'.
- Each parameter variable you use must have a matching metadata definition. Use `@param` to define metadata for your macro parameters.
- When using the information passed using parameters, refer to your parameters as $paramXXX where 'XXX' is the parameter name that you specifed in the `@param` metadata definition.
- Use `@noparams` if your macro does not accept parameters. ℹ Note that this will prevent your macro appearing in the macro browser.

On this page:

⚠ *The information on this page does not apply to Confluence OnDemand.*

Accessing your Macro's Body

Use the `$body` object within your user macro template to access the content passed to your macro in the macro body.

The `$body` object is available if you have specified that your macro has a body (in other words, if you have *not* selected **No macro body**).

Example: Let's assume your macro is called `helloworld`.
Enter the following code in your template:

```
Hello World: $body
```

A user, when editing a Confluence page, chooses your macro in the Macro Browser and then enters the following in the macro placeholder that is displayed in the edit view:

```
From Matthew
```

The wiki page will display the following:

> *Hello World: From Matthew*

Using Parameters in your User Macro

You can specify parameters for your macro, so that users can pass it information to determine its behaviour on a Confluence page.

How your Macro's Parameters are Used on a Confluence Page

When adding a macro to a Confluence page, the Macro Browser will display an input field for each of your macro's parameters. The field type is determined by the parameter type you specify for each parameter.

Defining the Parameters

Briefly, a parameter definition in the template contains:

- `@param`
- The parameter name
- A number of attributes (optional)

Format:

```
## @param MYNAME:title=MY TITLE|type=MY TYPE|desc=MY DESCRIPTION|required=true|multiple=true|default=MY DEFAULT VALUE
```

Additional notes:

- The order of the parameters in the template determines the order in which the Macro Browser displays the parameters.
- We recommend that you define the parameters at the top of the template.
- There may be additional attributes, depending on the parameter type you specify.

The sections below describe each of the attributes in detail.

Attribute Name	Description	Required / Recommended / Optional
(an unnamed, first attribute)	A unique name for the parameter. The parameter name is the first attribute in the list. The name attribute itself does not have a name. See the section on name below.	Required
title	The parameter title will appear in the Macro Browser. If you do not specify a title, Confluence will use the parameter name.	Recommended
type	The field type for the parameter. See the section on type below.	Recommended
desc	The parameter description will appear in the Macro Browser.	Optional
required	Specifies whether the user must enter information for this parameter. Defaults to 'false'.	Optional
multiple	Specifies whether the parameter accepts multiple values. Defaults to 'false'.	Optional
default	The default value for the parameter.	Optional

Parameter Name

The parameter name is the first attribute in the list. The name attribute itself does not have a name.

Example: The following code defines 2 parameters, named 'foo' and 'bar':

```
## @param foo
## @param bar
```

Parameter Type

The field type for the parameter. If you do not specify a type, the default is `string`.

Parameter Type	Description
boolean	Displays a checkbox to the user and passes the value 'true' or 'false' to the macro as a string.
enum	Offers a list of values for selection. You can specify the values to appear in a dropdown in the Macro Browser. Example of specifying the enum values: `## @param colour:title=Colour|type=enum|enumValues=Grey,Red,Yellow,Green` *Note about i18n:* Confluence does not support internationalisation of the enum values.The value the user sees is the one passed to the macro as the parameter value, with the capitalisation given. In this case 'Grey', 'Red', etc.
string	A text field. This is the default type. Example with a required field: `## @param status:title=Status|type=string|required=true|desc=Status to display`

<table>
<tr><td>confluence-content</td><td>Offers a control allowing the user to search for a page or blog post. Example:
<pre>## @param page:title=Page|type=confluence-content|required=true|desc=Select a page do use</pre></td></tr>
<tr><td>username</td><td>Search for user.
<pre>## @param user:title=Username|type=username|desc=Select username to display</pre></td></tr>
<tr><td>spacekey</td><td>Offers a list of spaces for selection. Passes the space key to the macro. Example:
<pre>## @param space:title=Space|type=spacekey</pre></td></tr>
<tr><td>date</td><td>Confluence accepts this type, but currently treats it in the same way as 'string'. Example:
<pre>## @param fromDate:title=From Date|type=date|desc=Date to start from. Format: dd/mm/YYYY</pre>
<i>Note about dates:</i> A user can enter a date in any format, you should validate the date format in your user macro.</td></tr>
<tr><td>int</td><td>Confluence accepts this type, but currently treats it in the same way as 'string'. Example with a default value:
<pre>## @param numPosts:title=Number of Posts|type=int|default=15|desc=Number of posts to display</pre></td></tr>
</table>

<table>
<tr><td>percentage</td><td>Confluence accepts this type, but currently treats it in the same way as 'string'. Example:<pre>## @param pcent:title=Percentage|type=percentage|desc=Number of posts to display</pre></td></tr>
</table>

Using the Parameters in your Macro Code

The parameters are available in your template as `$paramfoo`, `$parambar` for parameters named "foo" and "bar".

Normally, a parameter like `$paramfoo` that is missing will appear as '$paramfoo' in the output. To display nothing when a parameter is not set, use an exclamation mark after the dollar sign like this: `$!paramfoo`

Using No Parameters

If your macro does not accept parameters, you should use `@noparams` in your template. That will let Confluence know that it need not display a parameter input field in the Macro Browser.

If the user macro contains no parameters and does not specify `@noparams`, then the Macro Browser will display a free-format text box allowing users to enter undefined parameters. This can be confusing, especially if the macro does not accept parameters.

Example: Add the following line at the top of your template:

```
## @noparams
```

Objects Available to your Macro

Including the macro body and parameters, the following Confluence objects are available to the macro:

Variable	Description	Class Reference
`$body`	The body of the macro (if the macro has a body)	String
`$paramfoo`, `$parambar`, ... `$param<name>`	Named parameters ("foo", "bar") passed to your macro.	String
`$config`	The `BootstrapManager` object, useful for retrieving Confluence properties.	BootstrapManager
`$renderContext`	The `PageContext` object, useful for (among other things) checking `$renderContext.outputType`	PageContext

`$space`	The `Space` object that this content object (page, blog post, etc) is located in (if relevant).	Space
`$content`	The current `ContentEntity` object that this macro is a included in (if available).	ContentEntityObject

Macros can also access objects available in the default Velocity context, as described in the developer documentation.

Controlling Parameter Appearance in the Editor Placeholder

A macro developer (or author of a user macro) can control which fields of the macro should appear in the placeholder in the Confluence Editor.

Plugin Macro Metadata

The macro metadata for a plugin macro now has parameter options as shown in the following example:

```
<macro name="panel"
documentation-url="help.panel.macro">
            <category name="formatting"/>
            <parameters>
                <parameter name="title"
type="string">
                    <option
key="showNameInPlaceholder" value="false"
/>
                    <option
key="showValueInPlaceholder" value="true"
/>
                </parameter>
                <parameter
name="borderStyle" type="string"/>
                <parameter
name="borderColor" type="color"/>
<snip
```

The option `showNameInPlaceholder` specifies that in the above example the '`title`' parameters name should not be shown.

The option `showValueInPlaceholder` specifies that the user entered value for this parameter should be shown.

So, for the above example, the macro placeholder could show something like 'panel | my panel title'.
If `showNameInPlaceholder` was true instead of false it would show something like 'panel | title = my panel title'.

If a macro has neither option on any of it's parameters then the default behaviour is to show all parameters: full title and value. If one or more parameters has either option set then all parameters without the options set will default to false (i.e. will not be shown).

User Macro Metadata

The behaviour for a user macro is as described above, however the method of configuration is within the @param entry in the template.
So, the example from above would look something like:

```
## @param
title|type=string|option-showNameInPlaceholder=false|option-showValueInPlaceholder
=true
```

Related Topics

Writing User Macros
Examples of User Macros

Configuring the Office Connector

The Office Connector is a Confluence plugin that allows Confluence users to interact with Microsoft Office and Open Office in various ways. You can display content from Office documents on a wiki page and import content from an Office document into Confluence. Please refer to the User Guide for details of these interactions.

A System Administrator can enable or disable parts of the Office Connector and can configure options as described below.

On this page:

⚠ *The information on this page does not apply to Atlassian OnDemand sites with multiple apps. If you are using Confluence-only OnDemand, the information does apply.*

Enabling and Disabling the Office Connector and its Modules

The Office Connector is bundled with Confluence 2.10 and later, so you should not need to install it. But you may wish to enable or disable some of its modules.

A System Administrator can install, enable or disable plugins and plugin modules. You can read a general overview in Installing Plugins and Macros.

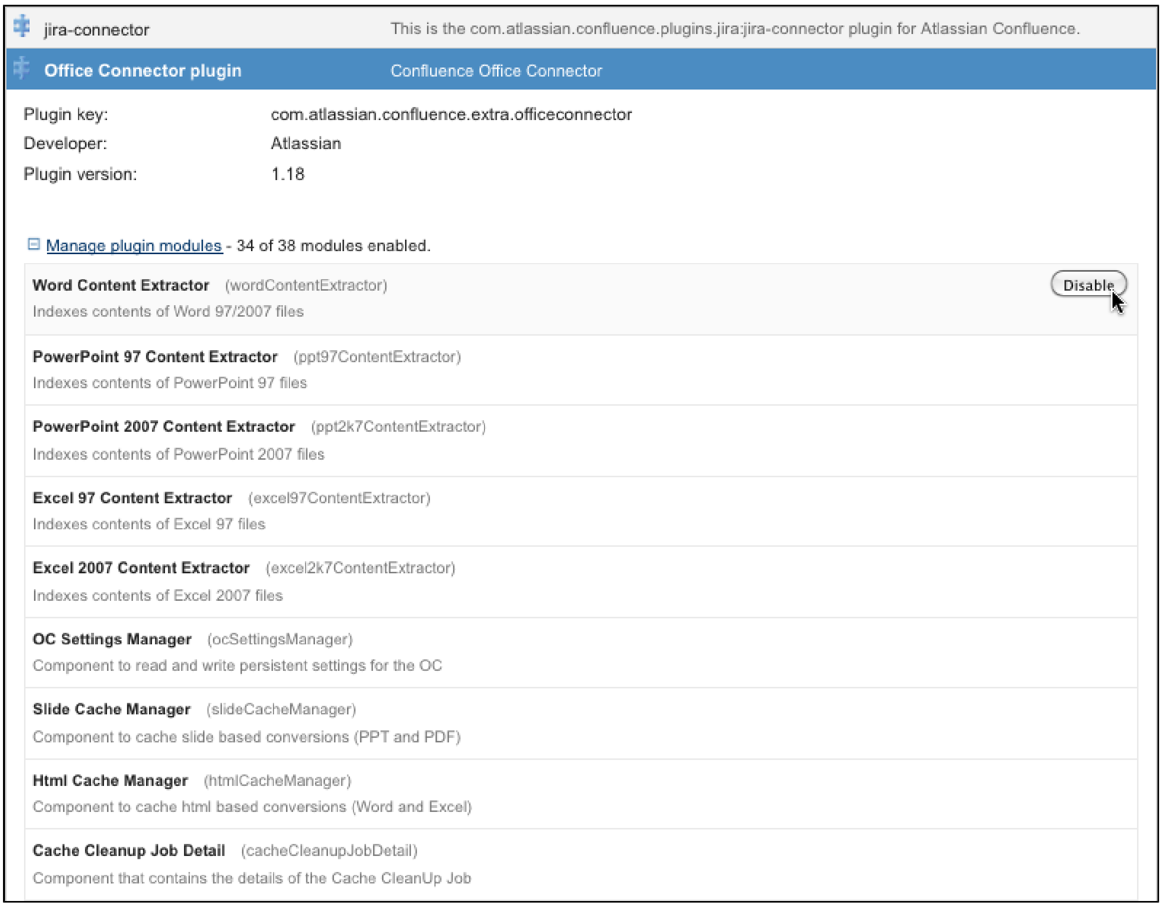
To enable or disable the Office Connector and its modules:

1. Select **Plugins**, under 'Configuration' in the left-hand panel of the Confluence Administration Console.
2. Click **Show system plugins** under 'System Plugins'.
3. Search the page for **Office Connector plugin** and select the link.
4. The 'Office Connector plugin' panel will appear near the top centre of the page, as shown in the screenshot below.
5. Now you can do one of the following:
   - **Configure plugin** – This will take you to the separate plugin configuration screen described below.
   - **Disable plugin** – Click this link if you want to disable all modules of the plugin, but leave the plugin

installed on your Confluence site.

- **Uninstall plugin** – Click this link if you want to remove the Office Connector permanently from your Confluence site. To restore it at a later date, you will need to re-install it from the Confluence Plugin Repository.
- **Manage plugin modules** – You can also enable or disable one or more of the Office Connector modules, as described in the table below.

Screenshot: Enabling the Office Connector plugin and its modules



jira-connector This is the com.atlassian.confluence.plugins.jira:jira-connector plugin for Atlassian Confluence.

Office Connector plugin Confluence Office Connector

Plugin key:	com.atlassian.confluence.extra.officeconnector
Developer:	Atlassian
Plugin version:	1.18

⊟ Manage plugin modules - 34 of 38 modules enabled.

Word Content Extractor (wordContentExtractor)
Indexes contents of Word 97/2007 files

PowerPoint 97 Content Extractor (ppt97ContentExtractor)
Indexes contents of PowerPoint 97 files

PowerPoint 2007 Content Extractor (ppt2k7ContentExtractor)
Indexes contents of PowerPoint 2007 files

Excel 97 Content Extractor (excel97ContentExtractor)
Indexes contents of Excel 97 files

Excel 2007 Content Extractor (excel2k7ContentExtractor)
Indexes contents of Excel 2007 files

OC Settings Manager (ocSettingsManager)
Component to read and write persistent settings for the OC

Slide Cache Manager (slideCacheManager)
Component to cache slide based conversions (PPT and PDF)

Html Cache Manager (htmlCacheManager)
Component to cache html based conversions (Word and Excel)

Cache Cleanup Job Detail (cacheCleanupJobDetail)
Component that contains the details of the Cache CleanUp Job

The following modules are available for the Office Connector plugin:

Module	Description
OC Settings Manager	Component to read and write persistent settings for the Office Connector.
Slide Cache Manager	Component to cache slide-based conversions when displaying PowerPoint and PDF documents.
Html Cache Manager	Component to cache HTML-based conversions when displaying Word and Excel documents.
File Cache Cleanup Job	This module is a recurring task that cleans up the Office Connector file cache.
File Cache Cleanup	This module is the trigger for the File Cache Cleanup Job.

Office Connector administration link	This module supplies the 'Office Connector Configuration' link in the left-hand panel of the Confluence Administration Console. The link gives access to the plugin configuration screen described below.
Link for previewing a search result	This modules supplies the 'View' link which appears next to attachments displayed in search results, where the attachment is an Office document.
Link for previewing an attachment	This modules supplies the 'View' link which appears next to attachments displayed on the 'Attachments' view of a page, where the attachment is an Office document.
viewfile	This module supplies the {viewfile} macro. See View File Macro.
viewdoc	This module supplies the Word document component of the {viewfile} macro.
viewxls	This module supplies the Excel document component of the {viewfile} macro.
viewppt	This module supplies the PowerPoint document component of the {viewfile} macro.
viewpdf	This module supplies the PDF document component of the {viewfile} macro.
editgrid	This module is used to migrate editgrid users to the Office Connector.
Import Word UI on page tabs	This module supplies a 'Doc Import' tab which appears in older versions of Confluence, next to the 'View', 'Edit', 'Attachments' and 'Info' tabs. Not relevant to Confluence 2.10 or later, except for custom themes.
Import Word UI on drop down menu	This modules supplies the 'Doc Import' link which appears in the Confluence 'Tools' dropdown menu.
Edit in Office javascript resource	This module contains the javascript resources for launching the desktop applications for editing Office documents.
Office Connector Servlet	This module allows Confluence users to edit their Confluence pages in Microsoft Word. It performs the conversion to and from Word.
Office Authenticator Filter	This module authenticates HTTP requests from Office applications.

PPT slide web service	This module allows Confluence users to view a PowerPoint presentation on a wiki page. It provides the slide images to the Flash control which displays the slides on the wiki page.
DOC and XLS image cache web service	This module is required if Confluence users want to view a Word document or an Excel spreadsheet on a wiki page. It allows images to be stored in a cache on the server, so that they can be retrieved when the browser renders the HTML page.
Office Connector Actions	This module must be enabled if the Office Connector is used.

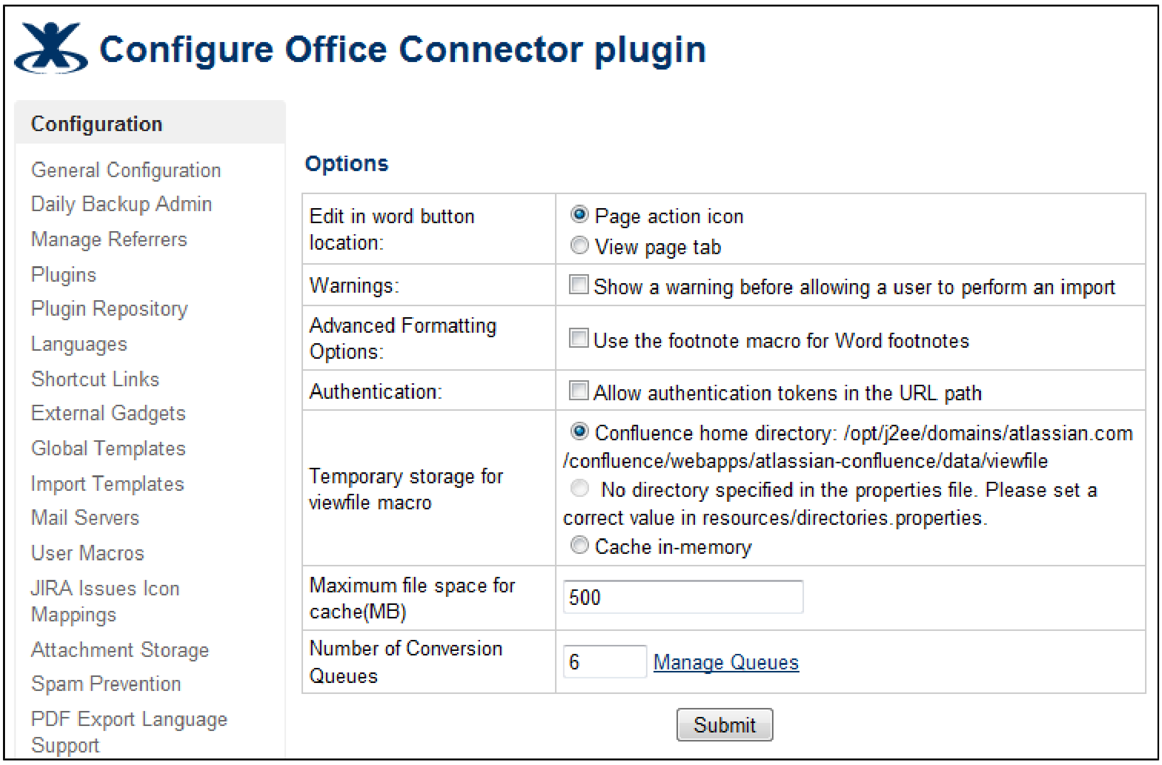
Configuring the Office Connector Options

A Confluence administrator can set the options described below, to determine the behaviour of the Office Connector on your Confluence site.

To set the configuration options for the Office Connector:

1. Select **Office Connector** under 'Configuration' in the left-hand panel of the 'Confluence Administration Console'. The 'Configure Office Connector plugin' screen will appear.
2. Set the configuration options as described in the table below.

Screenshot: Configuring the Office Connector options



Configure Office Connector plugin

Options

Edit in word button location:	● Page action icon ○ View page tab
Warnings:	□ Show a warning before allowing a user to perform an import
Advanced Formatting Options:	□ Use the footnote macro for Word footnotes
Authentication:	□ Allow authentication tokens in the URL path
Temporary storage for viewfile macro	● Confluence home directory: /opt/j2ee/domains/atlassian.com/confluence/webapps/atlassian-confluence/data/viewfile ○ No directory specified in the properties file. Please set a correct value in resources/directories.properties. ○ Cache in-memory
Maximum file space for cache(MB)	500
Number of Conversion Queues	6 Manage Queues

The configuration options are described in the table below:

Option	Default Value	Description

Warnings: Show a warning before allowing a user to perform an import	Disabled	If this option is enabled, the user will receive a warning when importing a Word document. The warning will tell the user when they are about to overwrite existing content.
Advanced Formatting Options: Use the footnote macro for Word footnotes	Disabled	If this option is enabled, a Confluence page created from an imported Word document will use the {footnote} macro from Adaptavist to render any footnotes contained in the document. Note that you will need to install the Footnotes plugin onto your Confluence site. For more information about this plugin and macro, please refer to the Footnotes plugin.
Authentication: Allow authentication tokens in the URL path	Disabled	If this option is enabled, the Office Connector will use authentication tokens in the URL.
Temporary storage for viewfile macro	The Confluence Home directory.	The {viewfile} macro will cache data temporarily. This option allows you to set the location of the cache. Available settings are: • **Confluence home directory** – The temporary file will be stored in your Confluence Home directory. • **A directory specified in the `directories.properties` file** – You can specify a location by editing the Office Connector's `directories.properties`file: 1. Go to the `bundled-plugins` directory in your Confluence Home directory. 2. Copy the Office Connector JAR file to a temporary location: `OfficeConnector-x.xx.jar`, where 'x.xx' is the version number.

3. Unzip the JAR file and find the `directories.properties` file in the `resources`directory. The content of the file looks like this:

```
#Complete the following line to set a custom cache directory.
#If resetting to blank, don't delete anything before or including the '='
com.benryan.confluence.word.edit.cacheDir=
```

4. Edit the last line, adding the path to your required temporary location directly after the '=' character. For example:
    - On Windows:

      ```
      com.benryan.confluence.word.edit.cacheDir=c:\my\path\
      ```

    - On Linux:

      ```
      com.benryan.confluence.word.edit.cacheDir=/home/myusername/my/path
      ```

5. Save the file, recreate the JAR and put it in the `bundled-plugins` directory in your Confluence Home directory, overwriting the original JAR.

- **Cache in-memory** – The temporary file will be held in memory. We recommend this option if you are running in a clustered environment.

Maximum file space for cache (MB)	500	This is the maximum size of the cache used by the {viewfile} macro. (See above.)
Number of Conversion Queues	6	This is the maximum number of threads used to convert PowerPoint or PDF slide shows. You can use this setting to manage Confluence performance, by limiting the number of threads so that the Office Connector does not consume too many resources. Click **Manage Queues** to view attachments that are still pending conversion.

Related Topics

Office Connector Prerequisites
Office Connector Limitations and Known Issues
Working with the Office Connector
Installing Plugins and Macros

Operating Large or Mission-Critical Confluence Installations

This page gives guidelines for operational management teams who are responsible for a large Confluence installation, or for a Confluence installation which is crucial to the business of their organisation.

Introduction to this Page

Motivation for Presenting these Guidelines

Most Confluence installations start off small. Ten people in an early-adoption department use it for a couple of weeks. Everything works well and the good news starts spreading. Adoption increases throughout the organisation. More and more people use the wiki, and more and more rely on Confluence being up and running. After a while even the CEO starts blogging. And then a system outage occurs.

Now what?

Wikis like Confluence often grow into mission-critical applications within just a few months. Often adoption is so fast that IT departments haven't had the time to scale up their support.

We have assembled some requirements to help you make sure that your installation of Confluence can be mission critical. There are no surprises to be found here — all of the requirements would apply to any other piece of software that is mission critical within your organisation.

Who should Read these Guidelines?

The guidelines **do not apply to you** if you are using Confluence with just a few dozen users, and no one really minds if Confluence is down for a couple of hours because your database has crashed.

But if any one of the following applies to you, then these guidelines are **a must read for you**!

- The wiki has become your organisation's documentation base.
- Your users can't work properly when Confluence is down.
- Your boss or customer threatens to terminate your contract if you don't meet a strict service level

agreement (SLA), such as 99.9% availability.

On this page:

⚠ *The information on this page does not apply to Confluence OnDemand.*

Requirements of Large or Mission-Critical Confluence Installations

Dedicated Hardware for Confluence

In a small work group with a few dozen or even hundreds of users, your Confluence installation can happily share the CPUs, memory and disks with other low-profile applications and a database.

But with thousands or even tens of thousands of users, you need dedicated hardware that runs Confluence and nothing else, and it needs to be fast hardware with plenty of RAM. While you *can* run Confluence in a virtualised environment such as VMware, we suggest you don't do it for mission-critical or high-load installations unless you are a real expert in virtualisation. Otherwise your other VMs might have performance problems which propagate to Confluence.

If you experience database-related problems, you should consider moving the Confluence database to a dedicated machine. Confluence itself can run queries that impact the performance of other applications, and other application problems or scheduled tasks can have an adverse affect on the usability of Confluence.

Dedicated Qualified Staff

If your Confluence installation is mission critical and your service level agreements require 24/7 up time, you need to be able to pinpoint problems quickly. You need qualified staff, dedicated to looking after Confluence, who are available during business hours and possibly beyond.

If you require assistance from the Atlassian Support team, you may need to answer some pretty technical questions to help us diagnose what is going on in your systems. Also keep in mind that Atlassian support assists you in finding problems in Confluence, but we can't help you administer your systems.

In particular, we recommend that you have dedicated staff in the roles listed below.

Operations Team with General Administrators

If your organisation relies on Confluence being up and running around the clock with very little downtime, you need people who can set up, maintain, tune and improve your Confluence installation. This requires at least one person, but ideally you will have a team of operational engineers.

If your wiki is mission critical, chances are that other IT systems within your organisation have already made it necessary to have such an operations team. So you will probably not need to hire someone specifically to administrate Confluence. But it is vital that supporting and maintaining Confluence is added to the list of responsibilities of that operations teams, and that you can get them to troubleshoot and analyse Confluence at short notice.

If problems arise and you need to contact Atlassian Support, these engineers will be our first point of contact. We may ask them to provide details of log files, application-server settings, monitoring systems, and so on.

Network Staff

If Confluence is mission critical for large numbers of users, it is vital that you have dedicated network staff available to track down problems when they arise.

A mission-critical installation will usually be used by hundreds or even thousands of users, and you don't want to keep them waiting because a network card breaks, or because someone has made an undocumented change to the network and you don't have an expert around who can figure it out.

Again, this only applies to mission-critical systems. If you use Confluence for less critical collaboration and knowledge sharing, and a broken network cable causing a day's downtime is no major catastrophe, then you will not need dedicated networking staff.

Database Staff

If Confluence is mission critical for a large number of users, you need an experienced database administrator (DBA) available to troubleshoot database performance issues and other potential problems. It is dangerous not to have an experienced full-time DBA at hand at short notice when running a mission critical application. While small installations of Confluence basically work 'out of the box', any system that involves high load or high-availability requirements needs continual monitoring, optimising and fine tuning of the Confluence database. Database monitoring is no trivial task — it's not something that anyone can learn quickly.

Developers

You may have decided to customise Confluence by changing its source-code, or by writing your own plugins. If your server is mission-critical, you must nominate staff who will be responsible for that code, and they must be up for the task. Otherwise you might end up in a situation in which your server experiences downtimes because of custom code is broken, or does not work with a newer version of Confluence anymore, but you can't fix the problem because no one knows how the customized code works, and you can't uninstall it either because it has become critical for your Confluence usage pattern. Keep good track of changes, and have someone available to jump into action if there is a problem Don't let the summer intern write mission-critical plugins, unless you have more senior staff to maintain that code as long as it is in use.

Constant Monitoring of Production Systems

You will need to monitor your production systems constantly.

When the wiki is the lifeblood of your organisation, you need know exactly what is going on inside, so that you can plan for future needs and analyse potential bottlenecks.

Monitoring involves a number of essential tasks, including those listed below:

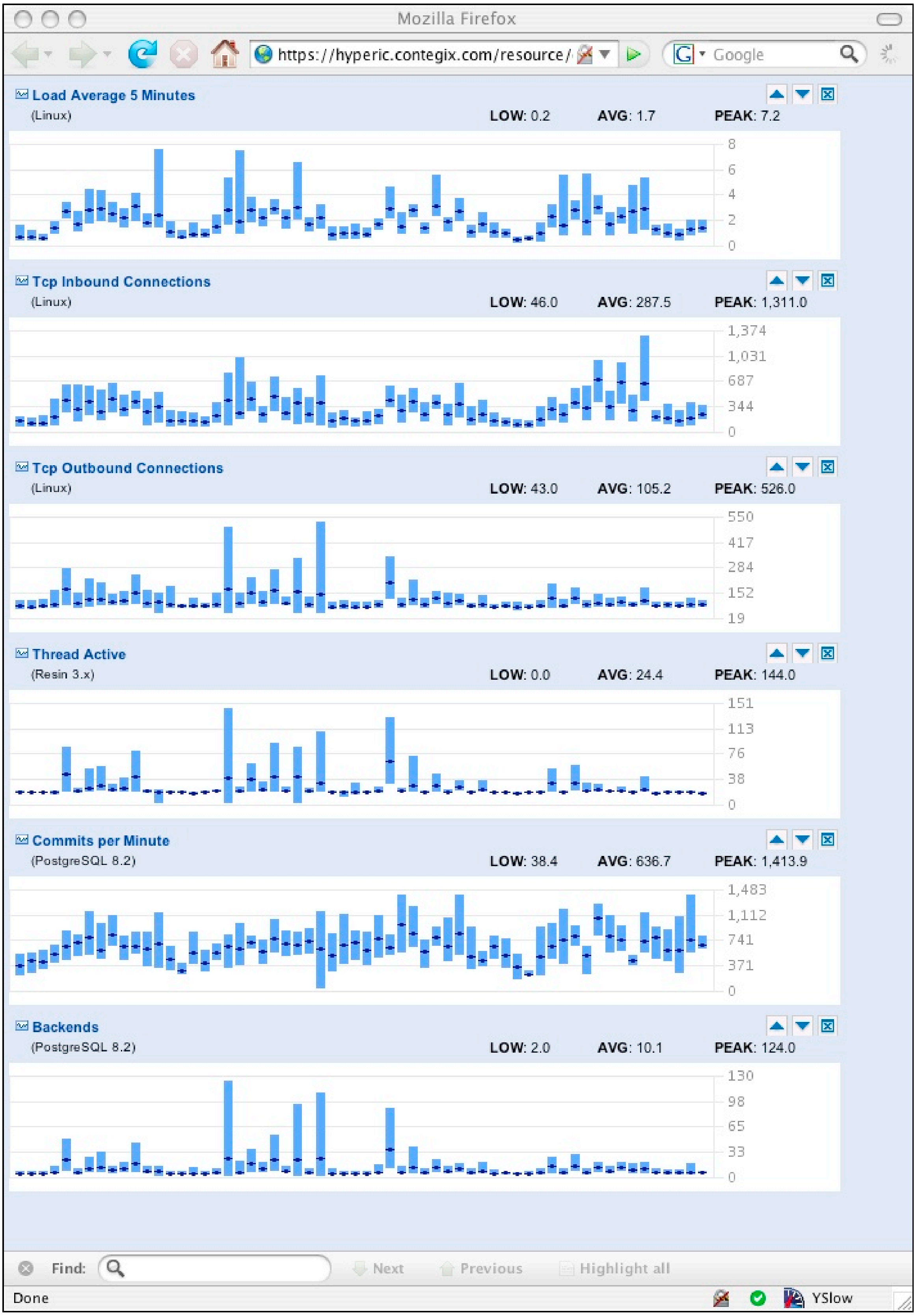
- Monitoring log files.
- Checking for HTTP-availability and performance (e.g. by getting the same page every five minutes and displaying the time on a graph).
- Looking at many different parameters such as load, connections, IO, database-trends, and so on.
- Charting long-term trends.
- Keeping an access log of requests to the web server. This is vital, especially when requesting performance-related support from Atlassian.

Monitoring a web application like Confluence implies also monitoring the subsystems it uses. Many outages and downtimes are caused by broken mail servers, databases running out of space, file systems filling up and so on. It is often possible to detect these trends way before the actual web application breaks down. Keep an eye on the file system, and if you see it is getting closer to 90% utilisation, you can mend the situation without Confluence breaking down. Or even if the worst case happens (e.g. the database breaks down and Confluence is affected straight away) then having the proper monitoring for the database server makes troubleshooting a lot easier.

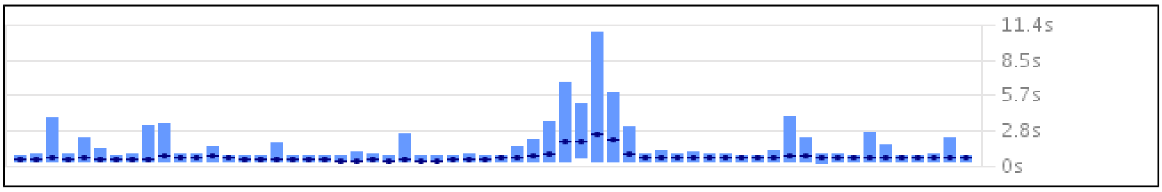
Tools for Monitoring Confluence

At Atlassian we use Hyperic. But the list of monitoring systems is long and we can't recommend a specific product over the other. If your organisation has a monitoring system already, make sure you hook up Confluence to it. If you don't have a monitoring system yet, you need to install one as soon as you feel Confluence is mission critical.

As an example of what our monitoring UI looks like, have a look at this screenshot:



The following screenshot shows one of our sensors looking at the HTTP response times of our documentation wiki over the last 8 days. You can clearly see an incident four days ago. Having the graph (and regularly looking at it) allowed us to pinpoint the problem. We analysed the access logs and found that webpage-profiling had been enabled but not disabled again, which caused performance problems.



This page would get too long if we described all our monitoring sensors - but just to give you an impression, this is what we monitor on the JVM level alone.

JVM basics

- Current Loaded Classes
- Daemon Thread Count
- Heap Memory Committed
- Heap Memory Max
- Heap Memory Used
- Loaded Classes
- Loaded Classes per Minute
- Object Pending Finalization Count
- Peak Thread Count
- Thread Count
- Unloaded Classes
- Unloaded Classes per Minute

JVM garbage collection

- Collection Count
- Collection Count per Minute
- Collection Time
- Collection Time per Minute

JVM memory: (Metrics for Eden space, Old Gen, Survivor space, Perm Gen)

- Commited Memory
- Used Memory

We get the same level of detail for our database, for the file system, for the CPU, for the network, and so on. Not all of this is needed all the time. But if your company depends on an application, then the more information you have at your fingertips the better. Fortunately these metrics can be extracted quite easily once you have a monitoring system in place.

Adherence to Strict Upgrade Procedures

Your organisation will have its own upgrading procedure. Here are a few recommendations that you should add to your list:

- Our main recommendation: Never change more than one component at a time. Sometimes it may be tempting to upgrade the server hardware when you upgrade Confluence, but we recommend you don't do that. It makes pinpointing errors much more difficult. So, for example, don't upgrade hard disks in conjunction with a Confluence version upgrade, don't change the Confluence configuration at the same time as you upgrade your Apache software, and don't upgrade a major third-party plugin the day you move your database system to a new machine. The list is endless, these were just a few examples to get you thinking.
- After each upgrade step, run Confluence for a couple of days to check that everything is still fine.
- Keep track diligently of what you change, and when. It will be nearly impossible for us to help you if you can't tell us what exactly you changed at what time.
- Keep a copy of all log files produced during the upgrade, together with notes about what changed between successive restarts.

Always take careful note of the upgrade notes published with the Release Notes of each Confluence version, as well as the Confluence Upgrade Guide.

Example

Here you can see an extract of our change log for `http://confluence.atlassian.com` — the server that hosts this very page.

Sydney time	Server time	Event	Reason/Purpose (including JIRA issues)
	2008-03-25 22:18	Started upgrade to 2.8-m9-r3 (build #1314)	
	2008-03-25 22:25	App server brought down due to failed database upgrade	
	2008-03-26 00:51	Server brought back up after database restored from backup. Running 2.8-m9-r3.	
	2008-03-28 04:18	GC algorithm changed from concurrent to parallel collector. Max heap increased from 1.4 GB to 2.0 GB	
	2008-04-24	Hyperic agent started with connection to Resin.	
	2008-05-08 20:30 - 22:30	Manual updates to menu.css, comments.js and comments.css in webapp	Temporary fix for @JIRA, @JIRA which was impacting performance
	2008-05-12	Updated cache sizes for five caches, bounced server.	Cache efficiency was low on these caches.
2008-05-13 18:00-18:20	2008-05-13 03:00-03:20	Upgrade from Resin 3.0 to Tomcat 5.5	
2008-05-14 16:30-17:00		Upgrade from Confluence 2.8.1-rc2 to 2.8.1-rc3	
	2008-05-14 20:30	Install new cronjob as j2ee for automating access log analysis	@JIRA

Testing of Upgrades before Production Implementation

You should test upgrades in a staging environment.

Before rolling out a new version of Confluence (or of the software or hardware that it uses, e.g. database systems, application servers, data storage), make sure that you test the upgrade with real data (e.g. a database dump) on a completely independent machine.

Here's an example of what such a test would pick up: The new release of Confluence may not be compatible with a custom third party plugin you have previously installed, thus breaking the plugin's functionality. You may not even know that anyone installed that plugin — but maybe many people are already using it. You'll want to find out about this before you actually roll out the new version of Confluence.

Here is an outline for a simple upgrade test:

1. Create a clone of your production environment, using a database dump to obtain a copy of the Confluence data. We'll call this your 'staging environment'.
2. Upgrade the staging environment to the new version of Confluence.
3. Ask a few selected users from different departments to check the pages they commonly access, but have them do it in the staging environment.

✅ Hint: In addition to finding weirdnesses with plugins, this may also show whether training for new functionality is needed in some of the departments. The IT department staff may be able to handle the upgrade to a new version of Confluence without training, but perhaps the sales representatives who use the wiki less often will need some training.

> **Getting a license for your staging environment**
> Only a **technical contact** for your commercial/academic license is able to create a Developer license.
>
> Atlassian supplies 'developer' licenses which can be used by existing commercial license holders who wish to deploy non-production installations of our software to use in QA/staging environments. Developer licenses are free of charge to commercial license holders and, like our commercial offerings, they include 12 months of updates starting from the date of purchase of the commercial license.
>
> If you hold a commercial license, you can obtain a free developer license by following these steps:
>
> 1. Log in to your Atlassian account.
> 2. Under the "Licenses" heading, all of your licenses will be displayed. Click the plus sign next to a license to view its details.
> 3. Click the **'View Developer License'** link in the bottom right corner of the license detail panel, below your commercial license key.

Enforcing Security Guidelines

Security is one of the most important issues for Confluence. We are constantly spending large amounts of effort to keep up with security threats and to Confluence's security model. We treat security breaches with utmost priority, and the recent releases have been improved to fend off advanced attack vectors like cross-site scripting (XSS), cross-site request forgery (XSRF) and header injection flaws. Altogether we believe that Confluence is a very secure product. But of course as with any software there are occasional bugs, and we are fixing security issues whenever they come up. We regularly release minor software releases that contain security fixes. This means you should upgrade your system frequently. Obviously this can affect your system's uptime. You should also make sure your whole infrastructure around Confluence is made robust as well (consider operating systems, webservers, application servers, networks, social engineering aspects, etc).

As with any other distributed system, you need to decide on a case by case basis if classified documents can be stored in it. It is common practice to store the most secure documents on computers that are not even connected to the physical intranet. Please contact your company's security officer to learn more about your enterprise's security procedures.

Make sure to have qualified staff around, so you can deal with security issues quickly. Once a security patch becomes available or a security incident happens, speed is essential.

Please refer to our dedicated Configuring Confluence Security page for more technical details.

Load-Testing Environments

Many customers ask us,

> *So, how many users and spaces can I put into Confluence, and what is the best hardware do to so?*

The answer is, 'It depends'.

It depends a lot on your use case. Confluence is so successful because it can cover a huge range of use cases. If most of your users only access Confluence infrequently, it is no problem to have 70 000 to 100 000 users. But if each user is a power-user who uses the system the whole day, there's a substantial decrease in number Confluence can take without tuning. If your pages are short, simple, and don't contain a lot of macros, then the situation will be vastly different from a system that relies heavily on macros, background-tasks, or other features.

If your system is large (for example serving more than 10 000 users or storing more than 1000 spaces) or mission-critical (which it could be with as few as 1000 users who use it all the time) you need one or more more load-testing environments.

Even if your system is working nicely for 20 000 users right now, it might take just another 2000 users to push it over the edge.

We recommend the following basic procedure:

- Set up an environment that closely resembles your production environment.
- Gather statistics from your production system.
- Regularly apply a similar kind of load (and slightly higher) to the load-testing environment.
- Analyse how well Confluence scales for your usage patterns.

The Confluence development team has load-testing scripts available which you can use to simulate load. You can also contact Atlassian Support for more details.

Tuning

You may need to be able to tune your installation in the ways mentioned below.

Optimising your System

If you have large numbers of users, then downloading all the static content (CSS, default images, JavaScript-files) may result in a high additional load on the application server that can be offloaded to a caching web server.

Please refer to the following additional information:

- Our general Performance Tuning page.
- Information on configuring a large Confluence installation.

Limiting Third-Party Plugins

You may have to restrict the number of third-party plugins installed on your Confluence instance.

Most third-party plugins are not specifically written for high-load environments. What works fine in low-load environments could have unexpected and adverse effects when thousands of users are competing for your application server's CPU time or for database IO.

A common source of problems is access to database connections. If you have fewer users than database connections, it does not matter if an operation holds on to a database connection for two seconds while it downloads some data from the internet. With hundreds of concurrent users, this could quickly become a bottleneck.

Confluence itself is tested and optimised to handle high loads and avoids these kinds of problems. But if you install a number of plugins that have not been tested against high load, your system may become unstable.

We recommend that you load test the common use cases of each unofficial third-party plugin if your Confluence installation is mission critical. Only activate plugins that are vital to your business, and never allow experimental plugins onto your production system until they have been tested in a staging environment.

Selecting and Tuning your JVM

You should select your JVM carefully and you may need to be able to tune it.

The selection of the JVM for your large Confluence instance can have a huge impact on the performance perceived by the users. Between versions 1.4 and 6 of the Sun Java JVM there have been some impressive improvements in performance, especially under high concurrent load.

Here are some essential guidelines:

- Always run the most recent point release of your selected JVM.
- Where ever possible run the most recent major release from your selected JVM manufacturer. The Sun JVM version 6 is much faster than 1.4, especially under high loads.
- Tune your garbage collection algorithms. Experiment with different algorithms and settings to get the response times you desire in your environment. Here are some specific guidelines for Sun JVM in the Sun documentation:
  - Java 6
  - Java 5
  - Java 1.4

Customising Confluence to Optimise Performance

You may need to customise Confluence for performance reasons. Depending on your usage scenario, there may be ways to enhance Confluence performance that become necessary when you reach a certain level of usage.

Here are some things you might decide to do:

- Remove the display of the space list on the Dashboard. See Customising the Dashboard.
- Configure any search appliances or other crawlers which are configured to index the Confluence site:
  - These should be suitably rate limited.
  - Configure them to crawl only pages in the `/display/` URL path, and only current versions of pages.

Please refer to our general Performance Tuning page for more details.

Related Topics

Performance Tuning
Configuring a Large Confluence Installation
Confluence Clustering Overview
Requesting Performance Support
Confluence Administrator's Guide

Confluence Configuration Guide
Server Hardware Requirements Guide
Fix Out of Memory Errors by Increasing Available Memory

Performance Tuning

> This document describes tuning your application for improved performance. It is not a guide for troubleshooting Confluence outages. Check Troubleshooting Confluence Hanging or Crashing for help if Confluence is crashing. NEW: Garbage Collector Performance Issues

Description

Like any server application, Confluence may require some tuning as it is put under heavier use. We do our best to make sure Confluence performs well under a wide variety of circumstances, but there's no single configuration that is best for everyone's environment and usage patterns.

If you are having problems with the performance of Confluence and need our help resolving them, you should read Requesting Performance Support.

Use the latest version of your tools

Use the latest versions of your application servers and Java runtime environments. Newer versions are usually better optimized for performance. As an example, our internal performance tests show a **20% speed-up** (when viewing pages under load) between Tomcat 6 on Java 6 vs Tomcat 5.5 on Java 5 **out of the box**.

Avoid swapping due to not enough RAM

Always watch the swapping activity of your server. If there is not enough RAM available, your server may start swapping out some of Confluence's heap data to your hard disk. This will slow down the JVM's garbage collection considerably and affect Confluence's performance. In clustered installations, swapping can lead to a Cluster Panic due to Performance Problems. This is because swapping causes the JVM to pause during Garbage Collection, which in turn can break the inter-node communication required to keep the clustered nodes in sync.

On this page:

⚠ *The information on this page does not apply to Confluence OnDemand.*

Careful about those other systems using the same infrastructure

It may sound tempting: Just have one powerful server hosting your database and/or application server, and run **all** your crucial programs on that server. **If** the system is set up perfectly, then you might be fine. Chances are however that you are missing something, and then one application's bug might start affecting other applications. So if Confluence is slow every day around noon, then maybe this is because another application is using the shared database to generate complicated reports at that time? Either make sure applications can't harm each other despite sharing the same infrastructure, or get these systems untangled, for example by moving them to separate instances that can be controlled better.

Choice of Database

The **embedded database** that is provided with Confluence is meant only to be used for evaluation, not for production Confluence sites. After the evaluation finishes, you will certainly need to switch to an external relational database management system. Beyond this, we do not recommend any particular RDBMS over another. We recommend using what you are familiar with, because your ability to maintain the database will probably make far more difference to what you get out of it than the choice of database itself.

Database Connection Pool

If load on Confluence is high, you may need more simultaneous connections to the database.

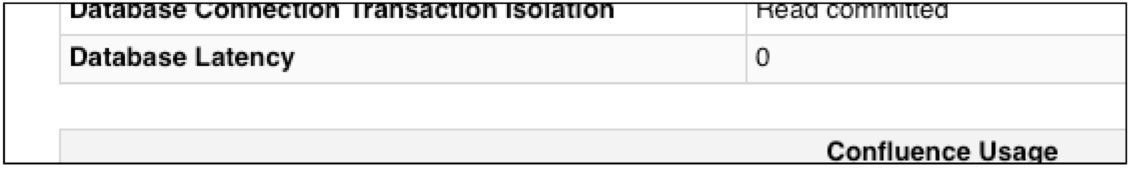
- If you are using JNDI data-sources, you will do this in your application server's configuration files.
- If you have configured Confluence to access the database directly, you will need to manually edit the hibernate.c3p0.max_size property in the confluence.cfg.xml file in your confluence.home directory. After you have changed the URL in this file, restart Confluence.

To assess whether you need to tune your database connection pool, take thread dumps during different times (including peak usage). Inspect how many threads have concurrent database connections.

Database in general

If Confluence is running slowly, one of the most likely cause is that there is some kind of bottleneck in (or around) the database.

The first item you should check is the **"Database Latency"** field in the System Information tab in the admin console.



Database Connection Transaction Isolation	Read committed
Database Latency	0
Confluence Usage	

The latency is calculated by sending a trivial request to the database, querying a table which is known to have only one column and one row. ("select * from CLUSTERSAFETY"). Obviously this query should be blazing fast, and return within 1 or 2 milliseconds. If the value displayed is between 3 and 5 milliseconds, you might already have an issue. If the value is above 10ms, then you **definitely** need to investigate and improve something! A few milliseconds may not sound so bad, but consider that Confluence sends quite a few database queries per page request, and those queries are a lot more complex too! High latency might stem from all sorts of problems (slow network, slow database, connection-pool contention, etc), so it's up to you to investigate. Don't stop improving until latency is below 2ms on average.

Obviously, latency is just the very first thing to look at. You may get zero latency and still have massive database problems, e.g. if your tables are poorly indexed. **So don't let a low latency fool you either.**

Database indexes

Especially if you have more than a few thousand active users, and all most obvious measures have been tried out but the database still seems to be under high load, you should consider engaging a database administrator (DBA) to tune the database specifically to the demands that your particular Confluence installation is placing on it. If you do not have a full-time DBA and can't even get one for temporary consulting, you may want to consult the database indexing advice that we have been gathering from customer reports and our own experience running and developing Confluence. The instructions on that page are for Oracle, but most of the indexes can be applied to (and will help with) any database.

(These database indexes are now created automatically when Confluence is installed, but existing installations upgrading to a more recent version may still need to add them manually)

Database Statistics and Query Analysers

Modern databases have query optimisers based on collecting statistics on the current data. Using the SQL EXPLAIN statement will provide you information on how well the query optimiser is performing. If the cost estimate is wildly inaccurate then you will need to run statistics collection on the database. The exact command will depend on your database and version. In most cases you can run statistics collection while Confluence is running, but due to the increased load on the database it's best to do this after normal hours or on a week-end.

Cache Tuning

To reduce the load on the database, and speed up many operations, Confluence keeps its own cache of data. Tuning the size of this cache may speed up Confluence (if the caches are too small), or reduce memory (if the caches are too big).

Please have a look at our documentation on Cache Performance Tuning for information on how to tune Confluence caches.

Antivirus Software

Antivirus software greatly decreases the performance of Confluence. Antivirus software that intercepts access to the hard disk is particularly detrimental, and may even cause errors with Confluence. You should configure your antivirus software to ignore the Confluence home directory, its index directory and any database-related directories.

Enabling HTTP Compression

If bandwidth is responsible for bottlenecking in your Confluence installation, you should consider enabling HTTP compression. This may also be useful when running an external facing instance to reduce your bandwidth costs. ⚠ Take note of the known issues with HTTP compression in versions of Confluence prior to 2.8, which may result in high memory consumption.

Virtual Operating Systems

Virtual Environments such as VMWare can cause Confluence CPU to spike. Run Confluence on a native OS. Refer to the list of supported operating systems for Confluence in the Supported Platforms topic.

⚠ In some situation the VMTools can crash, cause a excessive context switches and interrupts causing the JVM to run slowly and Confluence to start up very slowly.

Performance Testing

You should try out all configuration changes on a demo system. Ideally, you should run and customize loadtests that simulate user behaviour. Learn about how to test performance issues using the Performance Testing Scripts .

Access logs

You can find out which pages are slow and which users are accessing them by enabling Confluence's built-in access logging.

Built-in Profiler

You can identify the cause of page delays using Confluence's built-in profiler according to Troubleshooting Slow Performance Using Page Request Profiling.

Adjust Application Server Memory Settings

See Fix Out of Memory Errors by Increasing Available Memory.

Use A Web Server

For high-load environments, performance can be improved by using a web server such as Apache in front of the application server. There is a configuration guide to Running Confluence behind Apache.

When configuring your new web server, make sure you configure sufficient threads/processes to handle the load. This applies to both the web server and the application server connector, which are typically configured separately. If possible, you should enable connection pooling in your web server connections to the application server.

Parallel GC

If you have multiple CPU's on your server, you can add -XX:+UseParallelOldGC to your JAVA_OPTS options. This will allow garbage collection of the Tenured Space to happen in parallel with the application and can boost performance and can reduce slow performance spikes. For more information, please refer to our detailed page on Garbage Collector Performance Issues, and Sun's summary of collectors.

Troubleshoot possible memory leaks

Some external plugins, usually ones that have been written a long time ago and that are not actively maintained anymore, have been reported to consume memory and never return it. Ultimately this can lead to a crash, but first this manifests as reduced performance. The Troubleshooting Confluence Hanging or Crashing guide is a good place to start. Some of the known causes listed there could result in performance issues short of a crash or hang.

Some 3rd-party plugins were not written to scale to large enterprises' needs

Confluence has been optimized to work under high load and with many pages. Some 3rd party plugins however have been written with small size companies in mind, and can't cope with large numbers of concurrent users, or large numbers of pages and permissions, or large numbers of spaces. It is impossible to tell which ones will fail under which conditions, but it will always help to turn off 3rd-party plugins that are not strictly mission-critical while investigating performance issues.

RELATED TOPICS

Garbage Collector Performance Issues
Cache Performance Tuning
Cache Performance Tuning for Specific Problems
Performance Testing Scripts
Working with Confluence Logs
Operating Large or Mission-Critical Confluence Installations
Confluence Clustering Overview
Requesting Performance Support
Confluence Administrator's Guide
Confluence Configuration Guide

Cache Performance Tuning

Confluence performance can be significantly affected by the performance of its caches. It is essential for the administrator of a large production installation of Confluence to tune the caches to suit its environment. There are several configurable parameters for each of the cache regions, most notably cache size, cache expiry delay and eviction policy. In the majority of the cases, cache size is the parameter you would want to change. Fortunately, from Confluence 3.0, it is very easy to adjust cache sizes through the Administration Console. However, if you need to modify parameters other than a cache size, you would need to modify the relevant configuration files manually.

> ℹ If you only need to modify Confluence's maximum cache sizes, you can do this through the Cache Statistics feature of the Administration Console.

The cache performance information for your Confluence installation is available under **Administration > Cache Statistics**. More information about the numbers displayed here is available on Cache Statistics.

On this page:

⚠ *The information on this page does not apply to Confluence OnDemand.*

Cache tuning example

As an example of how to tune Confluence's caches, let's have a look at the following table:

Caches	% Used	% Effectiveness	Objects/Size	Hit/Miss/Expiry
Attachments	87%	29%	874/1000	78226/189715/187530
Content Attachments	29%	9%	292/1000	4289/41012/20569
Content Bodies	98%	81%	987/1000	28717/6671/5522
Content Label Mappings	29%	20%	294/1000	4693/18185/9150
Database Queries	96%	54%	968/1000	105949/86889/83334
Object Properties	27%	18%	279/1000	5746/25386/8102
Page Comments	26%	11%	261/1000	2304/17178/8606
Users	98%	5%	982/1000	6561/115330/114279

The caches above are of size 1000 (meaning that it can contain up to 1000 objects), which is the default size for caches in the default cache scheme. Refer to Confluence Cache Schemes for more explanation.

You can tell when a cache size needs to be increased because the cache has both:

- a high usage percentage (above 75%)
- a low effectiveness percentage.

Check the 'effectiveness' versus the 'percent used'. A cache with a low percent used need not have its size lowered; it does not use more memory until the cache is filled.

Based on this, the sizes of the "Attachments", "Database Queries", and "Users" caches should be increased to improve their effectiveness.

As the stored information gets older or unused it will expire and be eliminated from the cache. Cache expiry may be based on time or on frequency of use.

There is not much that you can do with a cache that has both a low percentage of usage and effectiveness. Over time, as the cache is populated with more objects and repeat requests for them are made, the cache's effectiveness will increase.

Finding the configuration file

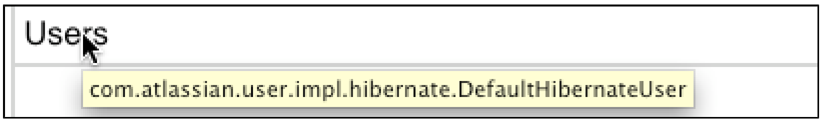
The caches are configured in `ehcache.xml` (for standard editions) or `confluence-coherence-cache-config-clustered.xml` (for clustered editions) which is stored in `<confluence-home>/config/`.

Oracle Coherence Licensing Change:

- Due to a license agreement change,Confluence is now available in two editions:
  - **Standard Edition** — Confluence with Ehcache's caching technology (available to customers with non-clustered Confluence licenses).
    ⚠ **If you are currently running a clustered installation of Confluence, please do not upgrade it with a standard edition of Confluence.**
  - **Clustered Edition** — Confluence with Oracle's Coherence clustering and distributed caching technology (available to customers with Confluence clustered licenses only).
- For more information about these changes, please refer to the Coherence License Changes document.
- If you have a Confluence clustered license, are running a clustered installation of Confluence and wish to upgrade to Confluence version 2.6 or later, please ensure that you download only a clustered edition of Confluence and please refer to the Confluence 3.0.1 Upgrade Notes for additional upgrade information.

Cache Key Mappings

The cache configuration file configures caches by their keys. When you move your mouse over the the cache names displayed on the cache statistics page, a tooltip will indicate the actual cache key for that cache name.



Users
com.atlassian.user.impl.hibernate.DefaultHibernateUser

Using our example from the table above, if we were to modify parameters for the `Users` cache we would need to change the cache with the key `com.atlassian.user.impl.hibernate.DefaultHibernateUser`. Do not get confused with `Users (External Mappings)` and `Users (External Groups)` which are in themselves, two separate caches. "Users" is the friendly name for `com.atlassian.user.impl.hibernate.DefaultHibernateUser`.

Standard Editions of Confluence

In standard editions of Confluence, the caching layer is Ehcache.

Understanding the Ehcache Configuration File

For more information about the Ehcache configuration file and a full reference on Ehcache configuration, please refer to the Ehcache configuration documentation.

Converting your Coherence configuration to Ehcache

> ⚠ This section only applies to customers who:
>
> - Have an installation of Confluence that was downloaded before the 4th of September 2009.
> - Intend to (or have already) upgraded to Confluence 3.0.1 or later (or to Confluence versions 2.6.3, 2.7.4, 2.8.3, 2.9.3 and 2.10.4).
> - Will use a non-clustered Confluence license for the Confluence upgrade.
> - Have implemented customisations to their Confluence installation's cache configuration file (`confluence-coherence-cache-config.xml`).

To maintain your existing cache configuration file settings, you will need to transfer any cache customisations you have implemented in the Coherence cache configuration file (`confluence-coherence-cache-config.xml`) to the relevant entries in the Ehcache cache configuration file (`ehcache.xml`).

Each cache has a `cache-mapping` element in the Coherence file (of which there is an equivalent `cache element` in the `ehcache.xml` file). Unfortunately, copying across your customisations is not quite a straightforward process because the Coherence file defines several 'caching schemes' to store the actual cache values, which in turn are referenced by the `cache-mapping` elements. In contrast, the `ehcache.xml` file does not support caching schemes and a cache's values are expressed explicitly in separate parameters of a `cache` element.

To convert your Coherence cache configuration file customisations across to the equivalent Ehcache file:

1. Open both the `confluence-coherence-cache-config.xml` and `ehcache.xml` files in a text editor. These files are located in the `<confluence-home>/config` directory.
   ℹ If you implemented your customisations in a version of Confluence prior to 3.0, you will most likely find the `confluence-coherence-cache-config.xml` file in the `<confluence-install>/confluence/WEB-INF/classes` directory.
2. In the customised `confluence-coherence-cache-config.xml` file:

   a. Identify the caching schemes that were customised in this file and make a note of the values of all its child elements.
      ℹ Typically, each caching scheme is located inside a `local-scheme` element and all of these are enclosed within the `cache-schemes` element, which appears towards the end of this file.
   b. Note each customised caching scheme by the content of its `scheme-name` element.
   c. For each `cache-mapping` element (which typically appears towards the top of this file), identify if it has a `scheme-name` element whose content matches one noted in the previous step and if so, make a note of its associated `cache-name` element.
3. In the `ehcache.xml` file:

   a. Identify each `cache` element whose 'name' parameter matches the `cache-name` elements noted in step '2c'.
   b. Using the mappings table below, apply the values noted in step '2a' to the appropriate parameters of the `cache` elements identified in the previous step ('3a').

Mappings table showing how elements of the Coherence cache configuration file map to parameters of the equivalent Ehcache file.

Coherence Element	Ehcache Attribute
`high-units`	`maxElementsInMemory`

`expiry-delay` > 0s	`timeToIdleSeconds` - Use this attribute for expiry delays greater than 0s along with the `eternal` attribute set to 'false'
`expiry-delay` = 0s	`eternal` - For expiry delays of 0s, set this attribute to 'true'.

Clustered Editions of Confluence

Understanding the Coherence configuration file

The Coherence configuration file is a mapping of *cache keys* to *cache schemes*. Each cache scheme controls the expiry, eviction policy and size of the caches linked to it. A cache scheme can extend another scheme.

For a full reference, see the Oracle's Coherence cache configuration documentation.

Defining Caching Scheme Mappings in Coherence Cache config file

If a cache key does not have an explicit definition in the caching scheme mappings (defined in `confluence-coherence-cache-config.xml`) then it will use the "default" `cache-mapping`.

In our example, `com.atlassian.user.impl.hibernate.DefaultHibernateUser` is not explicitly defined in the caching scheme mappings. Hence to increase the expiry-delay to 2 hours, we will need to define the mapping ourselves and add the following within the `<caching-scheme-mapping>...</caching-scheme-mapping>` tags:

```
<cache-mapping>
<cache-name>com.atlassian.user.impl.hibernate.DefaultHibernateUser</cache-name>
<scheme-name>cache:com.atlassian.user.impl.hibernate.DefaultHibernateUser</scheme-name>
</cache-mapping>
```

Then we will need to define a cache schema with name `cache:com.atlassian.user.impl.hibernate.DefaultHibernateUser` within `<caching-schemes>...</caching-schemes>` tags.

```
<local-scheme>
<scheme-name>cache:com.atlassian.user.impl.hibernate.DefaultHibernateUser</scheme-name>
<scheme-ref>default</scheme-ref>
<high-units>10000</high-units>
<expiry-delay>7200</expiry-delay>
</local-scheme>
```

It's possible to define a local-scheme mapping for a cache key without defining certain parameters (e.g. `<high-units>`). In such a cases, their parameters will be inherited from `scheme-ref` scheme, which is the `default` scheme in our case.

Important Caches

> The following suggestions are general guidelines. In cases of large databases, 20-30% of the size of the table may be unnecessarily large. Check the effectiveness and Percent Used categories in the cache for more specific assessments.

- **`com.atlassian.confluence.core.ContentEntityObject`** (known as **`Content Objects`** cache) should be set to at least 20-30% of the number of content entity objects (pages, comments, emails, news items) in your system. To find the number of content entity objects, use the query `select count(*) from CONTENT where prevver is null`.
- **`com.atlassian.confluence.core.ContentEntityObject.bodyContents`** (known as **`Content Body Mappings`** cache)
  should be set to at least 20% of the number of content entity objects (pages, comments, emails, news items) in your system. To find the number of content entity objects, use the query `select count(*) from CONTENT where prevver is null`.
- **`com.atlassian.confluence.security.PermissionCheckDispatcher.isPermitted()`** (known as **`User Authorized URLs`** cache)
  should be set to at least the number of concurrent users you expect to access Confluence at the same time
- **`com.atlassian.user.impl.hibernate.DefaultHibernateUser`** (known as **`Users`** cache) should be set to the number of users you have: `select count (*) from users`. Note that by default, this will also control the LDAP user's cache, including expiration.
- **`com.atlassian.confluence.security.SpacePermission`** (known as **`Permissions`** cache) should be set to the number of space permissions in your deployment (a good rule of thumb is 20 times the number of spaces). You can find the number of space permissions using the query `select count(*) from SPACEPERMISSIONS`.

Cache Tuning Follow-Up

After you have made changes to your cache config, doing a follow up on the changes in the next week or after the expected performance spike would be important.

Make sure that you take a screenshot of the cache statistics before and after the change. Then compare them with the cache statistics in the later period where performance improvement is expected.

> You can monitor what's in the cache by using a JSP included in the Confluence distribution. Browse to <base-URL>/admin/cachecontents.jsp to monitor the cache contents.

RELATED TOPICS

Cache Performance Tuning for Specific Problems
Confluence Cache Schemes
Performance Testing Scripts
Working with Confluence Logs
Operating Large or Mission-Critical Confluence Installations
Confluence Clustering Overview
Requesting Performance Support
Confluence Administrator's Guide
Confluence Configuration Guide

Cache Performance Tuning for Specific Problems

The following are more specific performance problems that can be resolved from tuning the cache.

LDAP cache sizes and expiry does not appear to be picked up.

This is a known problem, please refer to CONF-11858 for the solution.

> *The information on this page does not apply to Confluence OnDemand.*

"Edit Page" screen takes a long time to load

If your installation of Confluence is suffering from this problem, it may be due to a insufficient SpacePermissions cache size. To address this problem, first determine the number of space permission objects in your Confluence instance. You can do this by running this query against your database:

```
> select count(*) from SPACEPERMISSIONS
```

Now locate the cache entry for SpacePermissions in your `confluence-coherence-cache-config.xml`:

```
<local-scheme>

<scheme-name>cache:com.atlassian.confluence.security.CachingSpacePermissionManager.permissions</scheme-name>
        <scheme-ref>default</scheme-ref>
        <high-units>10000</high-units>
        <expiry-delay>0s</expiry-delay>
</local-scheme>
```

Adjust the **maxElementsInMemory** or **high-units** property to the number of space permissions you have (in the example above, I've used 10000). Also, just as important, you need to adjust the **timeToLiveSeconds** or **expiry-delay** property to `0`.

Note: 10K of space permissions consumes approximately 8MB of memory. Please ensure there is enough memory allocated to your instance to cater for this.

How to set specific cache settings

1. Find the cache name from the cache name mappings:
   - For **Confluence 2.5.x and earlier**, the cache name mappings are in file `confluence/WEB-INF/classes/com/atlassian/confluence/admin/actions/cache-name-mappings.properties`.
   - For **Confluence 2.6.0 and later**, you will find the cache name mappings in the file `com/atlassian/confluence/core/ConfluenceActionSupport.properties` which is packed into the `confluence-2.x.*.jar file`.
2. Find the appropriate `<cache-mapping>` tag in `confluence-coherence-cache-config.xml` or `confluence-coherence-cache-config-clustered.xml`. If the tag doesn't exist, you can create it within the `<caching-scheme-mapping>`tag.

   > ⚠ Attached to this page are corrected copies of confluence-coherence-cache-config.xml and confluence-coherence-cache-config-clustered.xml. These are updated from a bug CONF-11857.

3. The `<scheme-name>` will correspond to a `<local-scheme>`tag below. It refers to a scheme reference. Either change the high-units tag in the scheme reference, or add a high-units tag to override the scheme reference. For example, the following tag would change the Content Bodies cache from the default 1000 units to 2000 units:

```
<local-scheme>
<scheme-name>cache:com.atlassian.confluence.core.ContentEntityObject.bodyContents</scheme-name>
<high-units>2000</high-units>
<scheme-ref>default</scheme-ref>
<expiry-delay>0s</expiry-delay>
</local-scheme>
```

Another popular cache to change is the LDAP related User cache:

```
<local-scheme>
<scheme-name>user</scheme-name>
<scheme-ref>default</scheme-ref>
<high-units>5000</high-units>
<expiry-delay>300s</expiry-delay>
</local-scheme>
```

4. After updating the appropriate file, you do not need to repack it into the jar to use it. You can simply place the file in your `confluence/WEB-INF/classes/` directory. The file in this directory will override the settings in your jar file. If you want to back out the changes, you only need to remove the file from your `confluence/WEB-INF/classes/` directory — then the default values in the `confluence-coherence-cache-config.xml` located in your jar file will apply.

You can find more information about configuring the Coherence cache in the Coherence cache documentation.

RELATED TOPICS

Cache Performance Tuning
Performance Testing Scripts
Confluence Cache Schemes
Working with Confluence Logs
Operating Large or Mission-Critical Confluence Installations
Confluence Clustering Overview
Requesting Performance Support
Confluence Administrator's Guide
Confluence Configuration Guide

Confluence Cache Schemes

Default Scheme

If a cache has not been defined, then it will use the default cache size and expiry. As the start of your `confluence/WEB-INF/classes/confluence-coherence-cache-config.xml` file you will notice the following:

```
<cache-mapping>
  <cache-name>*</cache-name>
  <scheme-name>default</scheme-name>
</cache-mapping>
```

So basically all caches will default to using the default scheme, which is defined as below:

```
<!-- Default scheme -->
<local-scheme>
  <scheme-name>default</scheme-name>

<class-name>com.atlassian.confluence.cache.tangosol.ExpiryCountingLocalCache
</class-name>
  <high-units>1000</high-units>
  <expiry-delay>3600</expiry-delay>
</local-scheme>
```

I.e. with a size of 1000 Objects and an expiry of 3600 seconds. Other schemes use the above as their default and either override the size of the cache, or the length of the expiry.

> ⚠ *The information on this page does not apply to Confluence OnDemand.*

Common Schemes

In addition to the default scheme, there are also common schemes used in Confluence caches:

```
<!-- Common schemes -->
<local-scheme>
  <scheme-name>large</scheme-name>
  <scheme-ref>default</scheme-ref>
  <high-units>10000</high-units>
</local-scheme>
<local-scheme>
  <scheme-name>medium</scheme-name>
  <scheme-ref>default</scheme-ref>
  <high-units>5000</high-units>
</local-scheme>
<local-scheme>
  <scheme-name>small</scheme-name>
  <scheme-ref>default</scheme-ref>
  <high-units>100</high-units>
</local-scheme>
<local-scheme>

<scheme-name>large-transient</scheme-name>
  <scheme-ref>default</scheme-ref>
  <high-units>10000</high-units>
  <expiry-delay>300s</expiry-delay>
</local-scheme>
<local-scheme>
  <scheme-name>user</scheme-name>
  <scheme-ref>default</scheme-ref>
  <high-units>5000</high-units>
  <expiry-delay>300s</expiry-delay>
</local-scheme>
```

RELATED TOPICS

Cache Performance Tuning

Confluence Cache Schemes
Cache Performance Tuning for Specific Problems
Requesting Performance Support
Confluence Administrator's Guide
Confluence Configuration Guide

Memory usage and requirements

Managing Confluence's performance and memory usage really depends on what resources are available - Confluence will run faster if you give it lots of memory for its caches, but it should still be able to run quite well in low-memory environments, with the right tuning. Below are some tips on getting the most out of your Confluence site.

On this page:

⚠ *The information on this page does not apply to Confluence OnDemand.*

Increasing the amount of memory available to Confluence

See Increasing JIRA Memory for details on how to increase the memory available to web application servers typically used to run Confluence.

Embedded Database

The embedded HSQL database that comes with Confluence essentially holds all your data in memory while the Confluence server is running. If you are running out of memory, you should consider migrating Confluence to some external RDBMS.

Caching

By default, Confluence keeps large in-memory caches of data to improve its responsiveness and the user experience. The trade off is an increase in memory requirements to support the cache. Administrators of larger Confluence sites may need to configure the size of their caches to improve performance.

To customise Confluence's cache to meet your needs, see cache tuning.
To increase the amount of memory available to confluence, see Fix Out of Memory Errors by Increasing Available Memory.

Mail error queue

Confluence keeps a copy of all emails that it failed to send within an internal error queue. In the event of intermittent failures such as network connectivity issues, the emails in this queue can be manually resent when the problem is fixed. Under certain circumstances, the mail queue can fill up with large objects. The queue is regularly flushed, but if you get a *lot* of mail errors, you might get a spike in memory usage.

Attachments

The indexing of large attachments requires that the attachment be loaded into memory. In the case of large attachments, this can cause a temporary strain on the systems resources, and may result in indexing failing because the attachment could not be fully loaded into memory.

System backup / restore

The Confluence backup and restore process scales linearly with the size of data. This can have a significant impact on large Confluence instances where the amount of data exceeds the amount of available memory. If you are experiencing an `OutOfMemoryError` during either a backup or restore processes, then we strongly recommend that you choose and Production Backup Strategy.

If you encounter an `OutOfMemoryError` while restoring a backup and wish to overcome this issue by increasing memory, how much more will you need to make this process work? A good rule of thumb is to have a look at the size of the `entities.xml` file in your backup. This file contains all of the data Confluence will be loading, so at least that much is required. Add another 64-128Mb to ensure that Confluence has enough memory to load and function and that should be enough. To increase the amount of memory available to Confluence, see Fix Out of Memory Errors by Increasing Available Memory.

Known issues that we do not have control over.

There are also some memory issues we don't have any control over. For example,

- There's a memory leak in the Oracle 10g JDBC drivers. Not much we can do about that.
- one customer found a rather nasty memory leak that appeared to originate inside Tomcat 5, but only using the IBM JDK on PowerPC.

If you are having problems that appear to result from a memory leak, file an issue on http://support.atlassian.com . Our memory profiler of choice is YourKit. It would be helpful to us if you can provide us with a memory dump from that tool showing the leak.

Confluence is taking long periods of time to respond to some actions

A common cause of random pauses in Confluence is the JVM running garbage collection. To determine if this is what is happening, enable verbose garbage collection and look at how long Java is taking to free up memory. If the random pauses match when Java is running its garbage collection, garbage collection is the cause of the pause.

Verbose garbage collection will generate log statements that indicate when Java is collecting garbage, how long it takes, and how much memory has been freed.

To enable gc logging, start Confluence with the option `-XX:+PrintGCDetails -XX:+PrintGCTimeStamps -verbose:gc -Xloggc:gc.log`. Replace `gc.log` with an absolute path to a `gc.log` file.

For example, with a Windows service, run:

```
tomcat5 //US//Confluence
++JvmOptions="-XX:+PrintGCDetails
-XX:+PrintGCTimeStamps -verbose:gc
-Xloggc:c:\confluence\logs\gc.log"
```

or in `bin/setenv.sh`, set:

```
export CATALINA_OPTS="$CATALINA_OPTS
-XX:+PrintGCDetails -XX:+PrintGCTimeStamps
-verbose:gc
-Xloggc:${CATALINA_BASE}/logs/gc.log"
```

If you modify `bin/setenv.sh`, you will need to restart Confluence for the changes to take effect.

What can you do to minimise the time taken to handle the garbage collection? See http://java.sun.com/docs/hotspot/gc1.4.2/ for details on tuning the JVM to minimise the impact that garbage collection has on the running application.

Requesting Performance Support

Basic Performance Troubleshooting Steps

Begin with the following procedures:

1. Go through the Troubleshooting Confluence Hanging or Crashing page to identify the major known performance problems
2. Proceed with the Performance Tuning tips to help optimize performance

> ⚠ *The information on this page does not apply to Confluence OnDemand.*

Requesting Basic Performance Support

If those tips don't help or you're not sure where to start, open a support ticket starting with at least the basic information:

1. The atlassian-confluence.log
2. The catalina.out log (or your application server log), with a series of three thread dumps separated by 10 seconds
3. A description with as much detail as possible regarding:
   a. What changes have been made to the system?
   b. When did performance problems begin?
   c. When in the day do performance issues occur?
   d. What pages or operations experience performance issues?
   e. Is there a pattern?

Continue with as much of the Advanced Performance Troubleshooting information as you can.

Advanced Performance Troubleshooting

Please gather **all** of the information listed below and include it in your support request, even if you think you have a good idea what's causing the problem. That way we don't have to ask for it later.

System Information

Confluence Server

- Take a screenshot of Confluence's `Administration  System Information` (or save the page as

HTML)
- Take a screenshot of Confluence's `Administration  Cache Statistics` (or save the page as HTML)
- Find out the exact hardware Confluence is running on
  - How many CPUs? What make and model? What MHz?
  - How much memory is installed on the machine?
  - How much memory is assigned to Confluence's JVM? (i.e. what are the -Xmx and -Xms settings for the JVM?)
  - What other applications are being hosted on the same box?

Confluence Content

- How many *users* are registered in Confluence?
- On average, to how many *groups* does each user belong?
- How many *spaces* (global and personal) are there in your Confluence server?
- How many of those spaces would be viewable by the average user?
- Approximately how many *pages*? (Connect to your database and perform '`select count(*) from content where prevver is null and contenttype = 'PAGE'`')
- How much data is being stored in Bandana (where plugins usually store data)? (Connect to your database and perform '`select count(*), sum(length(bandanavalue)) from bandana`')

The Database

- What is the exact version number of Confluence's database server?
- What is the exact version number of the JDBC drivers being used to access it? (For some databases, the full filename of the driver JAR file will suffice)
- Is the database being hosted on the same server as Confluence?
- If it is on a different server, what is the network latency between Confluence and the database?
- What are the database connection details? How big is the connection pool? If you are using the standard configuration this information will be in your confluence_cfg.xml file. Collect this file. If you are using a Data source this information will be stored in your application server's configuration file, collect this data.

User Management

- Are you using external user management or authentication? (i.e. JIRA or LDAP user delegation, or single sign-on)
- If you are using external JIRA user management, what is the latency between Confluence and JIRA's database server?
- If you are using LDAP user management:
  - What version of which LDAP server are you using?
  - What is the latency between Confluence and the LDAP server?

Diagnostics

Observed Problems

- Which pages are slow to load?
  - If it is a specific wiki page, attach the wiki source-code for that page
- Are they always slow to load, or is the slowness intermittent?

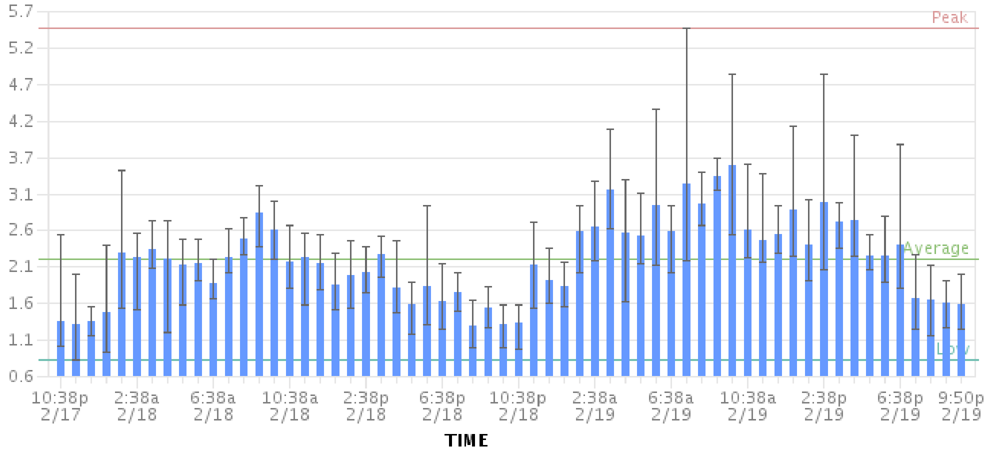
Monitoring data

Before drilling down into individual problems, helps a lot to understand the nature of the performance problem. Do we deal with sudden spikes of load, or is it a slowly growing load, or maybe a load that follows a certain pattern (daily, weekly, maybe even monthly) that only on certain occasions exceeds critical thresholds? It helps a lot to have access to continuous monitoring data available to get a rough overview.

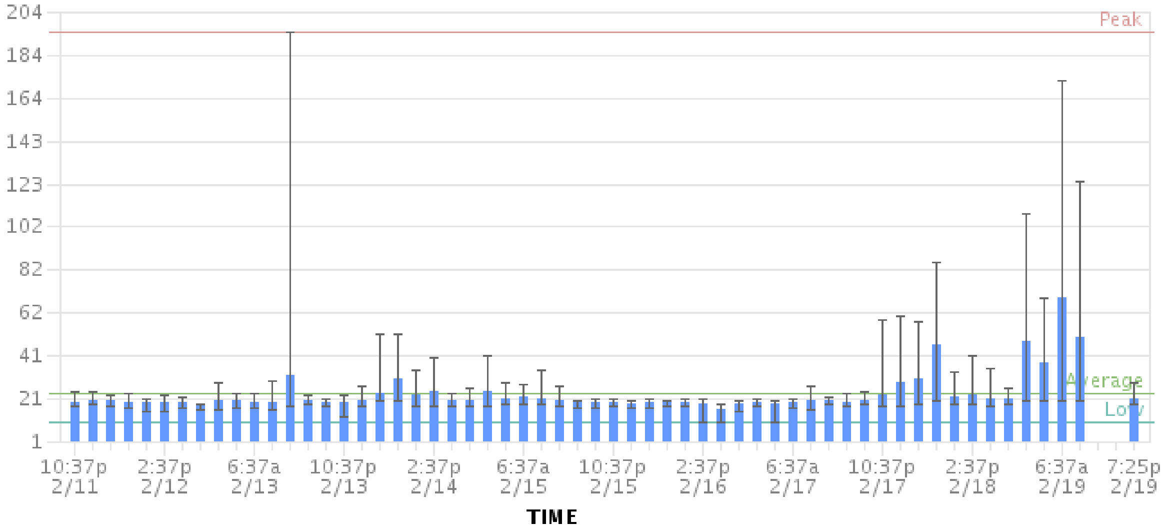
Here are sample graphs from the confluence.atlassian.com system, showing

Load

This graph shows the load for two consecutive days. The obvious pattern is that the machine is under decent load, which corresponds to the user activity, and there is no major problem.

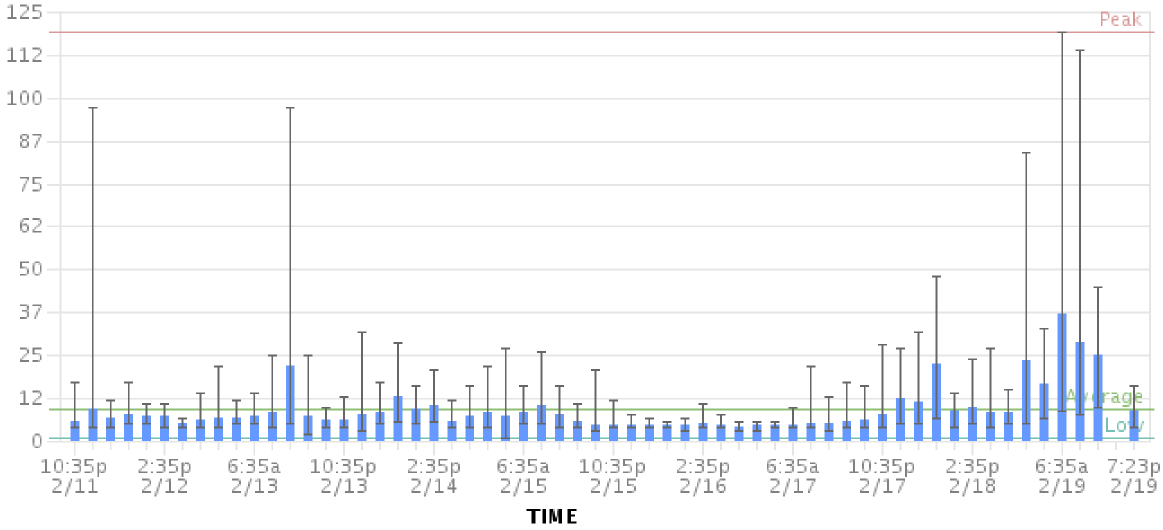


Resin Threads and Database Connections



Active number of Java Threads

These two charts show the active threads in the application server (first chart) and the size database connectio pool (second chart). As you can see, there was a sudden spike of server threads and a corresponding spike of db-connections.



The database connection pool size

The database connection pool size peaked over 112, which happened to be more than the maximum number c connections the database was configured for (100). So it was no surprise that some requests to Confluence failed and many users thought it had crashed, since many requests could not obtain the crucial database connections.

We were able to identify this configuration problem quite easily just by looking at those charts. The next spikes were uncritical because more database connections were enabled.

The bottom line being: it helps a lot to monitor your Confluence systems continuously (we use Hyperic, for example), and it helps even more if you are able to send us graphs when you encounter problems.

Access logs

- How to audit Confluence - enabling user access logging, including redirecting the logs to a separate file
  - You can run this file through a log file analyser such as AWStats, or manually look through for pages which are slow to load.

Profiling and Logs

- Enable Confluence's built-in profiling for long enough to demonstrate the performance problem using Troubleshooting Slow Performance Using Page Request Profiling.
  - If a single page is reliably slow, you should make several requests to that page
  - If the performance problem is intermittent, or is just a general slowness, leave profiling enabled for thirty minutes to an hour to get a good sample of profiling times
- Find Confluence's standard output logs (which will include the profiling data above). Take a zip of the entire logs directory.
- Take a thread dump during times of poor performance

CPU Load

- If you are experiencing high CPU load, please install the YourKit profile and attach two profiler dumps taken during a CPU spike. If the CPU spikes are long enough, please take the profiles 30-60 seconds apart. The most common cause for CPU spikes is a virtual machine operating system.
- If the CPU is spiking to 100%, try Live Monitoring Using the JMX Interface, in particular with the Top threads plugin.

Instance Metrics and Scripts

- It is essential to understand the user access and usage of your instance. Please use the access log scripts and sql scripts to generate Usage statistics for your instance.

Next Step

Open a ticket on https://support.atlassian.com and attach all the data you have collected. This should give us the information we need to track down the source of your performance problems and suggest a solution. Please follow the progress of your enquiry on the support ticket you have created.

If your site is non-responsive, please use our Live Support during business hours once you have created the ticket to escalate your problem.

Access Log Scripts

The access log scripts are attached to this page. To use the scripts:

1. Unzip the 7z file.
2. Copy all the daily access logs to a folder called `logs`.
3. Run `Atlassian-processDailyLog.rb`. This will generate a `csv` file called `summary.csv` and several directories which contain the access logs of each defined user action.
4. Run the appropriate script `Atlassian-processDailyLog-hourly.rb <admin/comment/create/edit/search/rss>`. Each script will generate a different `csv` file. For example, `Atlassian-processDailyLog-hourly.rb admin` will process the admin logs extracted in step 3.
5. Import the `csv` files to `www-log-Analysis.xls` (`summary.csv` to 'raw stats - daily' sheet and `admin.csv` to 'admin -hours' sheet, etc) to generate the load profiles and graphs. You may need to modify the number of rows in each sheet depending on the number of logs.

⚠ *The information on this page does not apply to Confluence OnDemand.*

Note

All scripts are written in Ruby and assume the log file name contains the string 'confluence.atlassian.com-access.log'. Scripts need to be changed if another name is used. Modify the line: `filenameRegexp = Regexp.new('confluence.atlassian.com-access.log')`

Troubleshooting Slow Performance Using Page Request Profiling

This page tells you how to enable page-request profiling. With profiling turned on, you will see a record of the time it takes (in milliseconds) to complete each action made on any Confluence page. If Confluence is responding slowly, an internal timing trace of the slow page request can help to identify the cause of the delay.

You will need access to the Confluence server to view a profile.

On this page:

⚠ *The information on this page does not apply to Confluence OnDemand.*

Enabling Page-Request Profiling

✓ To see just the slow performing macros, see Identifying Slow Performing Macros.

From **Confluence 2.7**, you can use the '**Logging and Profiling**' option to enable or disable profiling.

ⓘ You need to have System Administrator permissions in order to perform this function.

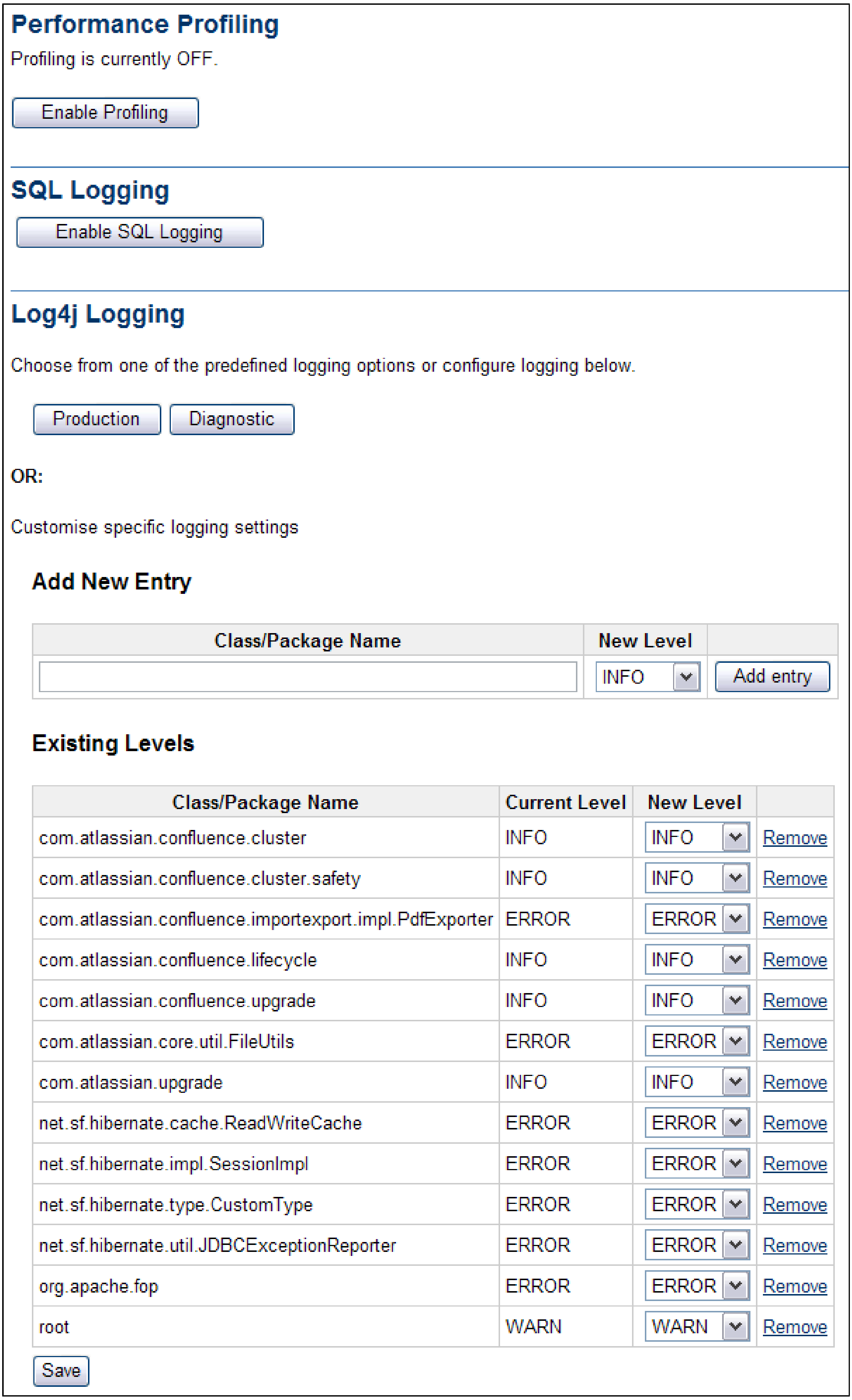
To enable page profiling,

1. Go to the '**Administration Console**' and click '**Logging and Profiling**' in the '**Administration**' section of the left-hand panel.
2. The '**Logging and Profiling**' screen appears. Click the '**Enable Profiling**' button.
   ⓘ If profiling is already enabled, the button will be labelled 'Disable Profiling' instead.

To disable page profiling,

1. Go to the '**Administration Console**' and click '**Logging and Profiling**' in the '**Administration**' section of the left-hand panel.
2. The '**Logging and Profiling**' screen appears. Click the '**Disable Profiling**' button.
   ⓘ If profiling is already disabled, the button will be labelled 'Enable Profiling' instead.

Screenshot: Changing Log Levels and Profiling



Performance Profiling

Profiling is currently OFF.

SQL Logging

Log4j Logging

Choose from one of the predefined logging options or configure logging below.

OR:

Customise specific logging settings

Add New Entry

Class/Package Name	New Level	
	INFO	Add entry

Existing Levels

Class/Package Name	Current Level	New Level	
com.atlassian.confluence.cluster	INFO	INFO	Remove
com.atlassian.confluence.cluster.safety	INFO	INFO	Remove
com.atlassian.confluence.importexport.impl.PdfExporter	ERROR	ERROR	Remove
com.atlassian.confluence.lifecycle	INFO	INFO	Remove
com.atlassian.confluence.upgrade	INFO	INFO	Remove
com.atlassian.core.util.FileUtils	ERROR	ERROR	Remove
com.atlassian.upgrade	INFO	INFO	Remove
net.sf.hibernate.cache.ReadWriteCache	ERROR	ERROR	Remove
net.sf.hibernate.impl.SessionImpl	ERROR	ERROR	Remove
net.sf.hibernate.type.CustomType	ERROR	ERROR	Remove
net.sf.hibernate.util.JDBCExceptionReporter	ERROR	ERROR	Remove
org.apache.fop	ERROR	ERROR	Remove
root	WARN	WARN	Remove

Profiling an Activity

1. Enable profiling, using either of the methods described above.
   Profiles for every page hit, for all users, will now be logged to your application server's default logs until Confluence is restarted. Note that each time a user visits a link, a single profile is printed.
2. Confirm that profiles are being written to the Confluence log file — see Working with Confluence Logs for location of the log files and other details.
3. Perform the activity that is resulting in unusually slow response time.
4. Copy the profile for that action. When deciding which profiles to copy, look for the links that took a long time to respond. If a single page is slow, only that profile is necessary. If Confluence is generally or intermittently slow, copy all profiles logged during the slowdown until a reasonable sample has been collected.
5. If you were instructed to profile your instance by Atlassian technical support, attach all relevant profiles to your support ticket.
6. Turn profiling off again, using either of the methods described above.
7. Confirm that profiles are no longer being printed to the Confluence log file.

Example of a Profile

Below are the first few lines of a normal profile for accessing a page called Confluence Overview.

```
[344ms] - /display/ds/Confluence+Overview
  [313ms] - SiteMesh: parsePage:
http://localhost:8080/display/ds/Confluenc
e+Overview
    [313ms] - XW Interceptor: Before
defaultStack: /pages/viewpage.action
(ViewPageAction.execute())
      [0ms] -
SpaceAwareInterceptor.intercept()
      [16ms] -
PageAwareInterceptor.intercept()
        [0ms] - AOP: PageManager.getPage()
        [16ms] - AOP:
PermissionManager.hasPermission()
          [0ms] - AOP:
SpacePermissionManager.hasPermission()
          [16ms] - AOP:
SpacePermissionManager.hasPermission()
        [0ms] - AOP:
SpacePermissionManager.hasPermission()
      [0ms] - AOP:
SpacePermissionManager.hasPermission()
      [281ms] - XW Interceptor: After
defaultStack: /pages/viewpage.action
(ViewPageAction.execute())
        [281ms] - XW Interceptor: After
validatingStack: /pages/viewpage.action
(ViewPageAction.execute())
           ...
```

Start Confluence with Profiling Enabled

There may be some situations where you may wish to have Confluence profiling enabled during startup. This may be useful if you restart often and may forget to enable profiling for Support/Trouble-shooting purposes.

Edit the file *CONFLUENCE_HOME\confluence\WEB-INF\web.xml*. You should see a stanza similar to the one below. Set the parameter value for **autostart** to **true**:

```
<filter>

<filter-name>profiling</filter-name>

<filter-class>com.atlassian.core.filters.P
rofilingAndErrorFilter</filter-class>
        <init-param>
            <!-- specify the which HTTP
parameter to use to turn the filter on or
off -->
            <!-- if not specified -
defaults to "profile.filter" -->

<param-name>activate.param</param-name>

<param-value>profile</param-value>
        </init-param>
        <init-param>
            <!-- specify the whether to
start the filter automatically -->
            <!-- if not specified -
defaults to "true" -->

<param-name>autostart</param-name>

<param-value>true</param-value>
        </init-param>
    </filter>
```

Remember to turn it back to **false** or your logs will grow very large.

RELATED TOPICS

Requesting Performance Support
Working with Confluence Logs

Compressing an HTTP Response within Confluence

Confluence supports HTTP GZip transfer encoding. This means that if a user's web browser supports it, Confluence will compress the data it sends to the user. This will speed up Confluence over slow or congested Internet links, and reduce the amount of bandwidth consumed by a Confluence server.

ℹ Gzipping the HTTP Response is available in Confluence 1.4 and later.

You should turn on Confluence's GZip encoding if:

- Users are accessing Confluence over the Internet, or a WAN connection with limited bandwidth.
- You wish to reduce the amount of data transfer between the Confluence server and client.

If you are accessing Confluence over a Local Area Network or over a particularly fast WAN, you may wish to leave GZip encoding disabled. If the network is fast enough that transferring data from Confluence to the user isn't a limiting factor, the additional CPU load caused by having to compress each HTTP response may in fact slow Confluence down.

⚠ *The information on this page does not apply to Confluence OnDemand.*

⛔ **Known issues in Confluence 2.7 and earlier**

There are known issues with the GZip filter and memory consumption evident in versions 2.7 of Confluence and earlier (CONF-9930). If you are running a large instance of Confluence 2.7 or earlier and frequently experiencing 'out of memory' errors, we recommend that you do not enable HTTP compression. These issues have been resolved in Confluence 2.8.

Enabling HTTP Compression

1. Choose **Browse** > **Confluence Admin**.
2. Select '**General Configuration**' in the left-hand panel.
3. Enable '**Compress HTTP Responses**'.

In Confluence 2.8 and later, you can configure which types of content are compressed within Confluence. By default, the following mime types will be compressed:

- text/htmltext
- javascript
- text/css
- text/plain
- application/x-javascript
- application/javascript

If you wish to change the types of content to be compressed, add a replacement `urlrewrite-gzip-default.xml` file within the `WEB-INF/classes/com/atlassian/gzipfilter/` directory in your Confluence Installation Directory. A sample file is provided as an attachment. Generally speaking, it is unlikely that you will need to alter this file.

RELATED TOPICS

Performance Tuning
Confluence Administrator's Guide

Performance Testing Scripts

Load Testing Confluence

This page contains scripts and hints on load-testing your Confluence installations.

Introduction

Before making a new Confluence instance available to your users it is useful to get a feel for how it will perform under your anticipated load and where you may need to consider improving your configuration to remove bottlenecks. Likewise, before making changes to your Confluence instance it would again be useful to assess the impact of these changes before making them live in a production context.

This kind of testing is not an exact science but the tools and process described here are intended to be a straightforward, configurable and extensible way of allowing you to begin this kind of load testing.

It will rarely be the case that these scripts will perform representative testing for you 'out of the box'. But either through configuration or by extending the scripts it should be possible to build an appropriate load test.

Load testing scripts are not designed for a production environment

The load testing scripts will update the data within the targeted Confluence instance and are not designed to be run against a production server. If you want to load test your production environment you will need to perform these tests on a backup of your data and restore your real data after the tests.

On this page:

⚠ *The information on this page does not apply to Confluence OnDemand.*

Setup

You will need the following -

- A Confluence server, set up and running with an admin user. The scripts assume a default username and password for this user: 'admin'/'admin'.
- Ensure the Confluence Remote API is enabled in the administration options. See Enabling the Remote API for details on how to configure this.
- Apache JMeter
- The load testing scripts and resources which are available in our public Maven repository — Please choose the version that most closely matches your Confluence version and download the ZIP or Gzip file in that directory. If in doubt, download the ZIP file archive.

> Users have reported problems when using the Windows built-in unzip utility. Please use a third party file archiving and extraction program (for example, 7-Zip) to extract these performance tests.

The test scripts have been updated to work with Confluence 3.4 in version 3.4. Using an older version of the tests will result in errors when running the test.

Quick, Just Tell Me How To Run It.

If you don't want to read the rest of this document, here are the main points:

1. Download and Unzip the performance tests
2. Open a command prompt and change directory to the `performanceTest` directory that has just been unzipped.
3. Create the test data:

   ```
   <jmeter location>/bin/jmeter -n -t jmeter-test-setup.jmx
   -Jspace.zip=<path to a demo space ZIP file> -Jadmin.user=<username>
   -Jadmin.pass=<password>
   ```

4. Run the test:

   ```
   <jmeter location>/bin/jmeter -n -t jmeter-test-fixedload.jmx
   ```

The remainder of this document is just an elaboration of those two steps.

> For information on how to use JMeter please refer to the manual

Creating the Test Data

A known data set is required to run the testing against. By default this is the Confluence demo space (space key = DS) although this can be changed (more on this later). If you decide to use the Confluence demo space, ensure that the group "confluence-users" is able to update content in this space.

The script `jmeter-test-setup.jmx` is used to:

- create a set of users to be used in the test
- import the Confluence demo space for running tests against.

You should first ensure that you don't already have the demo space (key = DS) on your test instance. Delete it if you do.

Run the script from the `performanceTest` directory as follows:

```
<jmeter location>/bin/jmeter -n -t
jmeter-test-setup.jmx -Jspace.zip=<path to
a space export.zip>-Jadmin.user=<username>
-Jadmin.pass=<password>
```

Where:

- `<path to a space export.zip>` is the absolute path to the space export zip you want to be used in your testing. For example, the path to `demo-site.zip` as found in your Confluence distribution or source: `<confluence install>/confluence/WEB-INF/classes/com/atlassian/confluence/setup/demo-site.zip`
- `<username>` and `<password>` are the username and password for an admin user that is able to create Confluence users and to import spaces.

By default the setup process will create 250 users — 50 each of the following formats: tstreader<n>, tstcommentor<n>, tsteditor<n>, tstcreator<n> and tstsearcher<n>. The password for each matches the username.

A typical run of the setup script will only take a few seconds.

Removing the Test Data

You can reverse the effects of the setup script by setting the `remove.data` parameter to `true`, e.g.

```
<jmeter location>/bin/jmeter -n -t
jmeter-test-setup.jmx -Jremove.data=true
-Jadmin.user=<username>
-Jadmin.pass=<password>
```

Setup Script Parameters

You can modify the behaviour of the setup script via JMeter parameters. These are supplied on the command line in the form `-J<parameter name>=<parameter value>`.

Parameter	Default	Explanation
script.base	.	The absolute path to the script. Defaults to the current working directory.
space.zip	N/A	The absolute path to space export zip file to be imported as test data.

remove.data	false	Run the script in reverse — remove all test data.
admin.user	admin	The admin user name used to import data and create users.
admin.pass	admin	The password for the admin user.
confluence.context	confluence	The confluence webapp context.
confluence.host	localhost	The address or host name of the test instance.
confluence.port	8080	The port of the test instance.
space.key	ds	The space key for the space import that will be tested against.
space.setup	true	Control whether the test space will be created (or removed).
commentor.max	250	The number of users to be created for making comments.
creator.max	250	The number of users to be created for adding pages.
editor.max	250	The number of users to be created for editing existing pages.
reader.max	250	The number of users to be created for viewing existing pages.
searcher.max	250	The number of users to be created for performing searches.
resource.max	250	The number of users to be created for downloading site resources.
attachments.max	250	The number of users to be created for downloading attachments.

Setup Script Output

On the console you will see no obvious indication of success or otherwise. JMeter will output something similar to this:

```
Created the tree successfully
Starting the test @ Mon Apr 14 17:35:08
EST 2008 (1208158508222)
Tidying up ... @ Mon Apr 14 17:35:08 EST
2008 (1208158508928)
... end of run
```

The `scripts location/results` directory will contain the file `jmeter-result-setuptest.jtl`. There were failures or errors if there are any assertions in this file that have the value `true` for the failure or error element, e.g.

```
<assertionResult>
<name>Manage Users</name>
<failure>true</failure>
<error>false</error>
<failureMessage>Test failed: URL expected
to contain
/browseusers.action/</failureMessage>
</assertionResult>
```

Running the Test

The test script itself will put Confluence under a fixed load. Each thread group will attempt to do a certain amount of work for a prescribed period of time (30 minutes by default). This is by design so that load during test runs can accurately be compared against each other.

Execute the test as follows:

```
<jmeter location>/bin/jmeter -n -t
jmeter-test-fixedload.jmx
```

Where:
`<scripts location>` is the absolute path to where you extracted the scripts e.g. `/Users/YourName/Download/performanceTest`. This is needed for the script to find its external resources.

Test Behaviour

The test has a number of parameters to tweak its behaviour but generally speaking it has the rough format of:

- 5 groups of users - readers, commentors, searchers, editors and creators.
    - readers simply view a set of individual pages or browse space functionality.
    - commentors add comments to a set of pages.
    - searchers perform searches on a fixed set of keywords.
    - editors make small additions to the end of a set of pages.
    - creators add new pages to a particular space.
- Each individual user in each group will repeat for a fixed amount of time with a small pause between each request.

Note that there is **no execution of JavaScript** by the client. Keep this in mind if you use this test to gauge Confluence performance in a production environment.

There is also very little use of permissions in these tests. All data involved is accessible to all of the test users.

Test Script Parameters

You can modify the behaviour of the test script via JMeter parameters. These are supplied on the command line in the form `-J<parameter name>=<parameter value>`.

Parameter	**Default**	**Explanation**
script.base	.	The absolute path to the script. Defaults to the current working directory.
confluence.context	confluence	The confluence webapp context.
confluence.host	localhost	The address or host name of the test instance.
confluence.port	8080	The port of the test instance.
create.page.prefix	Nihilist	The title prefix for any created page e.g. Nihilist00001.
script.runtime	1800	The amount of time the script will run for in seconds.

Test Thread Parameters

Parameter	**Default**	**Explanation**
threads.reader	15	Number of readers.
pause.reader	2000	The approximate (within 500ms) millisecond pause between reader repeats.
threads.searcher	8	Number of searchers.

pause.searcher	2000	The approximate (within 500ms) millisecond pause between searcher repeats.
threads.creator	3	Number of page creators.
pause.creator	2000	The approximate (within 500ms) millisecond pause between creator repeats.
threads.editor	3	Number of page editors.
pause.editor	2000	The approximate (within 500ms) millisecond pause between editor repeats.
threads.commentor	4	Number of page commentors.
pause.commentor	2000	The approximate (within 500ms) millisecond pause between commentor repeats.

> In version 3.0 of the tests, it's now possible to control the percentage executions of certain actions. These percentages are defined in the "Thread Details" configuration screen.

So with the default parameters, you are emulating a load on Confluence of 33 concurrent users who will each be hitting the server approximately every 2 seconds (16 users per second).

23 of these users are read only (searchers or readers) and 10 of them are read/write — 11 read only users per second and 5 read/write users per second.

Test Script Output

During the run of the test script Jmeter will output progress to the console of the form:

```
Created the tree successfully
Starting the test @ Fri Apr 18 00:07:39
EST 2008 (1208441259523)
Display Summary Results During Run + 462
in 77.6s = 5.9/s Avg: 1564 Min: 18 Max:
33738 Err: 1 (0.22%)
Display Summary Results During Run + 1338
in 189.9s = 7.0/s Avg: 3596 Min: 24 Max:
34545 Err: 0 (0.00%)
Display Summary Results During Run = 1800
```

```
in 257.6s = 7.0/s Avg: 3074 Min: 18 Max:
34545 Err: 1 (0.06%)
Display Summary Results During Run + 1046
in 200.9s = 5.2/s Avg: 4529 Min: 40 Max:
50461 Err: 0 (0.00%)
Display Summary Results During Run = 2846
in 438.2s = 6.5/s Avg: 3609 Min: 18 Max:
50461 Err: 1 (0.04%)
Display Summary Results During Run + 677
in 201.2s = 3.4/s Avg: 6638 Min: 46 Max:
27636 Err: 0 (0.00%)
Display Summary Results During Run = 3523
in 618.1s = 5.7/s Avg: 4191 Min: 18 Max:
50461 Err: 1 (0.03%)
Display Summary Results During Run + 561
in 197.5s = 2.8/s Avg: 8326 Min: 171 Max:
39494 Err: 0 (0.00%)
Display Summary Results During Run = 4084
in 798.3s = 5.1/s Avg: 4759 Min: 18 Max:
50461 Err: 1 (0.02%)
Display Summary Results During Run + 555
in 199.2s = 2.8/s Avg: 8247 Min: 160 Max:
45270 Err: 0 (0.00%)
Display Summary Results During Run = 4639
```

```
in 978.0s = 4.7/s Avg: 5177 Min: 18 Max:
504
```

Garbage Collector Performance Issues

This document relates broadly to memory management with Oracle's Hotspot JVM. These are recommendations based on Support's successful experiences with customers and their large Confluence instances.

Please **do not** use the Concurrent Mark Sweep (CMS) Collector with Confluence, unless otherwise advised by Atlassian Support. It requires extensive manual tuning and testing, and is likely to result in degraded performance.

The information on this page does not apply to Confluence OnDemand.

Summary

1. Set the Young space up to 30-40% of the overall heap: `-XX:NewSize=<between 30% and 40% of your Xmx value, eg, 384m>`
2. Use a parallel collector: `-XX:+UseParallelOldGC` (make sure this is **Old** GC)
3. limit the Tomcat connector's spare thread counts to minimize impact
4. *effectively* disable explicit garbage collection triggered from distributed remote clients `-Dsun.rmi.dgc.client.gcInterval=900000 -Dsun.rmi.dgc.server.gcInterval=900000`
5. Disable remote clients from triggering a full GC event `-XX:+DisableExplicitGC`
6. set the minimum and maximum Xmx and Xms values as the same (eg. `-Xms1024m -Xmx1024m`) to discourage address map swapping
7. Turn on GC logging (add the flags `-verbose:gc -Xloggc:<full-path-to-log> -XX:+PrintGCTimeStamps -XX:+PrintGCDetails`) and submit the logs in a support ticket
   a. (Optional) You can enable date stamps: `-XX:+PrintGCDateStamps` This makes the logs easier to read via the naked eye, but may run into problems if you're trying to use third-party applications to view the GC logs.
8. Use Java 1.6
9. Read below if heap > 2G

See Configuring System Properties for how to add these properties to your environment.

Background

Performance problems in Confluence, and in rarer circumstances for JIRA, generally manifest themselves in either:

- frequent or infrequent periods of viciously sluggish responsiveness, which requires a manual restart, or, the application eventually and almost inexplicably recovers
- some event or action triggering a non-recoverable memory debt, which in turn envelops into an application-fatal death spiral (Eg. overhead GC collection limit reached, or Out-Of-Memory).
- generally consistent poor overall performance across all Confluence actions

There are a wealth of simple tips and tricks that can be applied to Confluence, that can have a significantly tangible benefit to the long-term stability, performance and responsiveness of the application.

On this page:

Why Bad Things Happen

Confluence can be thought of like a gel or a glue, a tool for bringing things together. Multiple applications, data-types, social networks and business requirements can be efficiently amalgamated, leading to more effective collaboration. The real beauty of Confluence, however, is its agility to mould itself into your organizations' DNA - your existing business and cultural processes, rather than the other way around - your organization having to adapt to how the software product works.

The flip side of this flexibility is having many competing demands placed on Confluence by its users. Historically, this is an extraordinarily broad and deep set of functions, that really, practically can't be predicted for individual use cases.

The best mechanism to protect the installation is to place Confluence on a foundation where it is fundamentally more *resilient* and able to react and cope with competing user requirements.

Appreciate how Confluence and the JAVA JVM use memory

The Java memory model is naive. Compared to a unix process, which has four *intensive* decades of development built into time-slicing, inter-process communication and intelligent deadlock avoidance, the Java thread model really only has 10 years at best under its belt. As it is also an interpreted language, particular idiosyncrasies of the chosen platform Confluence is running can also influence how the JRE reacts. As a result it is sometimes necessary to *tune* the jvm parameters to give it a "hint" about how it should behave.

There are circumstances whereby the Java JVM will take a mediocre option in respect to resource contention and allocation and struggle along with ofttimes highly impractical goals. For example, The JRE will be quite happy to perform at 5 or 10% of optimum capacity if it means overall application stability and integrity can be ensured. This often translates into periods of extreme sluggishness, which effectively means that the application isn't stable, and isn't integral (as it cannot be accessed).

This is mainly because Java shouldn't make assumptions on what kind of runtime behavior an application needs, but it's plain to see that the charter is to assume 'business-as-usual' for a wide range of scenarios and really only react in the case of dire circumstances.

Memory is contiguous

The Java memory model *requires* that memory be allocated in a *contiguous* block. This is because the heap has a number of side data structures which are indexed by a scaled offset (ie n*512 bytes) from the start of the heap. For example, updates to references on objects within the heap are tracked in these "side" data structures.

Consider the differences between:

1. Xms (the *allocated* portion of memory)
2. Xmx (the *reserved* portion of memory)

Allocated memory is fully backed, memory mapped physical *allocation* to the application. That application now owns that segment of memory.

Reserved memory (the difference between Xms and Xmx) is memory which is *reserved* for use, but not physically mapped (or backed) by memory. This means that, for example, in the 4G address space of a 32bit system, the *reserved* memory segment can be used by other applications, but, because Java requires *contiguous* memory, if the *reserved* memory requested is occupied the OS must swap that memory out of the reserved space either to another non-used segment, or, more painfully, it must swap to disk.

Permanent Generation memory is also contiguous. The net effect is even if the system has vast quantities of *cumulative* free memory, Confluence demands *contiguous* blocks, and consequently undesirable swapping may occur if segments of requested size do not exist. See Causes of OutOfMemoryErrors for more details.

Please be sure to position Confluence within a server environment that can successfully complete competing requirements (operating system, contiguous memory, other applications, swap, and Confluence itself).

Figure out which (default) collector implementation your vendor is using

Default JVM Vendor implementations are subtly different, but in production can differ enormously.

The Oracle JVM *by default* splits the heap into three *spaces*

1. Young (New, divided into Eden and Survivor)
2. Tenured (Old)
3. Permanent Generation (classes & library dependencies)

Objects are central to the operation of Confluence. When a request is received, the Java runtime will create new objects to fulfill the request in the Eden Space. If, after some time, those objects are still required, they may be moved to the Tenured (Old) space. But, typically, the *overwhelming majority* of objects created die young, within the Eden space. These are objects like method local references within a while or for loop, or Iterators for scanning through Collections or Sets.

But in IBM J9 the default policy is for a single, contiguous space - one large heap. The net effect is that for large Websphere environments, garbage collection can be terribly inefficient - and capable of suffering outages during peak periods.

> ⚠ For *larger instances with performance issues*, it is recommended to tune Confluence such that there is a large Young space, at *up to* 50% the overall size of the heap.

`-XX:NewSize=XXXm` where XXX is the size in megabytes, is the command line parameter. `-XmnXXXm` can also be used interchangeably. Ie. -XX:NewSize=700m, -Xmn700m

By setting a larger `NewSize`, the net effect is that the JRE will spend less time garbage collecting, clearing dead memory references, compacting and copying memory between spaces, and more time *doing actual work*.

Use the Parallel Garbage Collector

Confluence out of the box, and Oracle Java as default, uses the *serial* garbage collector on the Full Tenured heap. The Young space is collected in parallel, but the Tenured is not. This means that at a time of load if a full collection event occurs, since the event is a 'stop-the-world' serial event then *all application threads* other than the garbage collector thread are taken off the CPU. This can have severe consequences if requests continue to accrue during these 'outage' periods. As a rough guide, for every gigabyte of memory allocated allow a full second (exclusive) to collect.

If we parallelize the collector on a multi-core/multi-cpu architecture instance, we not only *reduce* the total time of collection (down from whole seconds to fractions of a second) but we also improve the *resiliency* of the JRE in being able to recover from high-demand occasions.

Additionally, Oracle provide a CMS, Concurrent Mark-Sweep Collector (`-XX:+UseConcMarkSweepGC`), which is optimized for higher-throughput, server-grade instances. As a general rule, the Parallel Collector (-XX:+UseParallelOldGC) is the right choice for JIRA or Confluence installations, unless otherwise advised by support.

Restrict ability of Tomcat to 'cache' incoming requests

Quite often the fatal blow is swung by the 'backlog' of accumulated web requests whilst some critical resource (say the index) is held hostage by a temporary, expensive job. Even if the instance is busy garbage collecting due to load, Tomcat will still trigger new http requests and cache internally, as well as the operating system beneath which is also buffering incoming requests in the socket for Tomcat to pick up the next time it gets the CPU.

```
<Connector port="8090" protocol="HTTP/1.1"
      maxHttpHeaderSize="8192"
maxThreads="150" minSpareThreads="25"
maxSpareThreads="75"
useBodyEncodingForURI="true"
      enableLookups="false"
redirectPort="8443" acceptCount="100"
connectionTimeout="20000"
disableUploadTimeout="true"/>
```

Here the Tomcat Connector is configured for 150 "maxThreads" with an "acceptCount" of 100. This means up to 150 threads will awaken to accept (but importantly not to *complete*) web requests during performance outages, and 100 will be cached in a queue for further processing when threads are available. That's 250 threads, many of which can be quite expensive in and of themselves. Java will attempt to juggle all these threads concurrently and become extremely inefficient at doing so, exasperating the garbage collection performance issue.

Resolution: reduce the number of `maxThreads` and `acceptCount` to something slightly higher than normal 'busy-hour' demands.

Disable remote (distributed) garbage collection by Java clients

Many clients integrate third-party or their own custom applications to interrogate, or add content to Confluence via its RPC interface. The Distributed Remote Garbage Collector in the client uses RMI to trigger a remote GC event in the Confluence server. Unfortunately, as of this writing, a `System.gc()` call via this mechanism triggers a full, serial collection of the entire Confluence heap (as it needs to remove references to remote client objects in its own deterministic object graph). This is a deficiency in the configuration and/or implementation of the JVM. It has the potential to cause severe impact if the remote client is poorly written, or operating within a constricted JVM.

This can be disabled by using the flag `-XX:+DisableExplicitGC` at startup.

Virtual Machines are Evil

Vmware Virtual Machines, whilst being extremely convenient and fantastic, also cause particular problems for Java applications because it's very easy for host operating system resource constraints such as temporarily insolvent memory availability, or I/O swapping, to cascade into the Java VM and manifest as extremely unusual, frustrating and seemingly illogical problems. We already document some disk I/O metrics with VMware images. Although we now *officially* support the use of virtual instances we absolutely do not recommend them unless maintained correctly.

This is not to say that vmware instances cannot be used, but, they must be used with due care, proper maintenance and configuration. Besides, if you are reading this document because of poor performance, the first action should be to remove any virtualization. Emulation will never beat the real thing and always introduces more black box variability into the system.

Use Java 1.6

Java 1.6 is generally regarded via public discussion to have an approximate 20% performance improvement over 1.5. Our own internal testing revealed this statistic to be credible. 1.6 is compatible for all supported versions of Confluence, and we **strongly recommend** that installations not using 1.6 should migrate.

Use -server flag

The hotspot server JVM has specific code-path optimizations which yield an approximate 10% gain over the client version. Most installations *should* already have this selected by default, but it is still wise to force it with -server, especially on some Windows machines.

If using 64bit JRE for larger heaps, use `CompressedOops`

For every JDK release, Oracle also build a "Performance" branch in which specifically optimized performance features can be enabled; it is available on the Java SE page after a brief survey. These builds are certified production grade.

Some blogs have suggested a 25% performance gain and a reduction in heap size when using this parameter. The use and function of the `-XX:+UseCompressedOops` parameter is more deeply discussed on Oracle's Official Wiki (which itself uses Confluence!)

Use NUMA if on SPARC, Opteron or recent Intel (Nehalem or Tukwila onwards)

`-XX:+UseNUMA` flag enables the Java heap to take advantage of Non-Uniform-Memory-Architectures. JAVA will place data structures relevant to the thread which it owns / operates on, in memory locations closest to that particular processor. Depending on the environment, gains can be substantial. Intel market NUMA as Quick Path Interconnect™.

Use 32bit JRE if Heap < 2GB

Using a 64bit JRE when the heap is under 2GB will cause substantial degradation in heap size and performance. This is because nearly every object, reference, primitive, class and variable will use twice as much memory to be addressed.

A 64bit JRE/JDK is only recommended if heaps greater than 2GB are required. If so, use `CompressedOops`.

JVM core dumps can be instigated by memory pressures

If your instance of Confluence is throwing Java core dumps, it's known that memory pressure and space/generation sizings can influence the frequency and occurrence of this phenomena.

If your Tomcat process completely disappears and the logs record similar to:

```
#
# An unexpected error has been detected by
HotSpot Virtual Machine:
#
#  SIGSEGV (0xb) at pc=0xfe9bb960,
pid=20929, tid=17
#
# Java VM: Java HotSpot(TM) Server VM
(1.5.0_01-b08 mixed mode)
# Problematic frame:
# V  [libjvm.so+0x1bb960]
#

---------------  T H R E A D
---------------

Current thread (0x01a770e0):  JavaThread
"JiraQuartzScheduler_Worker-1"
[_thread_in_vm, id=17]

siginfo:si_signo=11, si_errno=0,
si_code=1, si_addr=0x00000000

Registers:
 O0=0xf5999882 O1=0xf5999882 O2=0x00000000
O3=0x00000000
 O4=0x00000000 O5=0x00000001 O6=0xc24ff0b0
O7=0x00008000
 G1=0xfe9bb80c G2=0xf5999a48 G3=0x0a67677d
G4=0xf5999882
 G5=0xc24ff380 G6=0x00000000 G7=0xfdbc3800
Y=0x00000000
 PC=0xfe9bb960 nPC=0xfe9bb964
```

then you should upgrade the JVM. See SIGSEGV Segmentation Fault JVM Crash.

Artificial Windows memory limit

On Windows, the maximum heap allocatable to the Tomcat 32bit wrapper process is around 1400MB. If the instance is allocated too close to this limit, **chronic garbage collection is likely to result**, often producing JAVA core dumps similar to:

```
#
# A fatal error has been detected by the
Java Runtime Environment:
#
# java.lang.OutOfMemoryError: requested
8388608 bytes for GrET in
C:\BUILD_AREA\jdk6_18\hotspot\src\share\vm
\utilities\growableArray.cpp. Out of swap
space?
#
#  Internal Error
(allocation.inline.hpp:39), pid=11572,
tid=12284
#  Error: GrET in
C:\BUILD_AREA\jdk6_18\hotspot\src\share\vm
\utilities\growableArray.cpp
#
# JRE version: 6.0_18-b07
# Java VM: Java HotSpot(TM) Server VM
(16.0-b13 mixed mode windows-x86 )
# If you would like to submit a bug
report, please visit:
#
http://bugreport.sun.com/bugreport/crash.j
sp
#

---------------  T H R E A D
---------------

Current thread (0x002af800):  GCTaskThread
[stack: 0x00000000,0x00000000] [id=12284]
```

or,

```
#
# A fatal error has been detected by the
Java Runtime Environment:
#
# java.lang.OutOfMemoryError: requested
123384 bytes for Chunk::new. Out of swap
space?
#
#  Internal Error (allocation.cpp:215),
pid=10076, tid=4584
#  Error: Chunk::new
#
# JRE version: 6.0_18-b07
# Java VM: Java HotSpot(TM) Server VM
(16.0-b13 mixed mode windows-x86 )
# If you would like to submit a bug
report, please visit:
#
http://bugreport.sun.com/bugreport/crash.j
sp
#

---------------  T H R E A D
---------------

Current thread (0x6ca4d000):  JavaThread
"CompilerThread1" daemon
[_thread_in_native, id=4584,
stack(0x6cd10000,0x6cd60000)]
```

Workarounds include:

- changing the server OS to something other than Windows. For example, Linux
- switching to the 64 bit Tomcat wrapper (this is not supported)
- reducing memory allocation to the Tomcat process. Try backing off 100MB at a time and observe the results.

Instigate useful monitoring techniques

At all times the best performance tuning recommendations are based on current, detailed metrics. This data is easily available and configurable and helps us **tremendously** at Atlassian when diagnosing reported performance regressions.

1. enable JMX monitoring
2. enable Confluence Access logging
3. enable Garbage Collection Logging
4. Take Thread dumps at the time of regression. If you can't get into Confluence, you can take one externally.
5. Jmap can take a memory dump in real time without impacting the application. Syntax: `jmap -heap:format=b <process_id>`

Great tools available include:

- The excellent VisualVM, documentation.
- Thread Dump Analyzer - a great all-round thread debugging tool, particularly for identifying deadlocks.
- Samurai, an excellent alternative thread analysis tool, good for iterative dumps over a period of time.
- GC Viewer - getting a bit long in the tooth, but is a good mainstay for GC analysis.
- GChisto - A GC analysis tool written by members of the Sun Garbage Collection team.

Documentation:

- Sun's White Paper on Garbage Collection in Java 6.
- Sun's state-of-the-art JavaOne 2009 session on garbage collection (registration required).
- IBM stack: Java 5 GC basics for WebSphere Application Server.
- An Excellent IBM document covering native memory, thread stacks, and how these influence memory constricted systems. Highly recommended for additional reading.
- The complete list of JRE 6 options
- I strongly recommend viewing George Barnett's Summit 2010 performance presentation, Pulling a Rabbit from a Hat.

> Atlassian recommends at the very least to get VisualVM up and running (you willneed JMX), and to add Access and Garbage Collection logging.

Tuning the frequency of full collections

The JVM will generally only collect on the full heap when it has no other alternative, because of the relative size of the Tenured space (it is typically larger than the Young space), and the natural probability of objects within tenured not being eligible for collection, i.e. they are still alive.

Some installations can trundle along, only ever collecting in Young space. As time goes on, some object will survive the initial Young object collection and be promoted to Tenured. At some point, it will be dereferenced and no longer reachable by the deterministic, directed object graph. However, the occupied memory will still be held in limbo as "dead" memory until a collection occurs in the Tenured space to clear and compact the space.

It is not uncommon for moderately sized Confluence installations to reclaim as much as 50% of the current heap size on a full collection; This is because full collections occur so infrequently. By reducing the occupancy fraction heap trigger, this means that more memory will be available at any time, meaning that fewer swapping/object collections will occur during the busy hour.

Atlassian would classify frequency tuning on collections as an **advanced** topic for further experimentation, and is provided for informational purposes only. Unfortunately, it's impractical for Atlassian to support these kinds of changes in general.

Performance tuning works

Atlassian has a number of high profile and some *extremely* high demanding, mission-critical clients who have successfully, usually through trial and error, applied these recommendations to production instances and have significantly improved their instances. For more information, please file a support case at support.atlassian.com.

Scheduled Jobs

The administration console allows you to schedule various administrative jobs in Confluence, so that they are executed at regular time intervals. The types of jobs which can be scheduled cover:

- Confluence site backups
- Storage optimisation jobs to clear Confluence's temporary files and caches
- Index optimisation jobs to ensure Confluence's search indexes are up to date
- Mail queue optimisation jobs to ensure Confluence's mail queue is maintained and notifications have been sent.

ⓘ You need to have System Administrator permissions in order to configure and execute jobs.

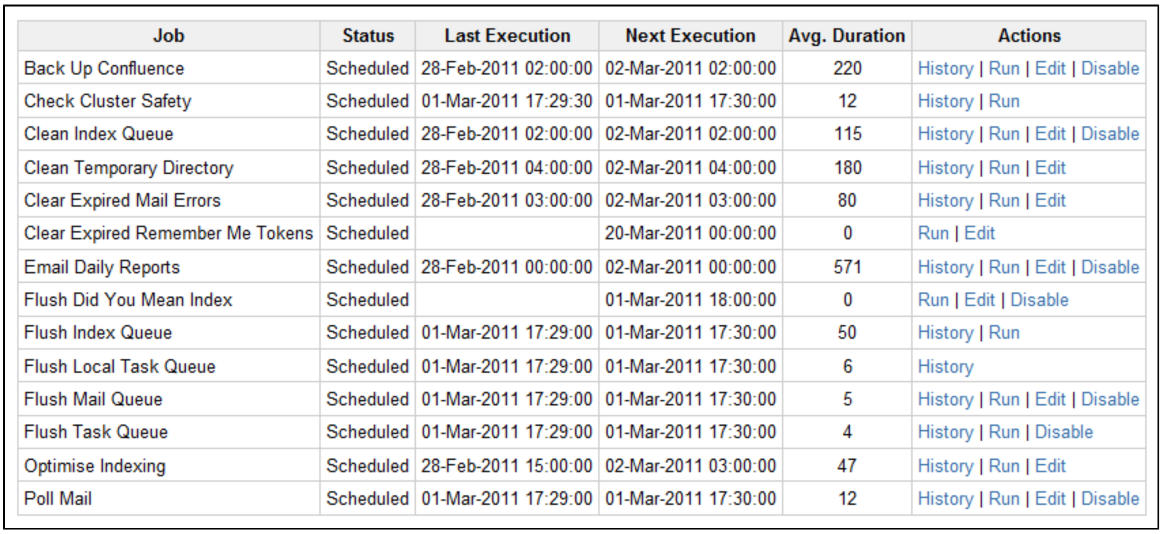
On this page:

⚠ *The information on this page does not apply to Confluence OnDemand.*

Accessing Confluence's Scheduled Jobs Configuration

To access Confluence's Scheduled Jobs configuration page:

1. Choose **Browse** > **Confluence Admin**.
2. Click '**Scheduled Jobs**' under '**Administration**' in the left panel to open the 'Scheduled Jobs' page. For each job listed down this page, the following information is shown:
   - **Job** — the name of a job.
   - **Status** — the job's status, which is either 'Scheduled' (it it is currently enabled) or 'Disabled'. See below for details on disabling or re-enabling a job.
   - **Last Execution** — the date and time when the job was last executed. This field will be empty of the job was never executed.
   - **Next Execution** — the date and time when the job is next scheduled to be executed. This field will contain dash symbol ('-') if the job is disabled.
   - **Avg. Duration** — the length of time (in milliseconds) that it took to complete the job's last execution.
   - **Actions** — allows you to configure the job, execute it manually, view a history of previous executions or disable the job.



Job	Status	Last Execution	Next Execution	Avg. Duration	Actions
Back Up Confluence	Scheduled	28-Feb-2011 02:00:00	02-Mar-2011 02:00:00	220	History | Run | Edit | Disable
Check Cluster Safety	Scheduled	01-Mar-2011 17:29:30	01-Mar-2011 17:30:00	12	History | Run
Clean Index Queue	Scheduled	28-Feb-2011 02:00:00	02-Mar-2011 02:00:00	115	History | Run | Edit | Disable
Clean Temporary Directory	Scheduled	28-Feb-2011 04:00:00	02-Mar-2011 04:00:00	180	History | Run | Edit
Clear Expired Mail Errors	Scheduled	28-Feb-2011 03:00:00	02-Mar-2011 03:00:00	80	History | Run | Edit
Clear Expired Remember Me Tokens	Scheduled		20-Mar-2011 00:00:00	0	Run | Edit
Email Daily Reports	Scheduled	28-Feb-2011 00:00:00	02-Mar-2011 00:00:00	571	History | Run | Edit | Disable
Flush Did You Mean Index	Scheduled		01-Mar-2011 18:00:00	0	Run | Edit | Disable
Flush Index Queue	Scheduled	01-Mar-2011 17:29:00	01-Mar-2011 17:30:00	50	History | Run
Flush Local Task Queue	Scheduled	01-Mar-2011 17:29:00	01-Mar-2011 17:30:00	6	History
Flush Mail Queue	Scheduled	01-Mar-2011 17:29:00	01-Mar-2011 17:30:00	5	History | Run | Edit | Disable
Flush Task Queue	Scheduled	01-Mar-2011 17:29:00	01-Mar-2011 17:30:00	4	History | Run | Disable
Optimise Indexing	Scheduled	28-Feb-2011 15:00:00	02-Mar-2011 03:00:00	47	History | Run | Edit
Poll Mail	Scheduled	01-Mar-2011 17:29:00	01-Mar-2011 17:30:00	12	History | Run | Edit | Disable

Screenshot above: Scheduled Jobs

Executing a Job Manually

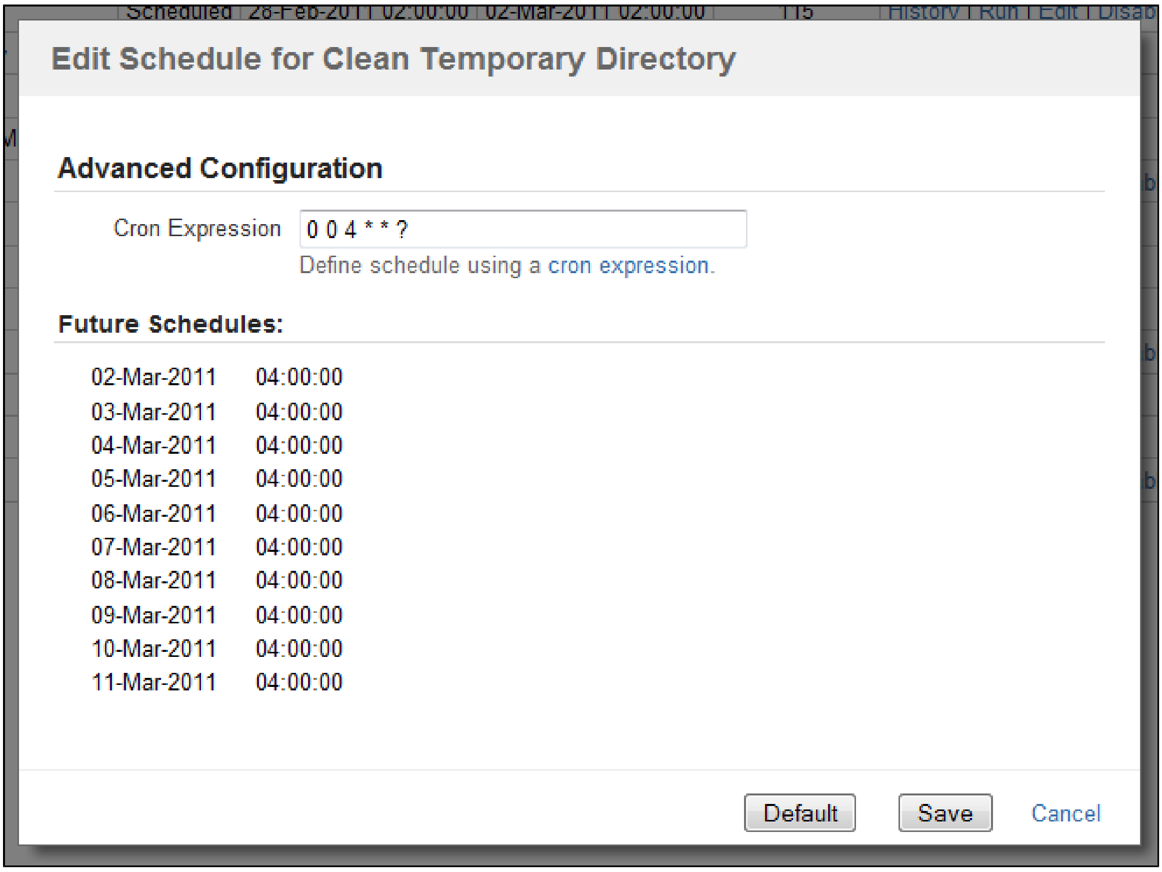
1. Access the 'Scheduled Jobs' configuration page (above).
2. Locate the job you wish to execute manually and click its '**Run**' link in the 'Actions' column. The job will be run immediately.
   ✅ Refer to 'Types of Jobs' (below) for detailed descriptions about each job.

   ℹ Not all jobs can be run manually.

Configuring a Job's Schedule

1. Access the 'Scheduled Jobs' configuration page (above).
2. Locate the job whose schedule you wish to configure and click its '**Edit**' link in the 'Actions' column. The job's 'Edit Schedule for job' dialog box opens.
   ✅ Refer to 'Types of Jobs' (below) for detailed descriptions about each job.
3. Enter an appropriate cron expression to define the frequency with which the job is executed.
   ✅ Refer to 'Cron Expressions' (below) for more details about their syntax. To revert the job's schedule back to its default settings, click the '**Default**' button.
4. Click '**Save**' to record your job's new schedule.

   ℹ Not all jobs' schedules are configurable.



Scheduled | 28-Feb-2011 02:00:00 | 02-Mar-2011 02:00:00 | 115 | History | Run | Edit | Disab
Default
Save
Cancel

Edit Schedule for Clean Temporary Directory

Advanced Configuration

Cron Expression: 0 0 4 * * ?

Define schedule using a cron expression.

Future Schedules:

02-Mar-2011	04:00:00
03-Mar-2011	04:00:00
04-Mar-2011	04:00:00
05-Mar-2011	04:00:00
06-Mar-2011	04:00:00
07-Mar-2011	04:00:00
08-Mar-2011	04:00:00
09-Mar-2011	04:00:00
10-Mar-2011	04:00:00
11-Mar-2011	04:00:00

Screenshot above: Configuring a Job's Schedule

Disabling/Re-enabling a Job

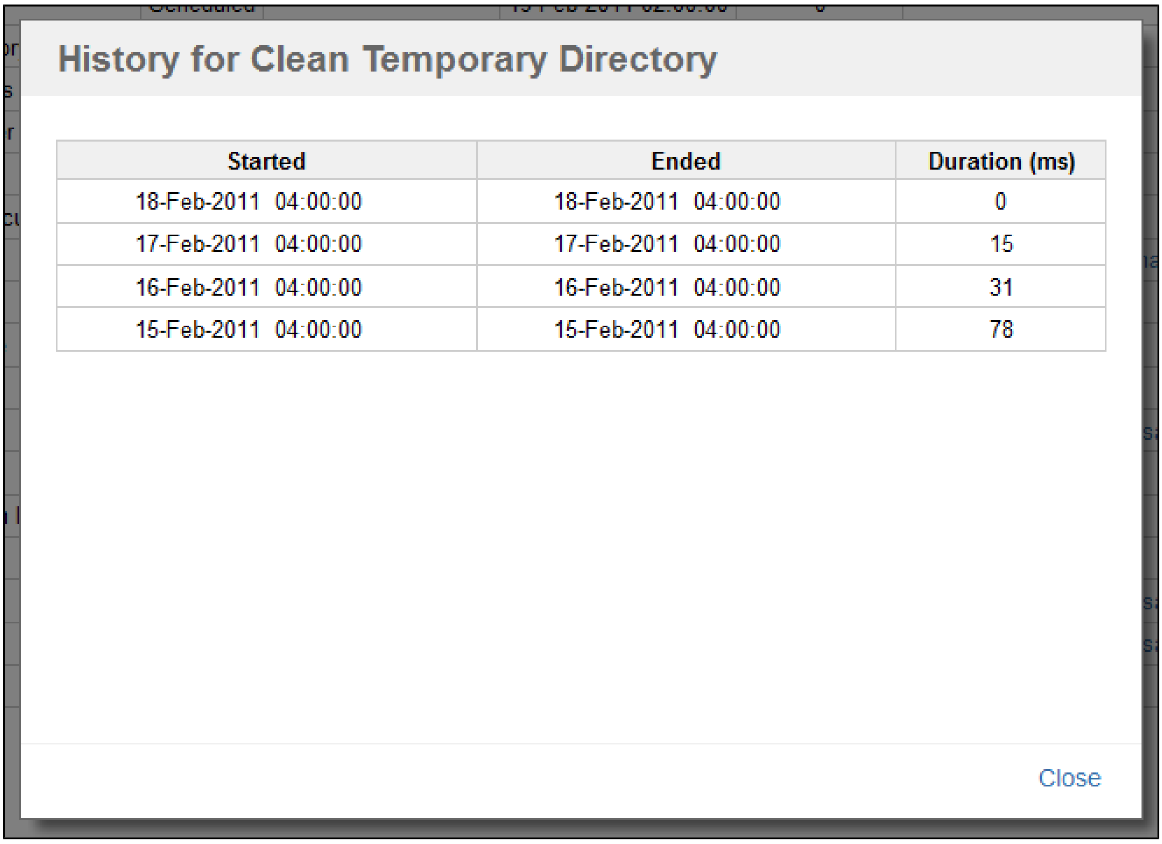
By default, all jobs in Confluence are enabled.

1. Access the 'Scheduled Jobs' configuration page (above).
2. Locate the job you wish to disable/re-enable.
   ✅ Refer to 'Types of Jobs' (below) for detailed descriptions about each job.
   - If a job is enabled, click its '**Disable**' link in the 'Actions' column to disable the job.
   - If a job is disabled, click its '**Enable**' link in the 'Actions' column to enable the job.

     ℹ Not all jobs in Confluence can be disabled.

Viewing a Job's Execution History

1. Access the 'Scheduled Jobs' configuration page (above).
2. Locate the job whose execution history you wish to view and click the '**History**' link.
   ℹ If a job has not completed at least one execution, its 'History' link will not be available.
   ✅ Refer to 'Types of Jobs' (below) for detailed descriptions about each job.
   The 'History for job' dialog box opens, showing a list of previous executions of the job in reverse chronological order, including the:
   - Start date and time
   - End date and time
   - The length of time (in milliseconds) that it took to complete the job



History for Clean Temporary Directory

Started	Ended	Duration (ms)
18-Feb-2011 04:00:00	18-Feb-2011 04:00:00	0
17-Feb-2011 04:00:00	17-Feb-2011 04:00:00	15
16-Feb-2011 04:00:00	16-Feb-2011 04:00:00	31
15-Feb-2011 04:00:00	15-Feb-2011 04:00:00	78

Screenshot above: Job Execution History

Types of Jobs

Job Name	Description	Execution Behaviour	Default Schedule
Back Up Confluence	Performs a backup of your entire Confluence site.	Per cluster	At 2am every day
Check Cluster Safety	For clustered Confluence installations, this job ensures that only one Confluence instance in the cluster writes to the database at a time. For standard (non-clustered) editions of Confluence, this job is useful for alerting customers who have accidentally connected a second Confluence instance to a Confluence database which is already in use.	Per cluster	Every 30 seconds

Clean Index Queue	Triggers a periodical clean of the index queue to ensure that its size does NOT grow indefinitely.	Per cluster	At 2am every day
Clean Temporary Directory	Cleans up temporary files generated in the 'temp' subdirectory of the Confluence home directory. This temp directory may be created by exports etc.	Per node	At 4am every day
Clear Expired Mail Errors	Clears notification errors in the mail error queue. A notification error is sent to the mail error queue whenever the notification fails to be sent due to an error.	Per cluster	At 3am every day
Clear Expired Remember Me Tokens	Clears all expired 'Remember Me' tokens from the Confluence site. Remember Me tokens expire after two weeks.	Per cluster	On the 20th of each month
Email Daily Reports	Emails a daily summary report of all Confluence changes to all subscribers. ℹ Since each email report only records changes from the last 24-hour period, it is recommended that you only change the time of this job whilst keeping the job's frequency to 24 hours.	Per cluster	At 12am every day
Flush Did You Mean Index	Flushes changes to the 'Did You Mean' index, which keeps the 'Did You Mean' feature up to date. Confluence records each content update in the 'Did You Mean' index.	Per node	Every 2 hours from 12 am

Flush Index Queue	Flushes changes to Confluence's index so that Confluence's search results are up to date. Confluence records each content update in its search index.	Per node	Every minute
Flush Local Task Queue	Flushes the local task queue. (These are internal Confluence tasks that are typically flushed at a high frequency.)	Per node	Every minute
Flush Mail Queue	Sends notifications that have been queued up in the mail queue.	Per cluster	Every minute
Flush Task Queue	Flushes the task queue. (These are internal Confluence tasks that are typically flushed at a high frequency.)	Per node	Every minute
Optimise Indexing	Compacts the confluence indexes to maintain searching performance. ✅ This task is demanding on system resources and does not need to be performed too regularly. If you see Confluence performance deteriorate around 3pm, try scheduling this job for 3am only and check if search performance remains reasonable.	Per node	At 3am and 3pm every day
Poll Mail	Polls POP accounts on all spaces that have them configured.	Per cluster	Every minute

Cron Expressions

A cron expression is a string of 6-7 'time interval' fields that defines the frequency with which a job is executed. Each of these fields can be expressed as either a numerical value or a special character and each field is separated by at least one space or tab character.

The table below is shows the order of time interval fields in a cron expression and each field's permitted numerical values.

You can specify a special character instead of a numerical value for any field in the cron expression to provide flexibility in defining a job's frequency. Common special characters include:

- '*' — a 'wild card' that indicates 'all permitted values'.
- '?' — indicates 'ignore this time interval' in the cron expression. That is, the cron expression will not be bound by the time interval (such as 'Month', 'Day of week' or 'Year') to which this character is specified.

For more information about cron expressions, please refer to the Cron Trigger tutorial on the Quartz website.

Order in cron expression	Time interval field	Permitted values*	Required?
1	Seconds	0-59	Yes
2	Minutes	0-59	Yes
3	Hours	0-23	Yes
4	Day of month	1-31	Yes
5	Month	1-12 or JAN-DEC	Yes
6	Day of week	1-7 or SUN-SAT	Yes
7	Year	1970-2099	No

* Excluding special characters.

RELATED TOPICS

Trigger Module
Configuring Backups

Search

No content found for label(s) modify-search.

⚠ *The information on this page does not apply to Confluence OnDemand.*

Setup Confluence To Index External Sites

Confluence Indexing External Sites

Confluence cannot easily index external sites due to technical reasons, but there are two alternatives:

1. Embed External Pages Into Confluence
2. Replace Confluence Search

⚠ *The information on this page does not apply to Confluence OnDemand.*

Technical Reasons

Confluence indexes pages using a customised Lucene search engine that returns matching pages, mail and blog posts for which the searcher has view permission. It would require significant source code modifications to enable Confluence to process search results from external pages, as the indexing process has been customised to utilise internal Confluence metadata. Note that users can still index content from new attachment filetypes.

Embed External Pages Into Confluence

If you only have a small number of external sites to index, you may prefer to enable the HTML-include Macro and use it embed the external content inside normal Confluence pages.

Replace Confluence Search

Use your own programmer resources to replace Confluence's internal search with a crawler that indexes both Confluence and external sites. This advanced option is easier than modifying the internal search engine. It requires removing Confluence internal search from all pages and replacing the internal results page with your own crawler front-end.

1. Setup a replacement federated search engine to index the Confluence site, as well as your other sites, and provide the results that way. You would need to host a web crawler, such as these open-source crawlers. Note that you can perform a search in Confluence via the remote API
2. Replace references to the internal search by modifying the site layout so that it links to your search front-end
3. Host another site containing the search front-end. You may wish to insert it into a suitable context path in your application server so that it appears to be from a path under Confluence. Tomcat sets Confluence's paths from the Confluence install\confluence\WEBINF\web.xml file.

RELATED TOPICS

Setup External Search Tool To Index Confluence

Setup External Search Tool To Index Confluence

Any web crawler can be configured to index Confluence content, for example the Google Search Appliance or similar. If a login is required to view content that will be indexed, you should create a Confluence user specifically for the search crawler to use. Grant this user view rights to all content you wish to index, but deny that user all delete and administration rights. This ensures that an aggressive crawler will not be able to perform actions that could modify the site. There is also a forum thread on Google Mini integration.

External applications can also use the search function in the Confluence Remote API.

⚠ *The information on this page does not apply to Confluence OnDemand.*

Related Information

No content found for label(s) modify-search.

Working with Confluence Logs

Confluence uses Apache's log4j logging service. This allows a developer or administrator to control the logging behavior and the log output file by editing a configuration file, without touching the application binary. There are six known log4j logging levels.

If you request help from Atlassian Support, we will almost always ask for the `atlassian-confluence.log` from the `confluence-home/logs` directory. You can access the logs from the Confluence Administration

Console, via the support tool. If you cannot access the Confluence Administration Console, check the properties file at `<confluence-installation>/confluence/WEB-INF/classes/confluence-init.properties`, look for the `confluence.home` setting in that file, then find the logs in the Confluence home directory.

On this page:

⚠ *The information on this page does not apply to Confluence OnDemand.*

Finding the Confluence Log Files

This section describes Confluence's default logging behaviour, assuming that you have not changed the destination of the logs. In order to unify logging across different application servers, Confluence uses the `atlassian-confluence.log` as its primary log, not the application server log.

Both the Confluence and Confluence EAR/WAR distributions follow the same default behaviour:

- When you start Confluence, log entries will be sent to the application server logs until Confluence has completed its initial bootstrap. Any log entries written to the console will be repeated into the log in the Confluence home directory as described below.
- Once the initial startup sequence is complete, all logging will be to `<confluence-home>/logs/atlassian-confluence.log`. For example: `c:/confluence/data/logs/atlassian-confluence.log`.

Note that the default location is the Confluence **home directory**, not the application server's log file. The home directory is specified in `<confluence-installation>/confluence/WEB-INF/classes/confluence-init.properties`.

Finding the Log Configuration File

Confluence's logging behaviour is defined in the following properties file:
`<CONFLUENCE-INSTALL>/confluence/WEB-INF/classes/log4j.properties`

This file is a standard log4j configuration file, as described in the Apache log4j documentation.

Changing the Destination of the Log Files

Terminology: In log4j, an output destination is called an 'appender'.

To change the destination of the log files, you need to stop Confluence and then change the settings in the '**Logging Location and Appender**' section of the `log4j.properties` file. The location of this file is described above.

In the standard properties file, you will find entries for two appenders:

- `com.atlassian.confluence.logging.ConfluenceHomeLogAppender` – This is a custom

appender which controls the default logging destination described above. This appender allows the following settings:
    - MaxFileSize
    - MaxBackupIndex
- `org.apache.log4j.RollingFileAppender` – If you want to log to a different location, uncomment the `RollingFileAppender` line and change the destination file in the line below it. Comment out the previous lines referring to the `ConfluenceHomeLogAppender`.

Confluence ships with the full suite of appenders offered by log4j. Read more about appenders in the log4j documentation.

Changing the Logging Levels

See Configuring Logging for instructions on how to change the logging configuration of Confluence.

Using Some Specific Confluence Logging Options

This section contains some pointers to specific log configurations you may need.

Log the Details of SQL Requests made to the Database

You may want to increase Confluence's logging so that it records individual SQL requests sent to the database. This is useful for troubleshooting specific problems.

You can enable detailed SQL logging in two ways:

- At runtime – see instructions above.
- Via the logging properties file – see the detailed instructions.

Log the Details of Users Viewing/Accessing each Confluence Page

You can configure the log to show which users are accessing which pages in Confluence. This can only be done via the logging properties file – see the detailed instructions.

Scanning Log Files for Known Problems

Confluence provides an inbuilt log scanner that will check your Confluence logs for errors and attempt to match them against known issues in our knowledge base and bug tracker. See Troubleshooting Problems and Requesting Technical Support.

Notes

- **Finding the thread dumps.** Thread dumps are logged to the application server log file.

RELATED TOPICS

Important Directories and Files
Enabling Detailed SQL Logging
Enabling user access logging
Generating a Thread Dump
Enabling Page Request Profiling
Troubleshooting Problems and Requesting Technical Support

Administrators Guide Home Confluence Documentation Home

log4j Logging Levels

Logging Levels

- **DEBUG** - designates fine-grained informational events that are most useful to debug an application (*what is going on*)
- **INFO** - announcements about the normal operation of the system - scheduled jobs running, services starting and stopping, user-triggered processes and actions
- **WARN** - any condition that, while not an error in itself, may indicate that the system is running sub-optimally
- **ERROR** - a condition that indicates something has gone wrong with the system
- **FATAL** - a condition that indicates something has gone wrong so badly that the system can not recover
- **TRACE** - n/a within confluence

> ℹ There are two ways to modify the logging levels, as described in Working with Confluence Logs.
>
> 1. Modifying the runtime log levels via the **Administration Console**.
> 2. Manually modifying the `<Confluence-Install>\confluence\WEB-INF\classes\log4j.properties` file.

> ⚠ *The information on this page does not apply to Confluence OnDemand.*

Default Log Level

The standard Confluence log level **WARN** is a way for Confluence to communicate with the server administrator. Logging at WARN level and higher should be reserved for situations that require some kind of attention from the server administrator, and for which corrective action is possible.

Reference : log4j manual

User Management

- Understanding User Management in Confluence
- Configuring User Directories
  - Configuring the Internal Directory
  - Connecting to an LDAP Directory
    - Configuring the LDAP Connection Pool
    - Configuring an SSL Connection to Active Directory
  - Connecting to an Internal Directory with LDAP Authentication
  - Connecting to Crowd or JIRA for User Management
    - Reverting from Crowd or JIRA to Internal User Management
  - Connecting to JIRA 4.2 or Earlier for User Management
  - Managing Multiple Directories
  - Managing Nested Groups
  - Synchronising Data from External Directories
  - Diagrams of Possible Configurations for User Management
  - User Management Limitations and Recommendations
  - Requesting Support for External User Management
- Confluence User Management
  - Searching For and Managing Users
  - Adding Users
  - Adding a Group
  - Adding or Removing Users in Groups
  - Changing Usernames

- Editing User Details
- Global Groups Overview
- Global Permissions Overview
- Removing a Group
- Removing or Deactivating a User
- Setting up Anonymous Access
- Viewing members of a group
- Restoring Passwords To Recover Admin User Rights
- Resetting the Login Count for a User

- Disabling the Built-In User Management

⚠ *The information on this page does not apply to Atlassian OnDemand sites with multiple apps. If you are using Confluence-only OnDemand, the information does apply.*

Understanding User Management in Confluence

This page introduces the concepts and components of user management in Confluence.

The components of user management are:

- **Authentication:** Determining what user identity is making a request to Confluence.
- **User management:** Storing and retrieving core information about users.
- **Group membership:** Storing and retrieving groups, and group membership.
- **Profile information:** Providing metadata associated with users.

It is important to understand that these are separate components of the user management system. When referring to 'LDAP integration', remember that you could use an LDAP directory for any or all of the above tasks.

On this page:

⚠ *The information on this page does not apply to Atlassian OnDemand sites with multiple apps. If you are using Confluence-only OnDemand, the information does apply.*

Authentication

Seraph

Almost all authentication in Confluence (and JIRA) is performed through Seraph, Atlassian's open source web authentication framework. The goal of Seraph is to provide a simple, extensible authentication system that we can use on any application server.

Seraph is implemented as a servlet filter. Its sole job is, given a web request, to associate that request with a particular user (or no user if the request is anonymous). It supports several methods of authentication, including HTTP Basic Authentication, form-based authentication, and looking up credentials already stored in the user's session.

Seraph itself performs no user management functions. It merely checks the credentials of the incoming request and delegates any user management functions (looking up a user, checking a user's password is correct) to Confluence's user management system.

If you were looking to integrate Confluence with your own single sign-on (SSO) infrastructure, you would do so by installing Atlassian Crowd or by writing a custom Seraph authenticator.

XML-RPC and SOAP Authentication

Normally, requests for Confluence's remote API will include an authentication token as the first argument. With this method of authentication, XML-RPC and SOAP authentication requests are checked directly against the user management framework, and tokens are assigned directly by the remote API subsystem. These requests do not pass through Seraph authenticators.

However, if the token argument is blank, Seraph will be used as a fallback authentication method for remote API requests. So, to use a custom Seraph authenticator with XML-RPC or SOAP requests, ensure that you pass an empty string as the authentication token to remote API methods.

Password Authentication and User Management

By default, password authentication is delegated from Seraph to the user management system. This is not necessary, however. Single sign-on systems may have no password authentication at all, and get all the necessary credentials from the SSO provider.

Confluence User Management Framework

User Management via the Confluence Administration Console

Configuring User Directories

A user directory is a place where you store information about users and groups. User information includes the person's full name, username, password, email address and other personal information. Group information includes the name of the group, the users that belong to the group, and possibly groups that belong to other groups.

The **internal** directory stores user and group information in the Confluence database. You can also connect to **external** user directories, and to Atlassian **Crowd** and **JIRA** as directory managers. You can configure multiple directories. For example Confluence can draw user information from both the database and an LDAP server.

See Configuring User Directories.

Managing Users and Groups

You can add users and groups, add members to groups, and add profile information to each user. See Confluence User Management.

If you have connected Confluence to more than one user directory, you need to define the **directory order**. Here is a summary of how the directory order affects the processing:

- The order of the directories is the order in which they will be searched for users and groups.
- Changes to users and groups will be made only in the first directory where the application has permission to make changes.

See Managing Multiple Directories.

Information about Earlier User Management Frameworks

Atlassian-User – Now Behind the Scenes

Atlassian-User is a user and group management framework developed by Atlassian. It provides user, group and profile management services to Confluence. In earlier versions of Confluence, you needed to configure your user directories by editing the `atlassian-user.xml` file directly. In Confluence 3.5 and later this is no longer necessary, nor is it possible. Please refer to the documentation for Confluence 3.4 or earlier, if you need details of this framework.

Refer to the Confluence 3.5 Upgrade Notes for details of the automatic migration that will occur during the upgrade process.

OSUser – Obsolete

OpenSymphony User was Confluence's core user management framework before Atlassian-User. Please refer to the documentation for Confluence 3.4 or earlier, if you need details of this framework.

RELATED TOPICS

HTTP authentication with Seraph
User Management

- Understanding User Management in Confluence
- Configuring User Directories
- Confluence User Management
- Disabling the Built-In User Management

Administrators Guide Home Confluence Documentation Home

Configuring User Directories

A user directory is a place where you store information about users and groups. User information includes the person's full name, username, password, email address and other personal information. Group information includes the name of the group, the users that belong to the group, and possibly groups that belong to other groups.

The **internal** directory stores user and group information in the Confluence database. You can also connect to **external** user directories, and to Atlassian **Crowd** and **JIRA** as directory managers.

⚠ *The information on this page does not apply to Atlassian OnDemand sites with multiple apps. If you are using Confluence-only OnDemand, the information does apply.*

Configuring User Directories in Confluence

To configure your Confluence user directories:

1. Choose **Browse** > **Confluence Admin**.
2. Click '**User Directories**' in the left-hand panel.

Connecting to a Directory

You can add the following types of directory servers and directory managers:

- Confluence's internal directory. See Configuring the Internal Directory.
- Microsoft Active Directory. See Connecting to an LDAP Directory.
- Various other LDAP directory servers. See Connecting to an LDAP Directory.
- An LDAP directory for delegated authentication. See Connecting to an Internal Directory with LDAP Authentication.
- Atlassian Crowd. See Connecting to Crowd or JIRA for User Management.
- Atlassian JIRA 4.3 or later. See Connecting Confluence to JIRA for User Management.
- Atlassian JIRA 4.2 or earlier, using the legacy database connection. See Connecting to JIRA 4.2 or Earlier for User Management.

You can add as many external user directories as you need. Note that you can define the **order** of the directories. This determines which directory Confluence will search first, when looking for user and group information. See Managing Multiple Directories.

Updating Directories

Limitations when Editing Directories

You cannot edit, disable or remove the directory your user belongs to. This precaution is designed to prevent administrators from locking themselves out of the application by changing the directory configuration in a way that prevents them logging in or removes their administration permissions.

This limitation applies to all directory types. For example:

- You cannot disable the internal directory if your user is an internal user.
- You cannot disable or remove an LDAP or a Crowd directory if your user comes from that directory.

In some situations, reordering the directories will change the directory that the current user comes from, if a user with the same username happens to exist in both. This behaviour can be used in some cases to create a copy of the existing configuration, move it to the top, then remove the old one. Note, however, that duplicate usernames are not a supported configuration.

You cannot remove the internal directory. This precaution aligns with the recommendation below that you always keep an administrator account active in the internal directory.

Recommendations

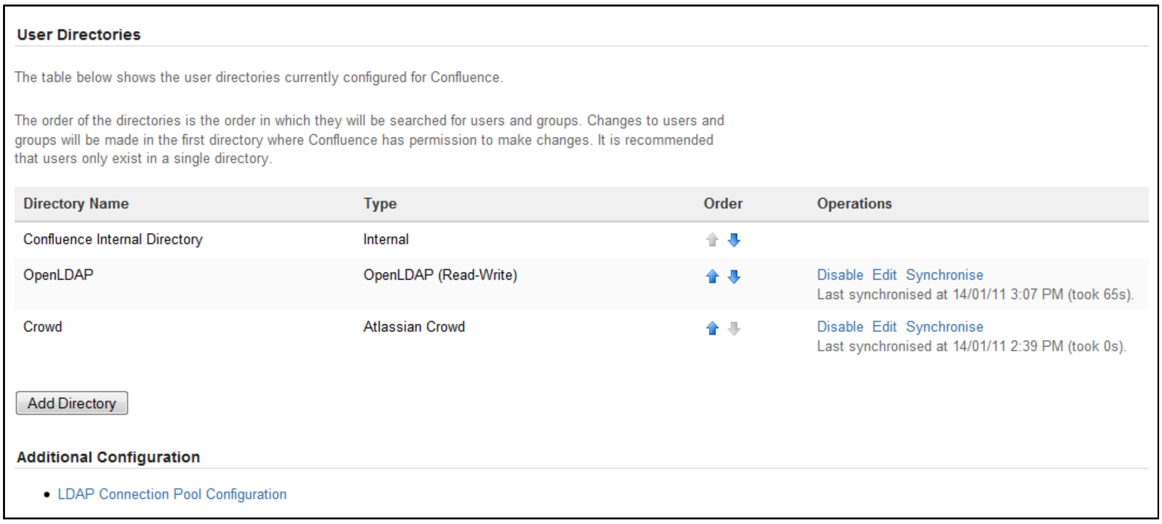
The recommended way to edit directory configurations is to log in as an internal user when making changes to external directory configuration.

⚠ We recommend that you keep either an administrator or system administrator user active in your internal directory for troubleshooting problems with your user directories.

Enabling, Disabling and Removing Directories

You can enable or disable a directory at any time. If you disable a directory, your configuration details will remain but the application will not recognise the users and groups in that directory.

You have to disable a directory before you can remove it. Removing a directory will remove the details from the database.



User Directories

The table below shows the user directories currently configured for Confluence.

The order of the directories is the order in which they will be searched for users and groups. Changes to users and groups will be made in the first directory where Confluence has permission to make changes. It is recommended that users only exist in a single directory.

Directory Name	Type	Order	Operations
Confluence Internal Directory	Internal	↑ ↓	
OpenLDAP	OpenLDAP (Read-Write)	↑ ↓	Disable Edit Synchronise Last synchronised at 14/01/11 3:07 PM (took 65s).
Crowd	Atlassian Crowd	↑ ↓	Disable Edit Synchronise Last synchronised at 14/01/11 2:39 PM (took 0s).

Add Directory

Additional Configuration

- LDAP Connection Pool Configuration

Screenshot above: Configuring user directories

RELATED TOPICS

- Configuring the Internal Directory
- Connecting to an LDAP Directory
- Connecting to an Internal Directory with LDAP Authentication
- Connecting to Crowd or JIRA for User Management
- Connecting to JIRA 4.2 or Earlier for User Management
- Managing Multiple Directories
- Managing Nested Groups
- Synchronising Data from External Directories
- Diagrams of Possible Configurations for User Management
- User Management Limitations and Recommendations
- Requesting Support for External User Management

- Adding Users
- Adding a Group

Administrators Guide Home Confluence Documentation Home

Configuring the Internal Directory

The internal directory stores user and group information in the Confluence database.

Overview

The internal directory is enabled by default at installation. When you create the first administrator during the setup procedure, that administrator's username and other details are stored in the internal directory.

If needed, you can configure one or more additional user directories. This is useful if you want to grant access to users and groups that are stored in a corporate directory or other directory server.

On this page:

- Overview
- Diagram of Possible Configuration

⚠ *The information on this page does not apply to Confluence OnDemand.*

Diagram of Possible Configuration

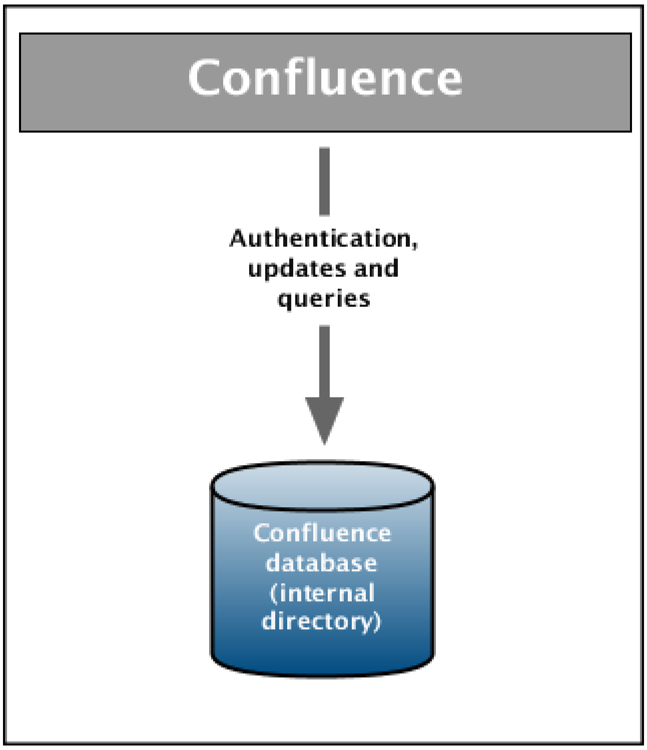

Confluence
Authentication, updates and queries
Confluence database (internal directory)

Diagram above: Confluence using its internal directory for user management.

RELATED TOPICS

Configuring User Directories

- Configuring the Internal Directory
- Connecting to an LDAP Directory
- Connecting to an Internal Directory with LDAP Authentication
- Connecting to Crowd or JIRA for User Management
- Connecting to JIRA 4.2 or Earlier for User Management
- Managing Multiple Directories
- Managing Nested Groups
- Synchronising Data from External Directories
- Diagrams of Possible Configurations for User Management
- User Management Limitations and Recommendations
- Requesting Support for External User Management

How to Reenable the Internal Directory (Knowledge base article)

Connecting to an LDAP Directory

You can connect your Confluence application to an LDAP directory for authentication, user and group management.

Overview

An LDAP directory is a collection of data about users and groups. LDAP (Lightweight Directory Access Protocol) is an Internet protocol that web applications can use to look up information about those users and groups from the LDAP server.

We provide built-in connectors for the most popular LDAP directory servers:

- Microsoft Active Directory
- Apache Directory Server (ApacheDS)
- Apple Open Directory
- Fedora Directory Server

- Novell eDirectory
- OpenDS
- OpenLDAP
- OpenLDAP Using Posix Schema
- Posix Schema for LDAP
- Sun Directory Server Enterprise Edition (DSEE)
- A generic LDAP directory server

When to use this option: Connecting to an LDAP directory server is useful if your users and groups are stored in a corporate directory. When configuring the directory, you can choose to make it read only, read only with local groups, or read/write. If you choose read/write, any changes made to user and group information in the application will also update the LDAP directory.

On this page:

⚠ *The information on this page does not apply to Confluence OnDemand.*

Connecting to an LDAP Directory in Confluence

To connect Confluence to an LDAP directory:

1. Choose **Browse** > **Confluence Admin**.
2. Click **User Directories** in the left-hand panel.
3. **Add** a directory and select one of these types:
   - **Microsoft Active Directory** – This option provides a quick way to select AD, because it is the most popular LDAP directory type.
   - **LDAP** – You will be able to choose a specific LDAP directory type on the next screen.
4. Enter the values for the settings, as described below.
5. Save the directory settings.
6. Define the **directory order** by clicking the blue up- and down-arrows next to each directory on the 'User Directories' screen. Here is a summary of how the directory order affects the processing:
   - The order of the directories is the order in which they will be searched for users and groups.
   - Changes to users and groups will be made only in the first directory where the application has permission to make changes.

   For details see Managing Multiple Directories.

Server Settings

Setting	Description

Name	Enter a meaningful name to help you identify the LDAP directory server. Examples: - `Example Company Staff Directory` - `Example Company Corporate LDAP`
Directory Type	Select the type of LDAP directory that you will connect to. If you are adding a new LDAP connection, the value you select here will determine the default values for many of the options on the rest of screen. Examples: - `Microsoft Active Directory` - `OpenDS` - And more.
Hostname	The host name of your directory server. Examples: - `ad.example.com` - `ldap.example.com` - `opends.example.com`
Port	The port on which your directory server is listening. Examples: - `389` - `10389` - `636` (for example, for SSL)
Use SSL	Tick this check box if the connection to the directory server is an SSL (Secure Sockets Layer) connection. Note that you will need to configure an SSL certificate in order to use this setting.
Username	The distinguished name of the user that the application will use when connecting to the directory server. Examples: - `cn=administrator,cn=users,dc=ad,dc=example,dc=com` - `cn=user,dc=domain,dc=name` - `user@domain.name`
Password	The password of the user specified above.

Schema Settings

Setting	**Description**

Base DN	The root distinguished name (DN) to use when running queries against the directory server. Examples: • `o=example,c=com` • `cn=users,dc=ad,dc=example,dc=com` • For Microsoft Active Directory, specify the base DN in the following format: `dc=domain1,dc=local`. You will need to replace the `domain1` and `local` for your specific configuration. Microsoft Server provides a tool called `ldp.exe` which is useful for finding out and configuring the the LDAP structure of your server.
Additional User DN	This value is used in addition to the base DN when searching and loading users. If no value is supplied, the subtree search will start from the base DN. Example: • `ou=Users`
Additional Group DN	This value is used in addition to the base DN when searching and loading groups. If no value is supplied, the subtree search will start from the base DN. Example: • `ou=Groups`

Permission Settings

Setting	Description
Read Only	LDAP users, groups and memberships are retrieved from your directory server and can only be modified via your directory server. You cannot modify LDAP users, groups or memberships via the application administration screens.
Read Only, with Local Groups	LDAP users, groups and memberships are retrieved from your directory server and can only be modified via your directory server. You cannot modify LDAP users, groups or memberships via the application administration screens. However, you can add groups to the internal directory and add LDAP users to those groups.
Read/Write	LDAP users, groups and memberships are retrieved from your directory server. When you modify a user, group or membership via the application administration screens, the changes will be applied directly to your LDAP directory server. Please ensure that the LDAP user specified for the application has modification permissions on your LDAP directory server.

Adding Users to Groups Automatically

Setting	Description
Default Group Memberships	*Option available in Confluence 3.5 and later, and JIRA 4.3.3 and later.* This field appears if you select the 'Read Only, with Local Groups' permission. If you would like users to be automatically added to a group or groups, enter the group name(s) here. To specify more than one group, separate the group names with commas. *In Confluence 3.5 to Confluence 3.5.1:* Each time a user logs in, their group memberships will be checked. If the user does not belong to the specified group(s), their username will be added to the group(s). If a group does not yet exist, it will be added locally. *In Confluence 3.5.2 and later, and JIRA 4.3.3 and later:* The first time a user logs in, their group memberships will be checked. If the user does not belong to the specified group(s), their username will be added to the group(s). If a group does not yet exist, it will be added locally. On subsequent logins, the username will *not* be added automatically to any groups. This change in behaviour allows users to be removed from automatically-added groups. In Confluence 3.5 and 3.5.1, they would be re-added upon next login. Please note that there is no validation of the group names. If you mis-type the group name, authorisation failures will result – users will not be able to access the applications or functionality based on the intended group name. Examples: • `confluence-users` • `confluence-users,jira-users,jira-developers`

Advanced Settings

Setting	Description
Enable Nested Groups	Enable or disable support for nested groups. Some directory servers allow you to define a group as a member of another group. Groups in such a structure are called 'nested groups'. If you are using groups to manage permissions, you can create nested groups to allow inheritance of permissions from one group to its sub-groups.

Use Paged Results	Enable or disable the use of the LDAP control extension for simple paging of search results. If paging is enabled, the search will retrieve sets of data rather than all of the search results at once. Enter the desired page size – that is, the maximum number of search results to be returned per page when paged results are enabled. The default is 1000 results.
Follow Referrals	Choose whether to allow the directory server to redirect requests to other servers. This option uses the node referral (JNDI lookup `java.naming.referral`) configuration setting. It is generally needed for Active Directory servers configured without proper DNS, to prevent a 'javax.naming.PartialResultException: Unprocessed Continuation Reference(s)' error.
Naive DN Matching	If your directory server will always return a consistent string representation of a DN, you can enable naive DN matching. Using naive DN matching will result in a significant performance improvement, so we recommend enabling it where possible. This setting determines how your application will compare DNs to determine if they are equal. • If this check box is ticked, the application will do a direct, case-insensitive, string comparison. This is the default and recommended setting for Active Directory, because Active Directory guarantees the format of DNs. • If this check box is not ticked, the application will parse the DN and then check the parsed version.
Enable Incremental Synchronisation	Enable incremental synchronisation if you only want changes since the last synchronisation to be queried when synchronising a directory. ⚠ Please be aware that when using this option, the user account configured for synchronisation must have read access to: • The `uSNChanged` attribute of all users and groups in the directory that need to be synchronised. • The objects and attributes in the Active Directory deleted objects container (see Microsoft's Knowledge Base Article No. 892806 for details). If at least one of these conditions is not met, you may end up with users who are added to (or deleted from) the Active Directory not being respectively added (or deleted) in JIRA.

Synchronisation Interval (minutes)	Synchronisation is the process by which the application updates its internal store of user data to agree with the data on the directory server. The application will send a request to your directory server every x minutes, where 'x' is the number specified here. The default value is 60 minutes.
Read Timeout (seconds)	The time, in seconds, to wait for a response to be received. If there is no response within the specified time period, the read attempt will be aborted. A value of 0 (zero) means there is no limit. The default value is 120 seconds.
Search Timeout (seconds)	The time, in seconds, to wait for a response from a search operation. A value of 0 (zero) means there is no limit. The default value is 60 seconds.
Connection Timeout (seconds)	This setting affects two actions. The default value is 0. • The time to wait when getting a connection from the connection pool. A value of 0 (zero) means there is no limit, so wait indefinitely. • The time, in seconds, to wait when opening new server connections. A value of 0 (zero) means that the TCP network timeout will be used, which may be several minutes.

User Schema Settings

Setting	Description
User Object Class	This is the name of the class used for the LDAP user object. Example: • `user`
User Object Filter	The filter to use when searching user objects. Example: • `(&(objectCategory=Person)(sAMAccountName=*))`
User Name Attribute	The attribute field to use when loading the username. Examples: • `cn` • `sAMAccountName`

User Name RDN Attribute	The RDN (relative distinguished name) to use when loading the username. The DN for each LDAP entry is composed of two parts: the RDN and the location within the LDAP directory where the record resides. The RDN is the portion of your DN that is not related to the directory tree structure. Example: • `cn`
User First Name Attribute	The attribute field to use when loading the user's first name. Example: • `givenName`
User Last Name Attribute	The attribute field to use when loading the user's last name. Example: • `sn`
User Display Name Attribute	The attribute field to use when loading the user's full name. Example: • `displayName`
User Email Attribute	The attribute field to use when loading the user's email address. Example: • `mail`
User Password Attribute	The attribute field to use when loading a user's password. Example: • `unicodePwd`

Group Schema Settings

Setting	Description
Group Object Class	This is the name of the class used for the LDAP group object. Examples: • `groupOfUniqueNames` • `group`
Group Object Filter	The filter to use when searching group objects. Example: • `(objectCategory=Group)`
Group Name Attribute	The attribute field to use when loading the group's name. Example: • `cn`

Group Description Attribute	The attribute field to use when loading the group's description. Example: • `description`

Membership Schema Settings

Setting	Description
Group Members Attribute	The attribute field to use when loading the group's members. Example: • `member`
User Membership Attribute	The attribute field to use when loading the user's groups. Example: • `memberOf`
Use the User Membership Attribute, when finding the user's group membership	Put a tick in the checkbox if your directory server supports the group membership attribute on the user. (By default, this is the 'memberOf' attribute.) • If this checkbox is ticked, your application will use the group membership attribute on the user when **retrieving the members of a given group**. This will result in a more efficient retrieval. • If this checkbox is not ticked, your application will use the members attribute on the group ('member' by default) for the search. • If the 'Enable Nested Groups' checkbox is ticked, your application will ignore the 'Use memberOf Attribute on the User' option and will use the members attribute on the group for the search.
Use the User Membership Attribute, when finding the members of a group	Put a tick in the checkbox if your directory server supports the group membership attribute on the user. (By default, this is the 'memberOf' attribute.) • If this checkbox is ticked, your application will use the group membership attribute on the user when **retrieving the list of groups to which a given user belongs**. This will result in a more efficient search. • If this checkbox is not ticked, your application will use the members attribute on the group ('member' by default) for the search.

Diagrams of Some Possible Configurations

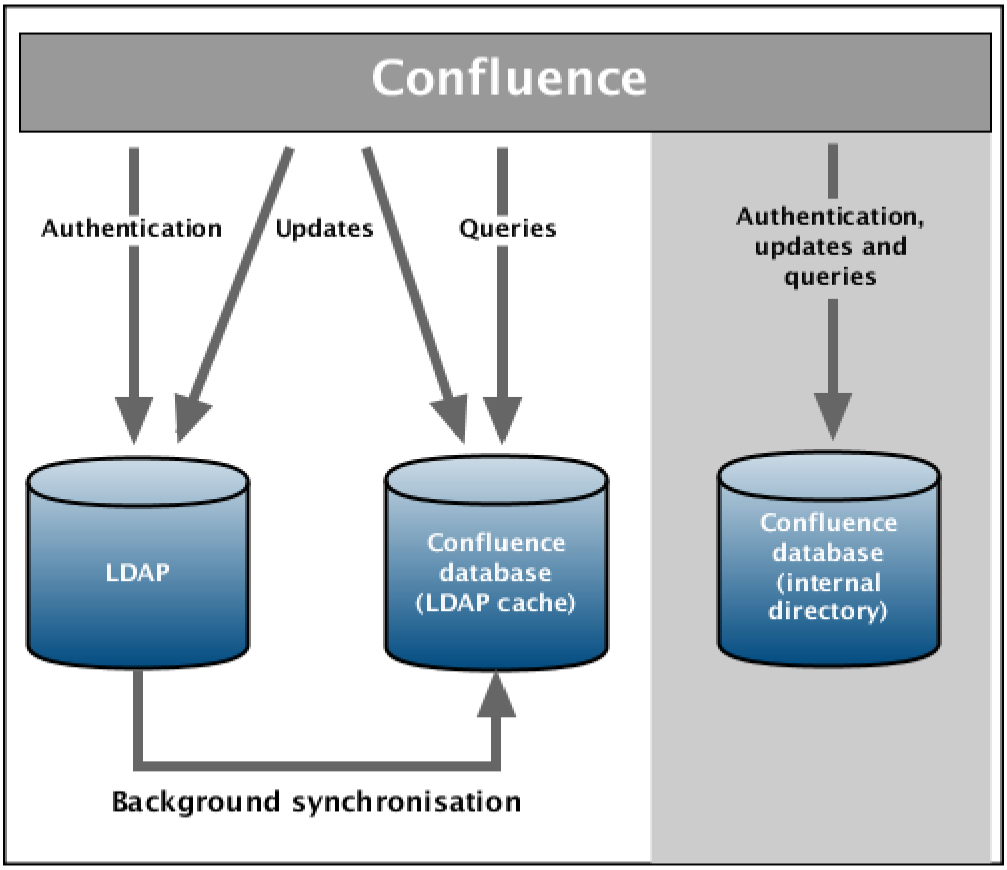

Confluence
Authentication
Updates
Queries
Authentication, updates and queries
LDAP
Confluence database (LDAP cache)
Confluence database (internal directory)
Background synchronisation

Diagram above: Confluence connecting to an LDAP directory.

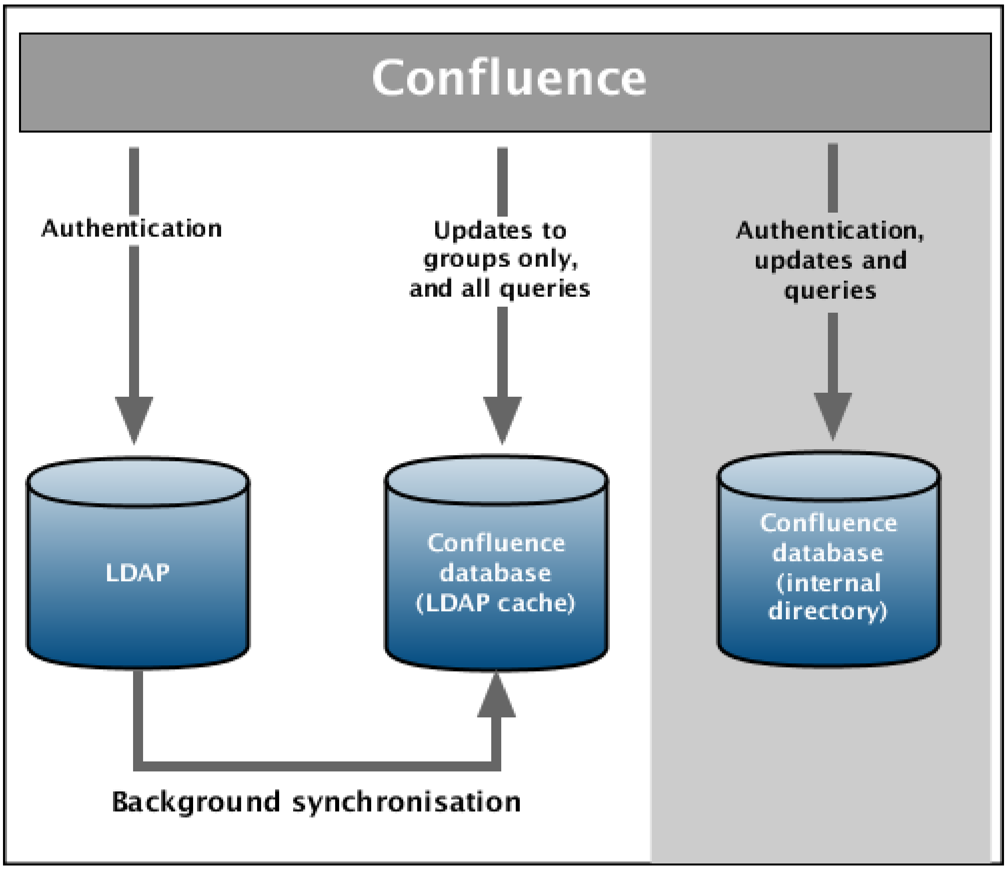

Confluence
Authentication
Updates to groups only, and all queries
Authentication, updates and queries
LDAP
Confluence database (LDAP cache)
Confluence database (internal directory)
Background synchronisation

Diagram above: Confluence connecting to an LDAP directory with permissions set to read only and local groups.

RELATED TOPICS

Configuring User Directories

- Configuring the Internal Directory
- Connecting to an LDAP Directory
- Connecting to an Internal Directory with LDAP Authentication
- Connecting to Crowd or JIRA for User Management
- Connecting to JIRA 4.2 or Earlier for User Management
- Managing Multiple Directories
- Managing Nested Groups
- Synchronising Data from External Directories
- Diagrams of Possible Configurations for User Management
- User Management Limitations and Recommendations
- Requesting Support for External User Management

Configuring the LDAP Connection Pool

When connection pooling is enabled, the LDAP directory server maintains a pool of connections and assigns them as needed. When a connection is closed, the directory server returns the connection to the pool for future use. This can improve performance significantly.

To configure your LDAP connection pool:

1. Choose **Browse** > **Confluence Admin**.
2. Click '**User Directories**' in the left-hand panel.
3. Click '**LDAP Connection Pool Configuration**' in the 'Additional Configuration' section.

> ⚠ *The information on this page does not apply to Atlassian OnDemand sites with multiple apps. If you are using Confluence-only OnDemand, the information does apply.*

Setting	Description	Default Value
Initial Pool Size	The number of LDAP connections created when initially connecting to the pool.	`1`
Preferred Pool Size	The optimal pool size. LDAP will remove idle connections when the number of connections grows larger than this value. A value of `0` (zero) means that there is no preferred size, so the number of idle connections is unlimited.	`10`

Maximum Pool Size	The maximum number of connections. When the number of connections reaches this value, LDAP will refuse further connections. As a result, requests made by an application to the LDAP directory server will be blocked. A value of `0` (zero) means that the number of connections is unlimited.	`0`
Pool Timeout (seconds)	The length of time, in seconds, that a connection may remain idle before being removed from the pool. When the application is finished with a pooled connection, the connection is marked as idle, waiting to be reused. A value of `0` (zero) means that the idle time is unlimited, so connections will never be timed out.	`30`
Pool Protocol	Only these protocol types will be allowed to connect to the LDAP directory server. If you want to allow multiple protocols, enter the values separated by a space. Valid values are: • `plain` • `ssl`	`plain ssl` (Both plain and ssl)
Pool Authentication	Only these authentication types will be allowed to connect to the LDAP directory server. If you want to allow multiple authentication types, enter the values separated by a space. See RFC 2829 for details of LDAP authentication methods. Valid values are: • `none` • `simple` • `DIGEST-MD5`	`simple`

Notes:

- The connection pool settings are system wide and will be used to create a new connection pool for every configured LDAP directory server.
- You must restart your application server for these settings to take effect.

RELATED TOPICS

Connecting to an LDAP Directory
Configuring User Directories

Administrators Guide Home Confluence Documentation Home

Configuring an SSL Connection to Active Directory

If you want to configure a read/write connection with Microsoft Active Directory, you will need to install an SSL certificate, generated by your Active Directory server, onto your Confluence server and then install the certificate into your JVM keystore.

⚠ *The information on this page does not apply to Atlassian OnDemand sites with multiple apps. If you are using Confluence-only OnDemand, the information does apply.*

Updating user, group, and membership details in Active Directory requires that your Atlassian application be running in a JVM that trusts the AD server. To do this, we generate a certificate on the Active Directory server, then import it into Java's `keystore`.

Prerequisites

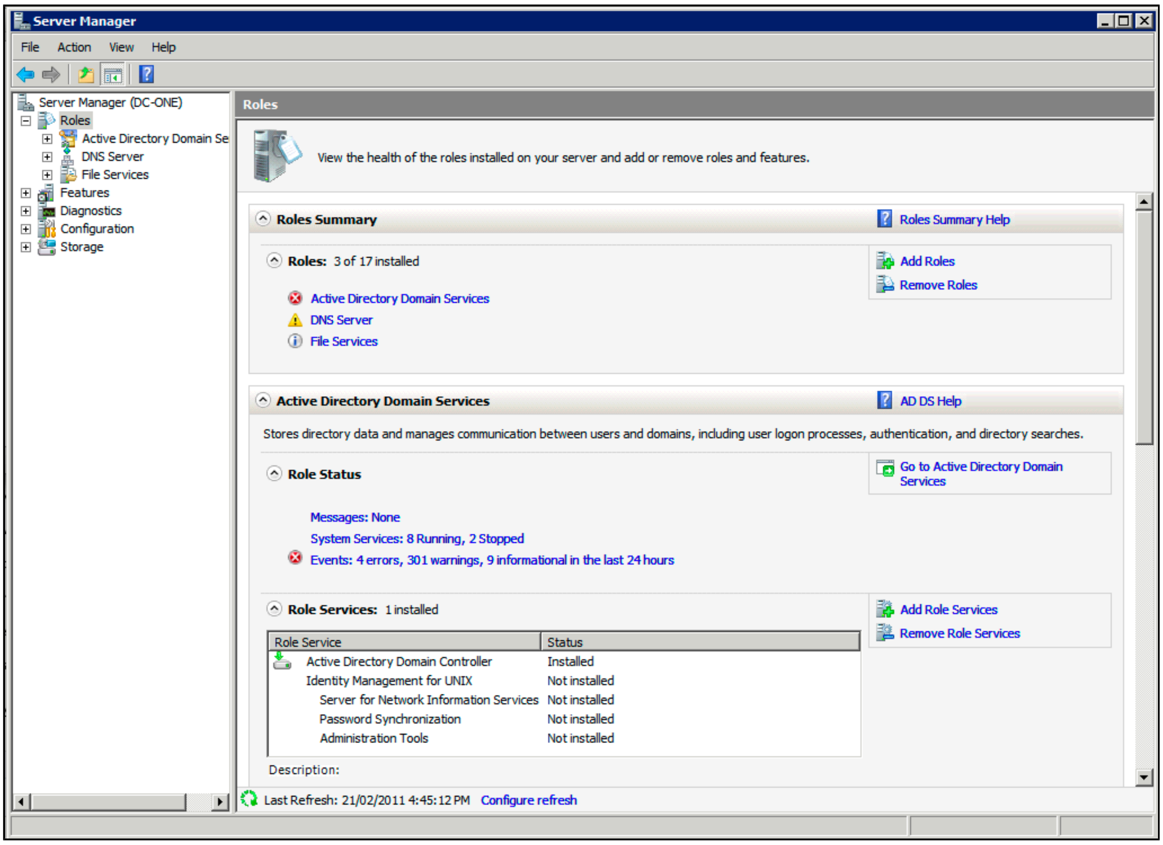
To generate a certificate, you need the following components installed on the Windows Domain Controller to which you're connecting.

Required Component	Description
Internet Information Services (IIS)	This is required before you can install Windows Certificate Services.
Windows Certificate Services	This installs a certification authority (CA) which is used to issue certificates. Step 1, below, explains this process.
Windows 2000 Service Pack 2	Required if you are using Windows 2000
Windows 2000 High Encryption Pack (128-bit)	Required if you are using Windows 2000. Provides the highest available encryption level (128-bit).

Step 1. Install the Active Directory Certificate Services

If Certificate Services are already installed, skip to step 2, below. The screenshots below are from Server 2008, but the process is similar for Server 2000 and 2003.

1. Log in to your Active Directory server as an administrator.
2. Click **Start**, point to **Administrative Tools**, and then click **Server Manager**.
3. In the **Roles Summary** section, click **Add Roles**.



View the health of the roles installed on your server and add or remove roles and features.

Roles Summary

Roles: 3 of 17 installed

- Active Directory Domain Services
- DNS Server
- File Services

Active Directory Domain Services

Stores directory data and manages communication between users and domains, including user logon processes, authentication, and directory searches.

Role Status

Messages: None
System Services: 8 Running, 2 Stopped
Events: 4 errors, 301 warnings, 9 informational in the last 24 hours

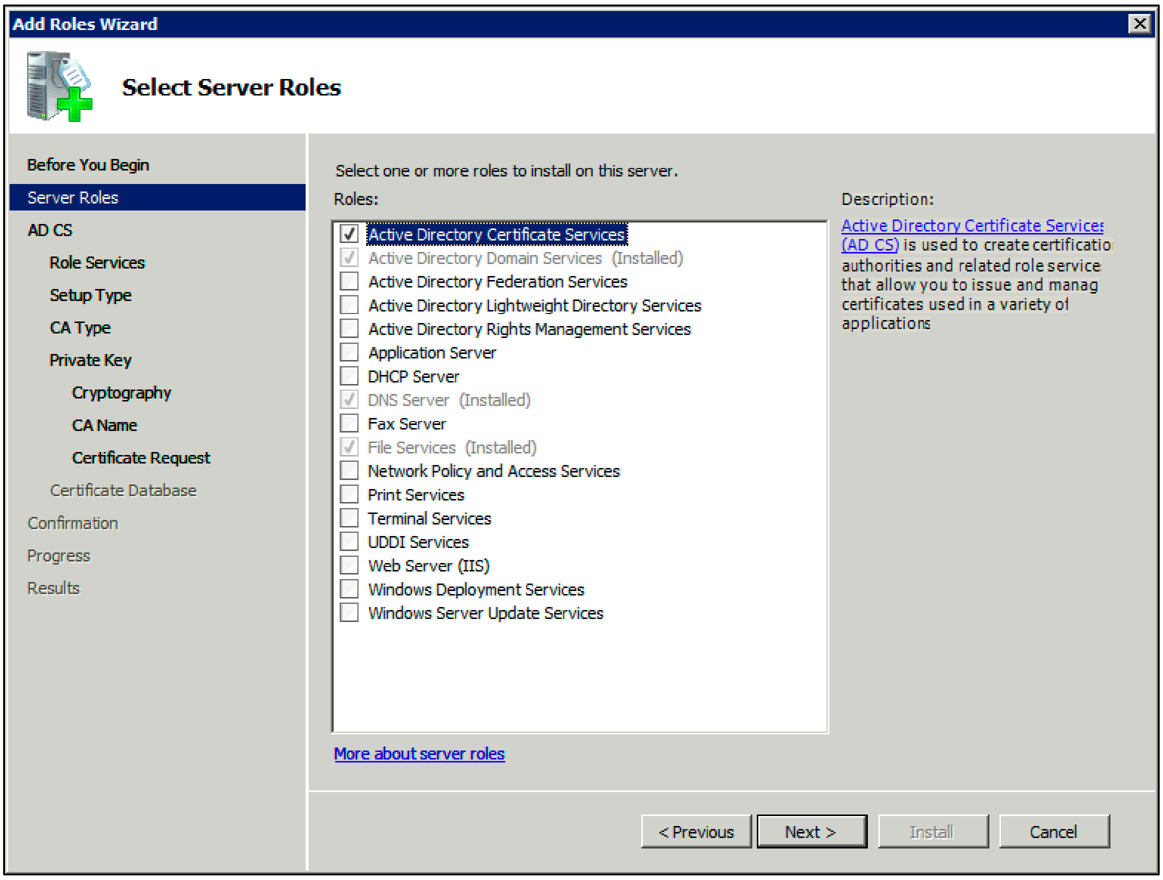
Role Services: 1 installed

Role Service	Status
Active Directory Domain Controller	Installed
Identity Management for UNIX	Not installed
Server for Network Information Services	Not installed
Password Synchronization	Not installed
Administration Tools	Not installed

Description:

Last Refresh: 21/02/2011 4:45:12 PM

4. On the **Select Server Roles** page, select the **Active Directory Certificate Services** check box. Click **Next** twice.



Select one or more roles to install on this server.

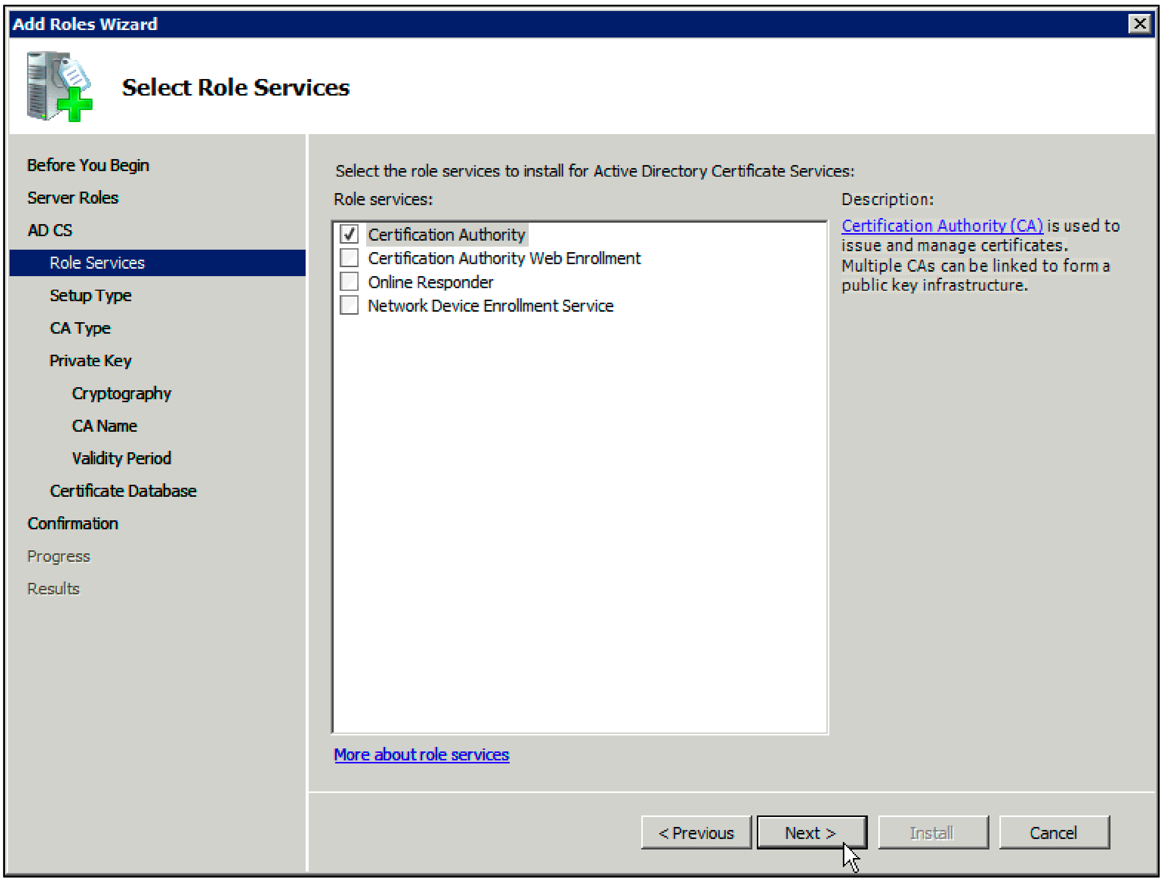
Roles:

☑ Active Directory Certificate Services
☑ Active Directory Domain Services (Installed)
☐ Active Directory Federation Services
☐ Active Directory Lightweight Directory Services
☐ Active Directory Rights Management Services
☐ Application Server
☐ DHCP Server
☑ DNS Server (Installed)
☐ Fax Server
☑ File Services (Installed)
☐ Network Policy and Access Services
☐ Print Services
☐ Terminal Services
☐ UDDI Services
☐ Web Server (IIS)
☐ Windows Deployment Services
☐ Windows Server Update Services

Description:

Active Directory Certificate Services (AD CS) is used to create certificatio authorities and related role service that allow you to issue and manag certificates used in a variety of applications

5. On the **Select Role Services** page, select the **Certification Authority** check box, and then click **Next**.



Select the role services to install for Active Directory Certificate Services:

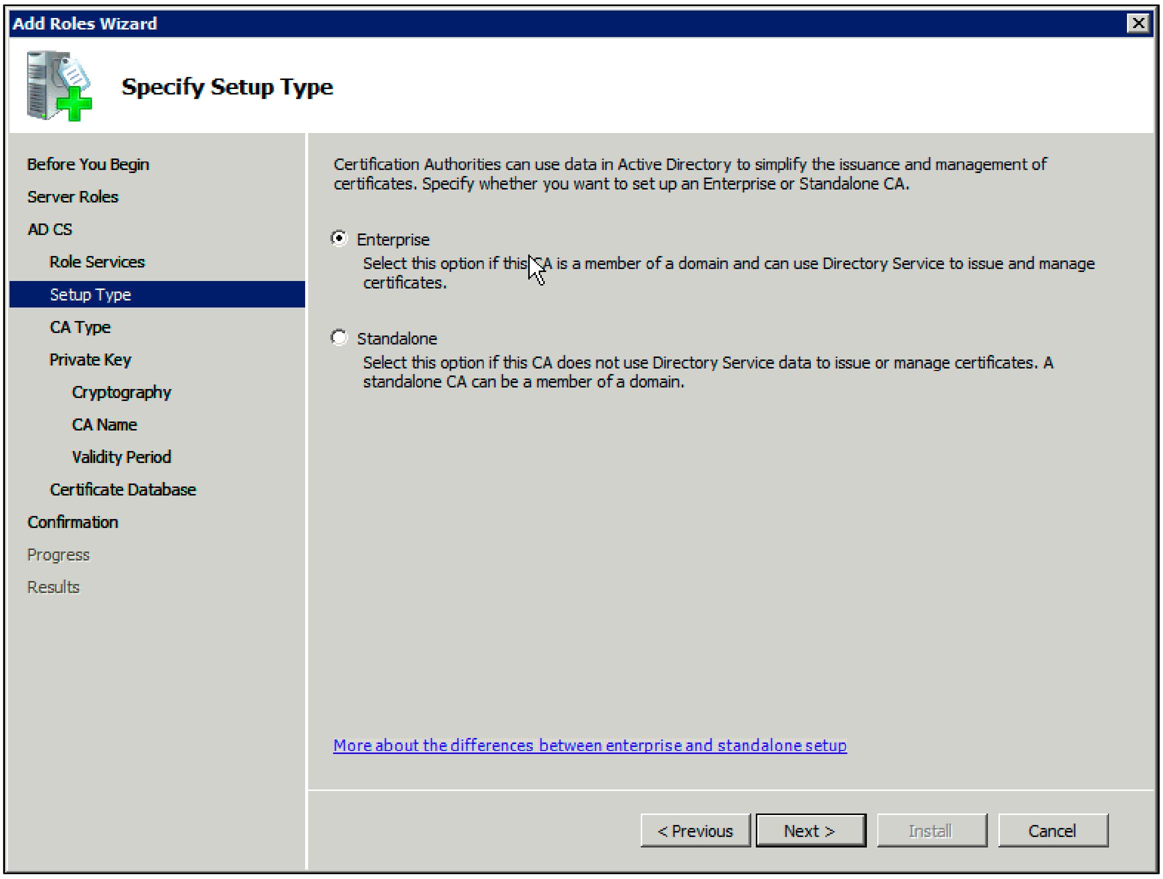
Role services:

- ☑ Certification Authority
- □ Certification Authority Web Enrollment
- □ Online Responder
- □ Network Device Enrollment Service

Description:

Certification Authority (CA) is used to issue and manage certificates. Multiple CAs can be linked to form a public key infrastructure.

6. On the **Specify Setup Type** page, click **Enterprise**, and then click **Next**.

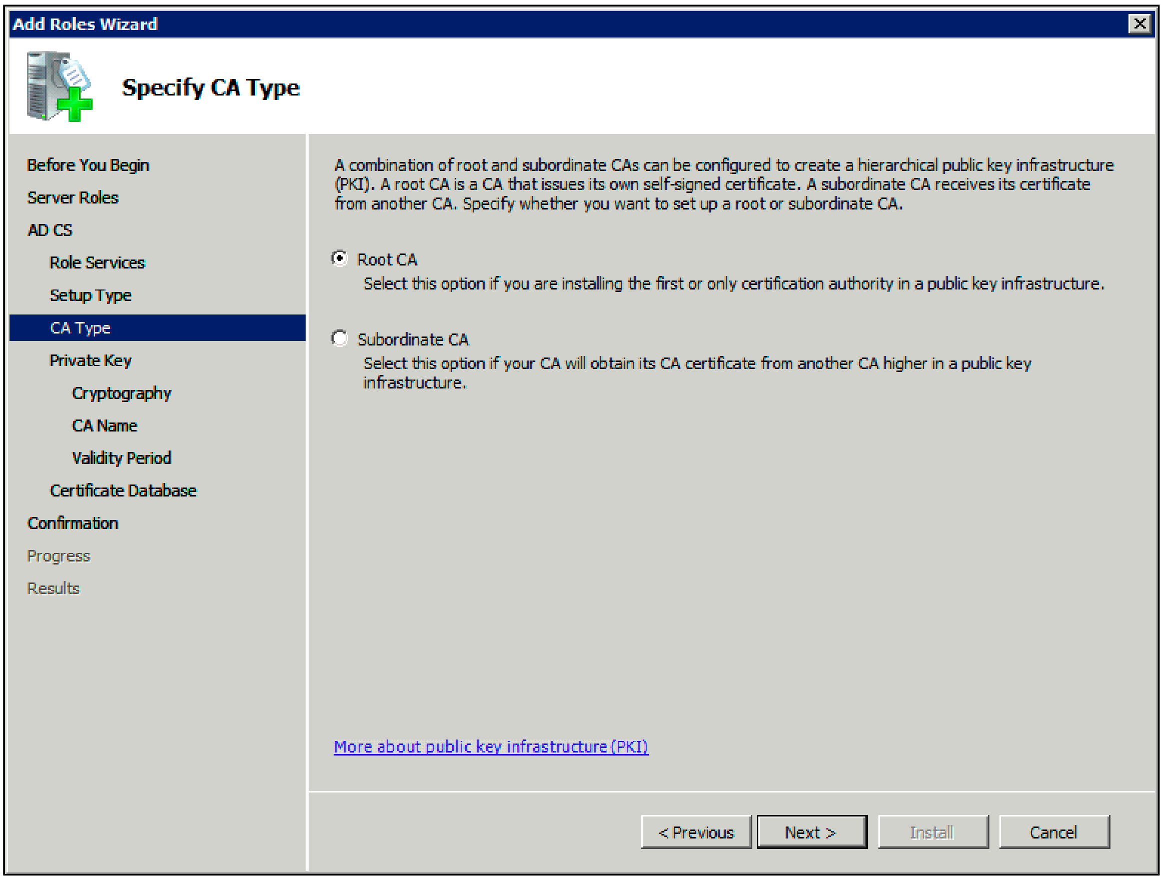


Certification Authorities can use data in Active Directory to simplify the issuance and management of certificates. Specify whether you want to set up an Enterprise or Standalone CA.

● Enterprise
Select this option if this CA is a member of a domain and can use Directory Service to issue and manage certificates.

○ Standalone
Select this option if this CA does not use Directory Service data to issue or manage certificates. A standalone CA can be a member of a domain.

7. On the **Specify CA Type** page, click **Root CA**, and then click **Next**.



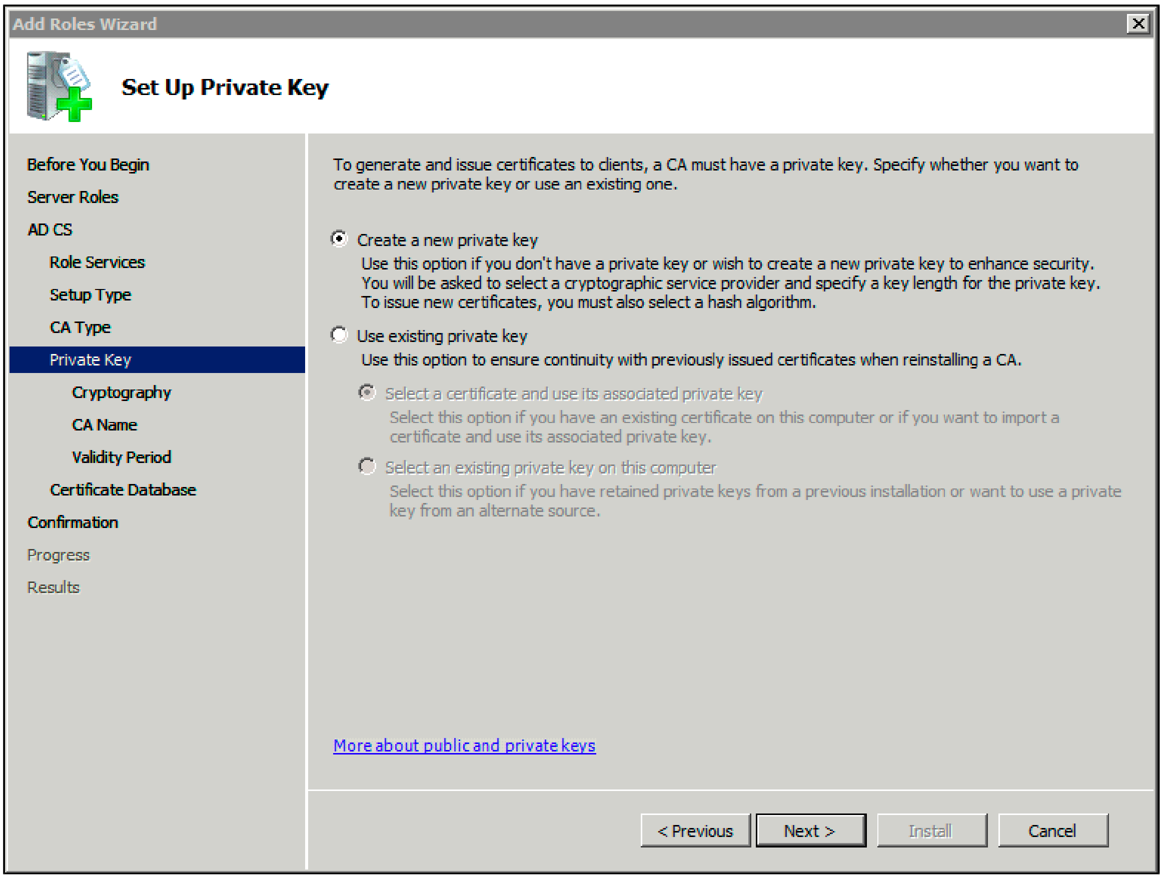
Specify CA Type

A combination of root and subordinate CAs can be configured to create a hierarchical public key infrastructure (PKI). A root CA is a CA that issues its own self-signed certificate. A subordinate CA receives its certificate from another CA. Specify whether you want to set up a root or subordinate CA.

● Root CA
Select this option if you are installing the first or only certification authority in a public key infrastructure.

○ Subordinate CA
Select this option if your CA will obtain its CA certificate from another CA higher in a public key infrastructure.

8. On the **Set Up Private Key** and **Configure Cryptography for CA** pages, you can configure optional configuration settings, including cryptographic service providers. However, the default values should be fine. Click **Next** twice.



Set Up Private Key

To generate and issue certificates to clients, a CA must have a private key. Specify whether you want to create a new private key or use an existing one.

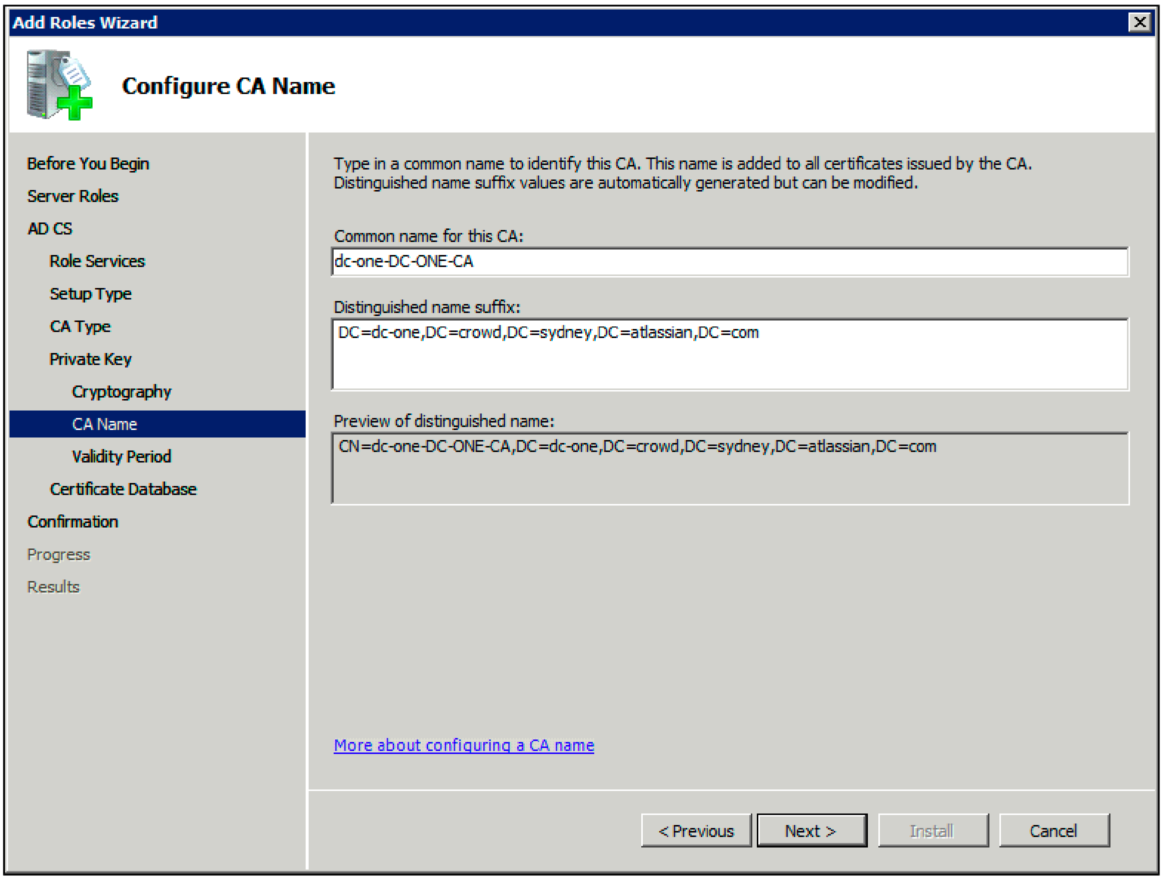
● Create a new private key
Use this option if you don't have a private key or wish to create a new private key to enhance security. You will be asked to select a cryptographic service provider and specify a key length for the private key. To issue new certificates, you must also select a hash algorithm.

○ Use existing private key
Use this option to ensure continuity with previously issued certificates when reinstalling a CA.

● Select a certificate and use its associated private key
Select this option if you have an existing certificate on this computer or if you want to import a certificate and use its associated private key.

○ Select an existing private key on this computer
Select this option if you have retained private keys from a previous installation or want to use a private key from an alternate source.

9. In the **Common name for this CA** box, type the common name of the CA, and then click **Next**.



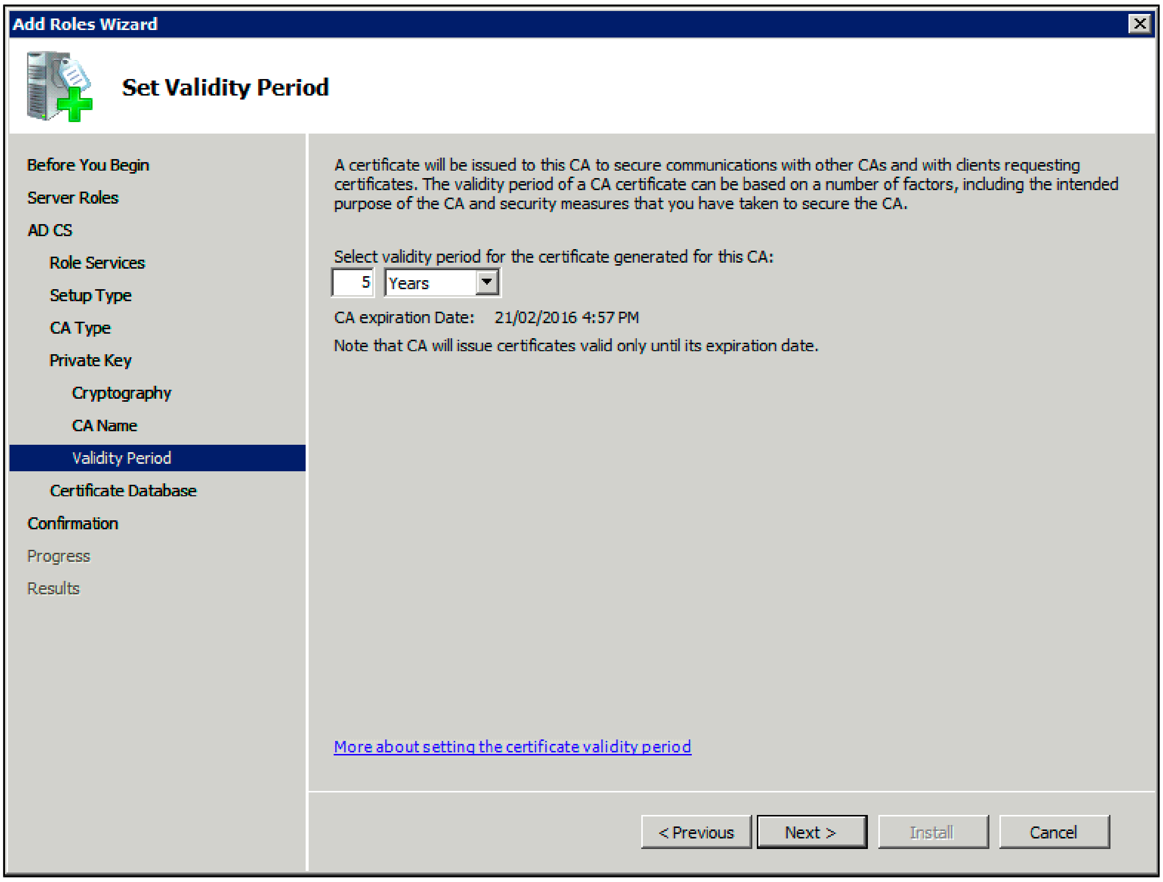
Type in a common name to identify this CA. This name is added to all certificates issued by the CA. Distinguished name suffix values are automatically generated but can be modified.

Common name for this CA: dc-one-DC-ONE-CA

Distinguished name suffix: DC=dc-one,DC=crowd,DC=sydney,DC=atlassian,DC=com

Preview of distinguished name: CN=dc-one-DC-ONE-CA,DC=dc-one,DC=crowd,DC=sydney,DC=atlassian,DC=com

10. On the **Set Validity Period** page, accept the default values or specify other storage locations for the certificate database and the certificate database log, and then click **Next**.



Set Validity Period

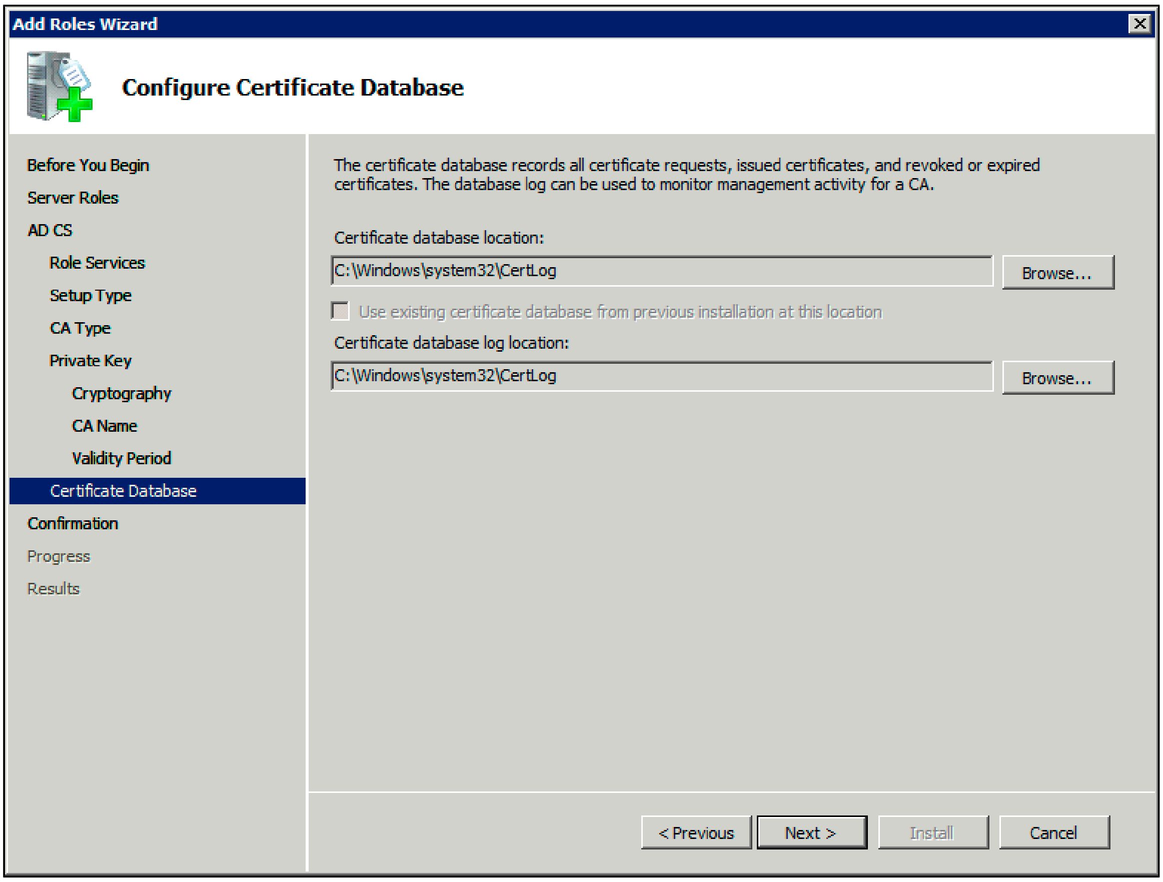
A certificate will be issued to this CA to secure communications with other CAs and with clients requesting certificates. The validity period of a CA certificate can be based on a number of factors, including the intended purpose of the CA and security measures that you have taken to secure the CA.

Select validity period for the certificate generated for this CA:

5 Years

CA expiration Date: 21/02/2016 4:57 PM

Note that CA will issue certificates valid only until its expiration date.



Configure Certificate Database

The certificate database records all certificate requests, issued certificates, and revoked or expired certificates. The database log can be used to monitor management activity for a CA.

Certificate database location:

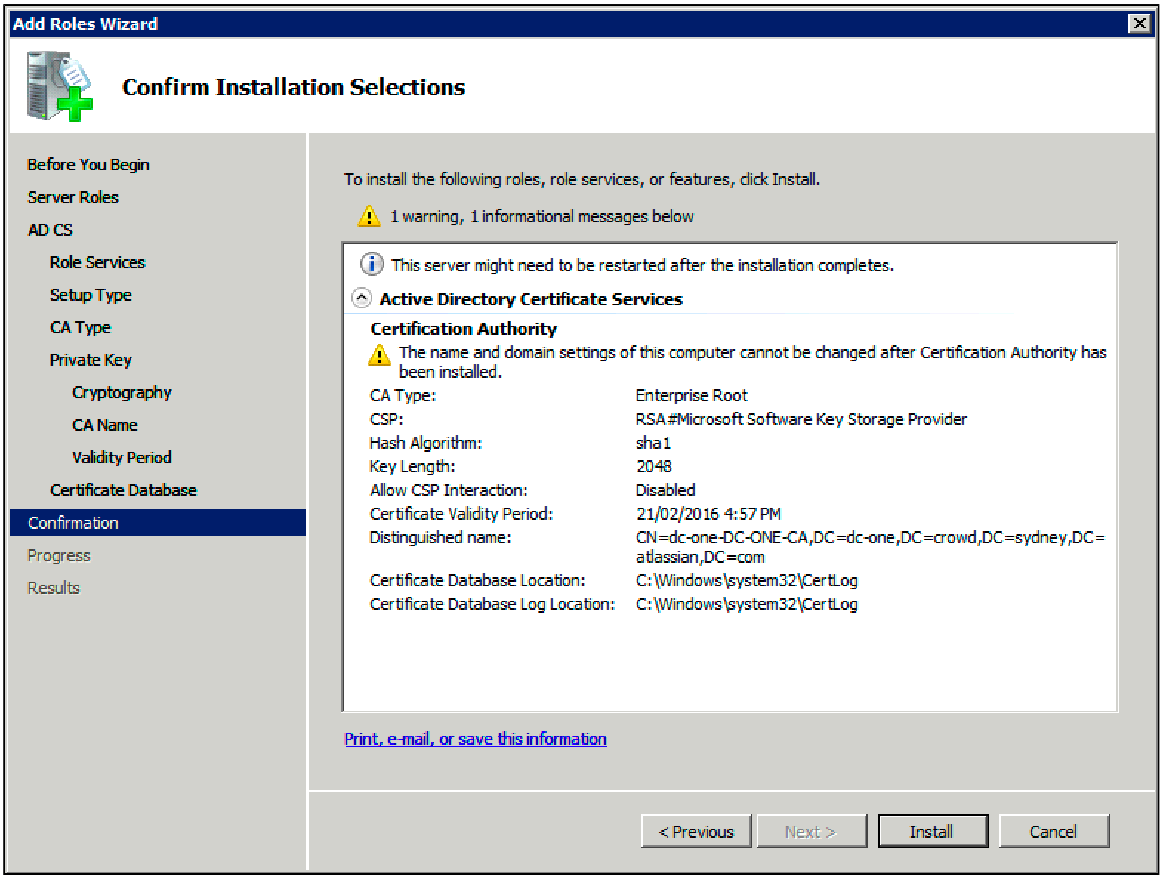
C:\Windows\system32\CertLog

□ Use existing certificate database from previous installation at this location

Certificate database log location:

C:\Windows\system32\CertLog

11. After verifying the information on the **Confirm Installation Selections** page, click **Install**.



Confirm Installation Selections

To install the following roles, role services, or features, click Install.

⚠ 1 warning, 1 informational messages below

ⓘ This server might need to be restarted after the installation completes.

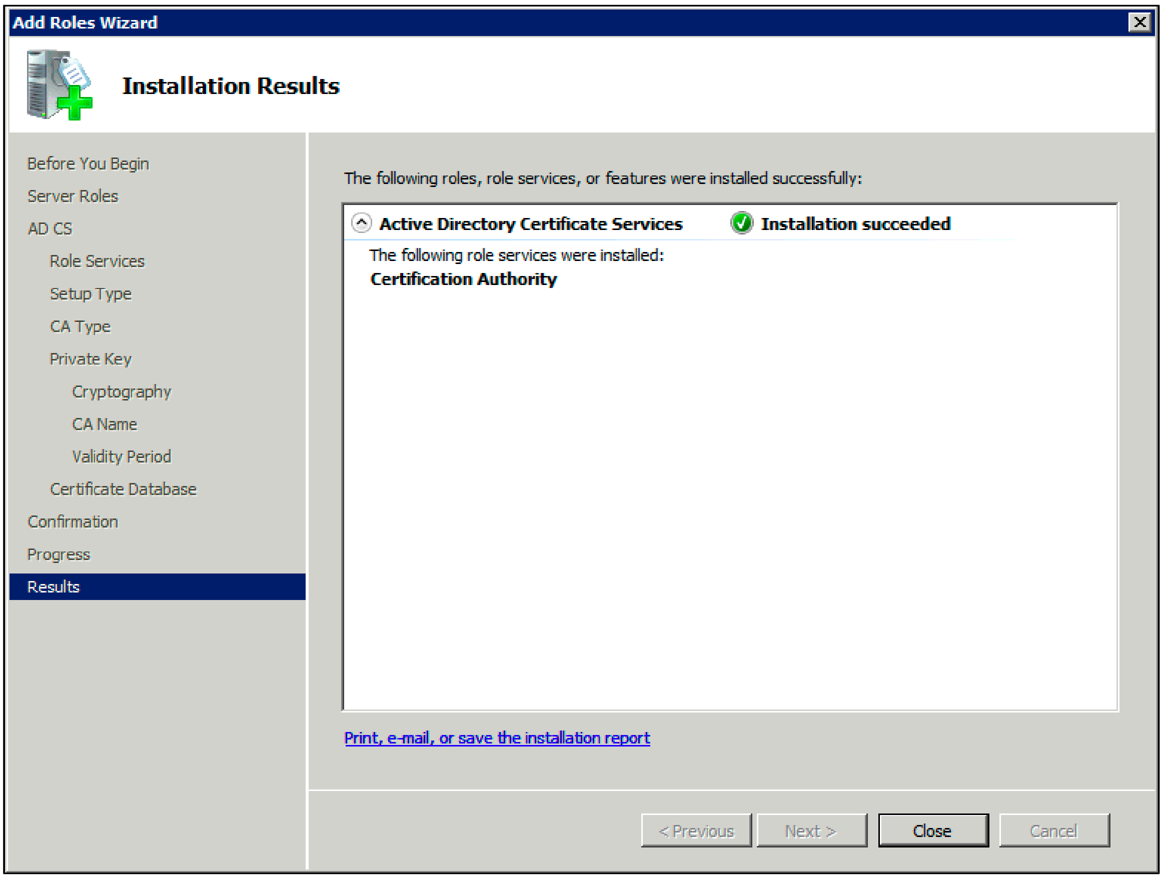
Active Directory Certificate Services

Certification Authority

⚠ The name and domain settings of this computer cannot be changed after Certification Authority has been installed.

CA Type:	Enterprise Root
CSP:	RSA#Microsoft Software Key Storage Provider
Hash Algorithm:	sha1
Key Length:	2048
Allow CSP Interaction:	Disabled
Certificate Validity Period:	21/02/2016 4:57 PM
Distinguished name:	CN=dc-one-DC-ONE-CA,DC=dc-one,DC=crowd,DC=sydney,DC=atlassian,DC=com
Certificate Database Location:	C:\Windows\system32\CertLog
Certificate Database Log Location:	C:\Windows\system32\CertLog

12. Review the information on the results screen to verify that the installation was successful.



Installation Results

The following roles, role services, or features were installed successfully:

Active Directory Certificate Services ✓ **Installation succeeded**

The following role services were installed:

Certification Authority

Step 2. Obtain the Server Certificate

The steps above describe how to install the certification authority (CA) on your Microsoft Active Directory server. Next, you will need to add the Microsoft Active Directory server's SSL certificate to the list of accepted certificates used by the JDK that runs your application server.

The Active Directory certificate is automatically generated and placed in root of the C:\ drive, matching a file format similar to the tree structure of your Active Directory server. For example: `c:\ad2008.ad01.atlassian.com_ad01.crt`.

You can also export the certificate by executing this command on the Active Directory server:

```
certutil -ca.cert client.crt
```

Step 3. Import the Server Certificate

For an application server to trust your directory's certificate, the certificate must be imported into your Java runtime environment. The JDK stores trusted certificates in a file called a keystore. The default keystore file is called `cacerts` and it lives in the `jre\lib\security` sub-directory of your Java installation.

In the following examples, we use `server-certificate.crt` to represent the certificate file exported by your directory server. You will need to alter the instructions below to match the name actually generated.

Windows

1. Navigate to the directory in which Java is installed. It's probably called something like `C:\Program Files\Java\jdk1.5.0_12`.
2. Run the command below, where `server-certificate.crt` is the name of the file from your directory server:

```
keytool -import -keystore .\jre\lib\security\cacerts -file
server-certificate.crt
```

3. `keytool` will prompt you for a password. The default keystore password is `changeit`.
4. When prompted `Trust this certificate? [no]:` enter `yes` to confirm the key import:

```
Enter keystore password:  changeit
Owner: CN=ad01, C=US
Issuer: CN=ad01, C=US
Serial number: 15563d6677a4e9e4582d8a84be683f9
Valid from: Tue Aug 21 01:10:46 ACT 2007 until: Tue Aug 21 01:13:59 ACT
2012
Certificate fingerprints:
         MD5:  D6:56:F0:23:16:E3:62:2C:6F:8A:0A:37:30:A1:84:BE
         SHA1:
73:73:4E:A6:A0:D1:4E:F4:F3:CD:CE:BE:96:80:35:D2:B4:7C:79:C1
Trust this certificate? [no]:  yes
Certificate was added to keystore
```

You may now use the '**Secure SSL**' option when connecting your application to your directory server.

UNIX

1. Navigate to the directory in which Java is installed. `cd $JAVA_HOME` will usually get you there.

2. Run the command below, where `server-certificate.crt` is the name of the file from your directory server:

   ```
   sudo keytool -import -keystore ./jre/lib/security/cacerts -file
   server-certificate.crt
   ```

3. `keytool` will prompt you for a password. The default keystore password is `changeit`.
4. When prompted `Trust this certificate? [no]:` enter yes to confirm the key import:

   ```
   Password:
   Enter keystore password:  changeit
   Owner: CN=ad01, C=US
   Issuer: CN=ad01, C=US
   Serial number: 15563d6677a4e9e4582d8a84be683f9
   Valid from: Tue Aug 21 01:10:46 ACT 2007 until: Tue Aug 21 01:13:59 ACT
   2012
   Certificate fingerprints:
            MD5:  D6:56:F0:23:16:E3:62:2C:6F:8A:0A:37:30:A1:84:BE
            SHA1:
   73:73:4E:A6:A0:D1:4E:F4:F3:CD:CE:BE:96:80:35:D2:B4:7C:79:C1
   Trust this certificate? [no]:  yes
   Certificate was added to keystore
   ```

You may now use the '**Secure SSL**' option when connecting your application to your directory server.

Mac OS X

1. Navigate to the directory in which Java is installed. This is usually `/Library/Java/Home`.
2. Run the command below, where `server-certificate.crt` is the name of the file from your directory server:

   ```
   sudo keytool -import -keystore ./jre/lib/security/cacerts -file
   server-certificate.crt
   ```

3. `keytool` will prompt you for a password. The default keystore password is `changeit`.
4. When prompted `Trust this certificate? [no]:` enter yes to confirm the key import:

   ```
   Password:
   Enter keystore password:  changeit
   Owner: CN=ad01, C=US
   Issuer: CN=ad01, C=US
   Serial number: 15563d6677a4e9e4582d8a84be683f9
   Valid from: Tue Aug 21 01:10:46 ACT 2007 until: Tue Aug 21 01:13:59 ACT
   2012
   Certificate fingerprints:
            MD5:  D6:56:F0:23:16:E3:62:2C:6F:8A:0A:37:30:A1:84:BE
            SHA1:
   73:73:4E:A6:A0:D1:4E:F4:F3:CD:CE:BE:96:80:35:D2:B4:7C:79:C1
   Trust this certificate? [no]:  yes
   Certificate was added to keystore
   ```

You may now use the '**Secure SSL**' option when connecting your application to your directory server.

RELATED TOPICS

Connecting to an LDAP Directory
Configuring User Directories

Administrators Guide Home Confluence Documentation Home

Connecting to an Internal Directory with LDAP Authentication

You can connect your Confluence application to an LDAP directory for delegated authentication. This means that Confluence will have an internal directory that uses LDAP for authentication only. There is an option to create users in the internal directory automatically when they attempt to log in, as described in the settings section.

Overview

An internal directory with LDAP authentication offers the features of an internal directory while allowing you to store and check users' passwords in LDAP only. Note that the 'internal directory with LDAP authentication' is separate from the default 'internal directory'. On LDAP, all that the application does is to check the password. The LDAP connection is read only. Every user in the internal directory with LDAP authentication must map to a user on LDAP, otherwise they cannot log in.

When to use this option: Choose this option if you want to set up a user and group configuration within your application that suits your needs, while checking your users' passwords against the corporate LDAP directory. This option also helps to avoid the performance issues that may result from downloading large numbers of groups from LDAP.

On this page:

⚠ *The information on this page does not apply to Atlassian OnDemand sites with multiple apps. If you are using Confluence-only OnDemand, the information does apply.*

Connecting Confluence to an Internal Directory with LDAP Authentication

To connect to an internal directory but check logins via LDAP:

1. Choose **Browse** > **Confluence Admin**.
2. Click '**User Directories**' in the left-hand panel.
3. **Add** a directory and select type '**Internal with LDAP Authentication**'.
4. Enter the values for the settings, as described below.
5. Save the directory settings.
6. If you want LDAP users to be used in place of existing internal users, move the 'Internal with LDAP Authentication' directory to the top of the list. You can define the **directory order** by clicking the blue up-

and down-arrows next to each directory on the '**User Directories**' screen. Here is a summary of how the directory order affects the processing:
  - The order of the directories is the order in which they will be searched for users and groups.
  - Changes to users and groups will be made only in the first directory where the application has permission to make changes.

  For details see Managing Multiple Directories.

7. Add your users and groups in Confluence. See Adding Users and Adding a Group.

Server Settings

Setting	Description
Name	A descriptive name that will help you to identify the directory. Examples: • `Internal directory with LDAP Authentication` • `Corporate LDAP for Authentication Only`
Directory Type	Select the type of LDAP directory that you will connect to. If you are adding a new LDAP connection, the value you select here will determine the default values for some of the options on the rest of screen. Examples: • `Microsoft Active Directory` • `OpenDS` • And more.
Hostname	The host name of your directory server. Examples: • `ad.example.com` • `ldap.example.com` • `opends.example.com`
Port	The port on which your directory server is listening. Examples: • `389` • `10389` • `636` (for example, for SSL)
Use SSL	Select this check box if the connection to the directory server is an SSL (Secure Sockets Layer) connection. Note that you will need to configure an SSL certificate in order to use this setting.
Username	The distinguished name of the user that the application will use when connecting to the directory server. Examples: • `cn=administrator,cn=users,dc=ad,dc=example,dc=com` • `cn=user,dc=domain,dc=name` • `user@domain.name`

Password	The password of the user specified above.

Copying Users on Login

Setting	Description
Copy User on Login	This option affects what will happen when a user attempts to log in. If this check box is selected, the user will be created automatically in the internal directory that is using LDAP for authentication when the user first logs in and their details will be synchronised on each subsequent log in. If this check box is not selected, the user's login will fail. If you select this check box the following additional fields will appear on the screen, which are described in more detail below: • Default Group Memberships • Synchronise Group Memberships • User Schema Settings (described in a separate section below)
Default Group Memberships	This field appears if you select the **Copy User on Login** check box. If you would like users to be automatically added to a group or groups, enter the group name(s) here. To specify more than one group, separate the group names with commas. Each time a user logs in, their group memberships will be checked. If the user does not belong to the specified group(s), their username will be added to the group(s). If a group does not yet exist, it will be added to the internal directory that is using LDAP for authentication. Please note that there is no validation of the group names. If you mis-type the group name, authorisation failures will result – users will not be able to access the applications or functionality based on the intended group name. Examples: • `confluence-users` • `confluence-users,jira-users,jira-developers`

Synchronise Group Memberships	This field appears if you select the **Copy User on Login** check box. If this check box is selected, group memberships specified on your LDAP server will be synchronised with Confluence each time the user logs in. If you select this check box the following additional fields will appear on the screen, both described in more detail below: • Group Schema Settings (described in a separate section below) • Membership Schema Settings (described in a separate section below)

Schema Settings

Setting	Description
Base DN	The root distinguished name (DN) to use when running queries against the directory server. Examples: • `o=example,c=com` • `cn=users,dc=ad,dc=example,dc=com` • For Microsoft Active Directory, specify the base DN in the following format: `dc=domain1,dc=local`. You will need to replace the `domain1` and `local` for your specific configuration. Microsoft Server provides a tool called `ldp.exe` which is useful for finding out and configuring the the LDAP structure of your server.
User Name Attribute	The attribute field to use when loading the username. Examples: • `cn` • `sAMAccountName`

Advanced Settings

Setting	Description
Use Paged Results	Enable or disable the use of the LDAP control extension for simple paging of search results. If paging is enabled, the search will retrieve sets of data rather than all of the search results at once. Enter the desired page size – that is, the maximum number of search results to be returned per page when paged results are enabled. The default is 1000 results.

Follow Referrals	Choose whether to allow the directory server to redirect requests to other servers. This option uses the node referral (JNDI lookup `java.naming.referral`) configuration setting. It is generally needed for Active Directory servers configured without proper DNS, to prevent a 'javax.naming.PartialResultException: Unprocessed Continuation Reference(s)' error.

User Schema Settings

Note: this section is only visible when **Copy User on Login** is enabled.

Setting	Description
Additional User DN	This value is used in addition to the base DN when searching and loading users. If no value is supplied, the subtree search will start from the base DN. Example: • `ou=Users`
User Object Class	This is the name of the class used for the LDAP user object. Example: • `user`
User Object Filter	The filter to use when searching user objects. Example: • `(&(objectCategory=Person)(sAMAccountName=*))`
User Name RDN Attribute	The RDN (relative distinguished name) to use when loading the username. The DN for each LDAP entry is composed of two parts: the RDN and the location within the LDAP directory where the record resides. The RDN is the portion of your DN that is not related to the directory tree structure. Example: • `cn`
User First Name Attribute	The attribute field to use when loading the user's first name. Example: • `givenName`
User Last Name Attribute	The attribute field to use when loading the user's last name. Example: • `sn`
User Display Name Attribute	The attribute field to use when loading the user's full name. Example: • `displayName`

User Email Attribute	The attribute field to use when loading the user's email address. Example: • `mail`

Group Schema Settings

Note: this section is only visible when both **Copy User on Login** and **Synchronise Group Memberships** are enabled.

Setting	Description
Additional Group DN	This value is used in addition to the base DN when searching and loading groups. If no value is supplied, the subtree search will start from the base DN. Example: • `ou=Groups`
Group Object Class	This is the name of the class used for the LDAP group object. Examples: • `groupOfUniqueNames` • `group`
Group Object Filter	The filter to use when searching group objects. Example: • `(objectCategory=Group)`
Group Name Attribute	The attribute field to use when loading the group's name. Example: • `cn`
Group Description Attribute	The attribute field to use when loading the group's description. Example: • `description`

Membership Schema Settings

Note: this section is only visible when both **Copy User on Login** and **Synchronise Group Memberships** are enabled.

Setting	Description
Group Members Attribute	The attribute field to use when loading the group's members. Example: • `member`

User Membership Attribute	The attribute field to use when loading the user's groups. Example: • `memberOf`
Use the User Membership Attribute, when finding the user's group membership	Select the check box if your directory server supports the group membership attribute on the user. (By default, this is the 'memberOf' attribute.) • If this check box is selected, your application will use the group membership attribute on the user when **retrieving the members of a given group**. This will result in a more efficient retrieval. • If this check box is not selected, your application will use the members attribute on the group ('member' by default) for the search.

Diagrams of Possible Configurations

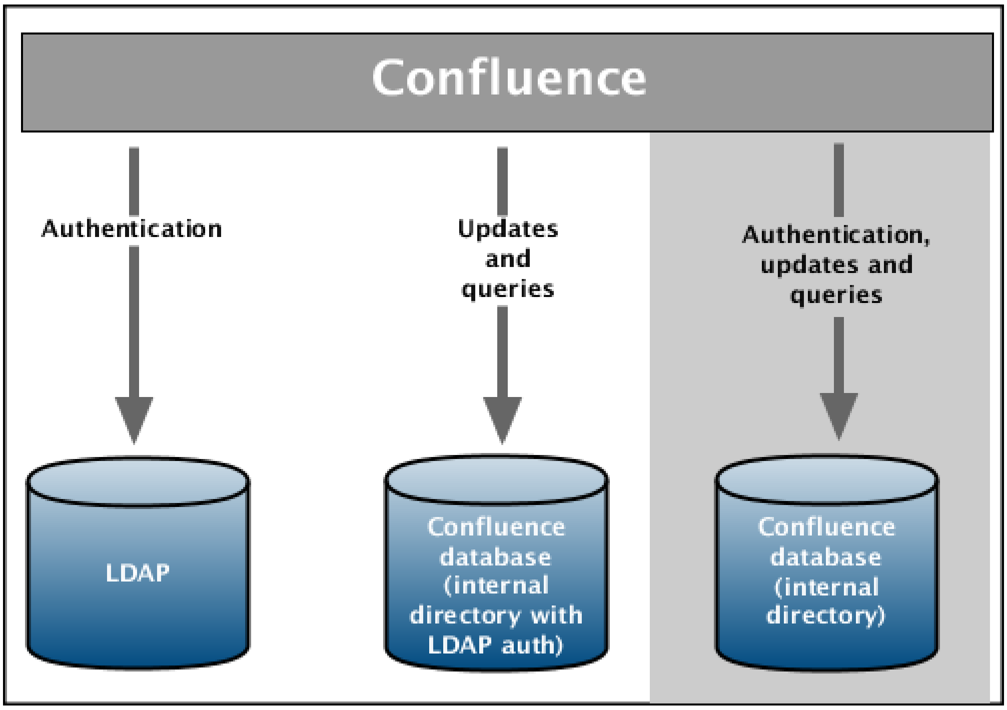

Confluence
Authentication
Updates and queries
Authentication, updates and queries
LDAP
Confluence database (internal directory with LDAP auth)
Confluence database (internal directory)

Diagram above: Confluence connecting to an LDAP directory for authentication only.

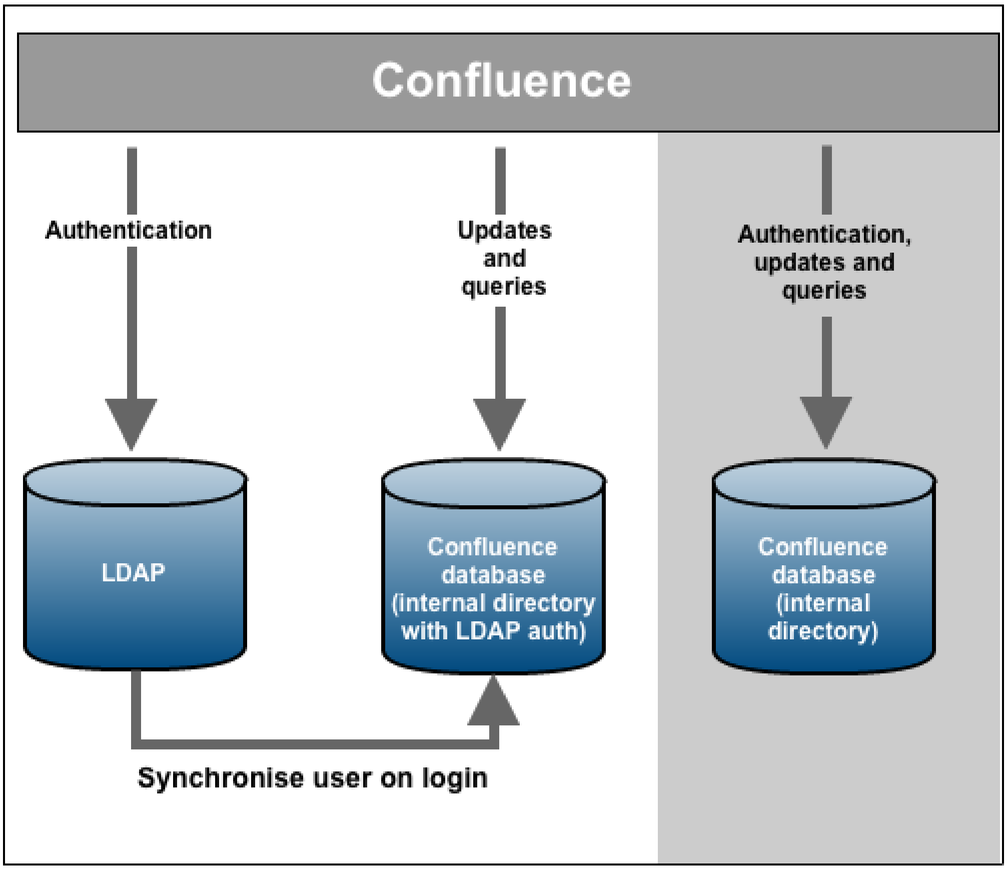

Confluence
Authentication
Updates and queries
Authentication, updates and queries
LDAP
Confluence database (internal directory with LDAP auth)
Confluence database (internal directory)
Synchronise user on login

Diagram above: Confluence connecting to an LDAP directory for authentication only, with each user synchronised with the internal directory that is using LDAP authentication when they log in to Confluence.

RELATED TOPICS

Configuring User Directories

- Configuring the Internal Directory
- Connecting to an LDAP Directory
- Connecting to an Internal Directory with LDAP Authentication
- Connecting to Crowd or JIRA for User Management
- Connecting to JIRA 4.2 or Earlier for User Management
- Managing Multiple Directories
- Managing Nested Groups
- Synchronising Data from External Directories
- Diagrams of Possible Configurations for User Management
- User Management Limitations and Recommendations
- Requesting Support for External User Management

Administrators Guide Home Confluence Documentation Home

Connecting to Crowd or JIRA for User Management

You can connect your Confluence application to Atlassian Crowd or to JIRA (version 4.3 or later) for management of users and groups, and for authentication (verification of a user's login).

On this page:

⚠ *The information on this page does not apply to Confluence OnDemand.*

Connecting Confluence to Crowd for User Management

Atlassian Crowd is an application security framework that handles authentication and authorisation for your web-based applications. With Crowd you can integrate multiple web applications and user directories, with support for single sign-on (SSO) and centralised identity management. The Crowd Administration Console provides a web interface for managing directories, users and their permissions. See the Crowd Administration Guide.

When to use this option: Connect to Crowd if you want to use the full Crowd functionality to manage your directories, users and groups. You can connect your Crowd server to a number of directories of all types that Crowd supports, including custom directory connectors.

To connect Confluence to Crowd:

1. Go to your **Crowd Administration Console** and define the Confluence application to Crowd. See the Crowd documentation: Adding an Application.
2. Choose **Browse** > **Confluence Admin**.
3. Click '**User Directories**' in the left-hand panel.
4. **Add** a directory and select type '**Atlassian Crowd**'. Enter the settings as described below.
5. Save the directory settings.
6. Define the **directory order** by clicking the blue up- and down-arrows next to each directory on the '**User Directories**' screen. Here is a summary of how the directory order affects the processing:
    - The order of the directories is the order in which they will be searched for users and groups.
    - Changes to users and groups will be made only in the first directory where the application has permission to make changes.

    For details see Managing Multiple Directories.
7. If required, configure Confluence to use Crowd for single sign-on (SSO) too. See the Crowd documentation: Integrating Crowd with Atlassian Confluence.

Crowd Settings in Confluence

Setting	Description
Name	A meaningful name that will help you to identify this Crowd server amongst your list of directory servers. Examples: • `Crowd Server` • `Example Company Crowd`
Server URL	The web address of your Crowd console server. Examples: • `http://www.example.com:8095/crowd/` • `http://crowd.example.com`
Application Name	The name of your application, as recognised by your Crowd server. Note that you will need to define the application in Crowd too, using the Crowd administration Console. See the Crowd documentation on adding an application.

Application Password	The password which the application will use when it authenticates against the Crowd framework as a client. This must be the same as the password you have registered in Crowd for this application. See the Crowd documentation on adding an application.

Crowd Permissions

Setting	Description
Read Only	The users, groups and memberships in this directory are retrieved from Crowd and can only be modified via Crowd. You cannot modify Crowd users, groups or memberships via the application administration screens.
Read/Write	The users, groups and memberships in this directory are retrieved from Crowd. When you modify a user, group or membership via the application administration screens, the changes will be applied directly to Crowd. Please ensure that the application has modification permissions for the relevant directories in Crowd. See the Crowd documentation: Specifying an Application's Directory Permissions.

Advanced Crowd Settings

Setting	Description
Enable Nested Groups	Enable or disable support for nested groups. Before enabling nested groups, please check to see if the user directory or directories in Crowd support nested groups. When nested groups are enabled, you can define a group as a member of another group. If you are using groups to manage permissions, you can create nested groups to allow inheritance of permissions from one group to its sub-groups.
Synchronisation Interval (minutes)	Synchronisation is the process by which the application updates its internal store of user data to agree with the data on the directory server. The application will send a request to your directory server every x minutes, where 'x' is the number specified here. The default value is 60 minutes.

Connecting Confluence to JIRA for User Management

> Note that the license tiers for JIRA and Confluence do not need to match to use this feature. For example, you can manage a Confluence 50 user license with JIRA, even if JIRA only has a 25 user license.

Subject to certain limitations, you can connect a number of Atlassian web applications to a single JIRA server for centralised user management.

When to use this option: You can only connect to a server running **JIRA 4.3 or later**. Choose this option as an alternative to Atlassian Crowd, for simple configurations with a limited number of users.

If you are running JIRA 4.2 or earlier, please see Connecting to JIRA 4.2 or Earlier for User Management.

To connect Confluence to JIRA 4.3 or later:

1. Go to your **JIRA administration screen** and define the Confluence application to JIRA:
   - For JIRA 4.3.x, select **'Other Applications'** from the **'Users, Groups & Roles'** section of the 'Administration' menu.
   - For JIRA 4.4 or later, select **'Users' > 'JIRA User Server'** in Administration mode.
   - Click **'Add Application'**.
   - Enter the **application name** and **password** that Confluence will use when accessing JIRA.
   - Enter the **IP address** or addresses of your Confluence server. Valid values are:
     - A full IP address, e.g. `192.168.10.12`.
     - A wildcard IP range, using CIDR notation, e.g. `192.168.10.1/16`. For more information, see the introduction to CIDR notation on Wikipedia and RFC 4632.
   - **Save** the new application.
2. Set up the JIRA user directory in Confluence:
   - Choose **Browse** > **Confluence Admin**.
   - Click '**User Directories**' in the left-hand panel.
   - **Add** a directory and select type '**Atlassian JIRA**'.
   - Enter the settings as described below. When asked for the **application name** and **password**, enter the values that you defined for your Confluence application in the settings on JIRA.
   - Save the directory settings.
   - Define the **directory order** by clicking the blue up- and down-arrows next to each directory on the ' **User Directories**' screen. Here is a summary of how the directory order affects the processing:
     - The order of the directories is the order in which they will be searched for users and groups.
     - Changes to users and groups will be made only in the first directory where the application has permission to make changes.

   For details see Managing Multiple Directories.
3. In order to use Confluence, users must be a member of the `confluence-users` group or have Confluence 'can use' permission. Follow these steps to configure your Confluence groups in JIRA:
   a. Add the `confluence-users` and `confluence-administrators` groups in JIRA.
   b. Add your own username as a member of both of the above groups.
   c. Choose one of the following methods to give your existing JIRA users access to Confluence:
      - Option 1: In JIRA, find the groups that the relevant users belong to. Add the groups as members of one or both of the above Confluence groups.
      - Option 2: Log in to Confluence using your JIRA account and go to the Confluence **Administration Console**. Click '**Global Permissions**' and assign the '**can use**' permission to the relevant JIRA groups.

JIRA Settings in Confluence

Setting	Description
Name	A meaningful name that will help you to identify this JIRA server amongst your list of directory servers. Examples: • `JIRA Server` • `My Company JIRA`

Server URL	The web address of your JIRA server. Examples: - `http://www.example.com/8080` - `http://jira.example.com`
Application Name	The name used by your application when accessing the JIRA server that acts as user manager. Note that you will also need to define your application to that JIRA server, via the '**Other Applications**' option in the 'Users, Groups & Roles' section of the 'Administration' menu.
Application Password	The password used by your application when accessing the JIRA server that acts as user manager.

JIRA Permissions

Setting	**Description**
Read Only	The users, groups and memberships in this directory are retrieved from the JIRA server that is acting as user manager. They can only be modified via that JIRA server.
Read/Write	The users, groups and memberships in this directory are retrieved from the JIRA server that is acting as user manager. When you modify a user, group or membership, the changes will be applied directly to your application and to the JIRA server that is acting as user manager.

Advanced JIRA Settings

Setting	**Description**
Enable Nested Groups	Enable or disable support for nested groups. Before enabling nested groups, please check to see if nested groups are enabled on the JIRA server that is acting as user manager. When nested groups are enabled, you can define a group as a member of another group. If you are using groups to manage permissions, you can create nested groups to allow inheritance of permissions from one group to its sub-groups.
Synchronisation Interval (minutes)	Synchronisation is the process by which the application updates its internal store of user data to agree with the data on the directory server. The application will send a request to your directory server every x minutes, where 'x' is the number specified here. The default value is 60 minutes.

Diagrams of Some Possible Configurations

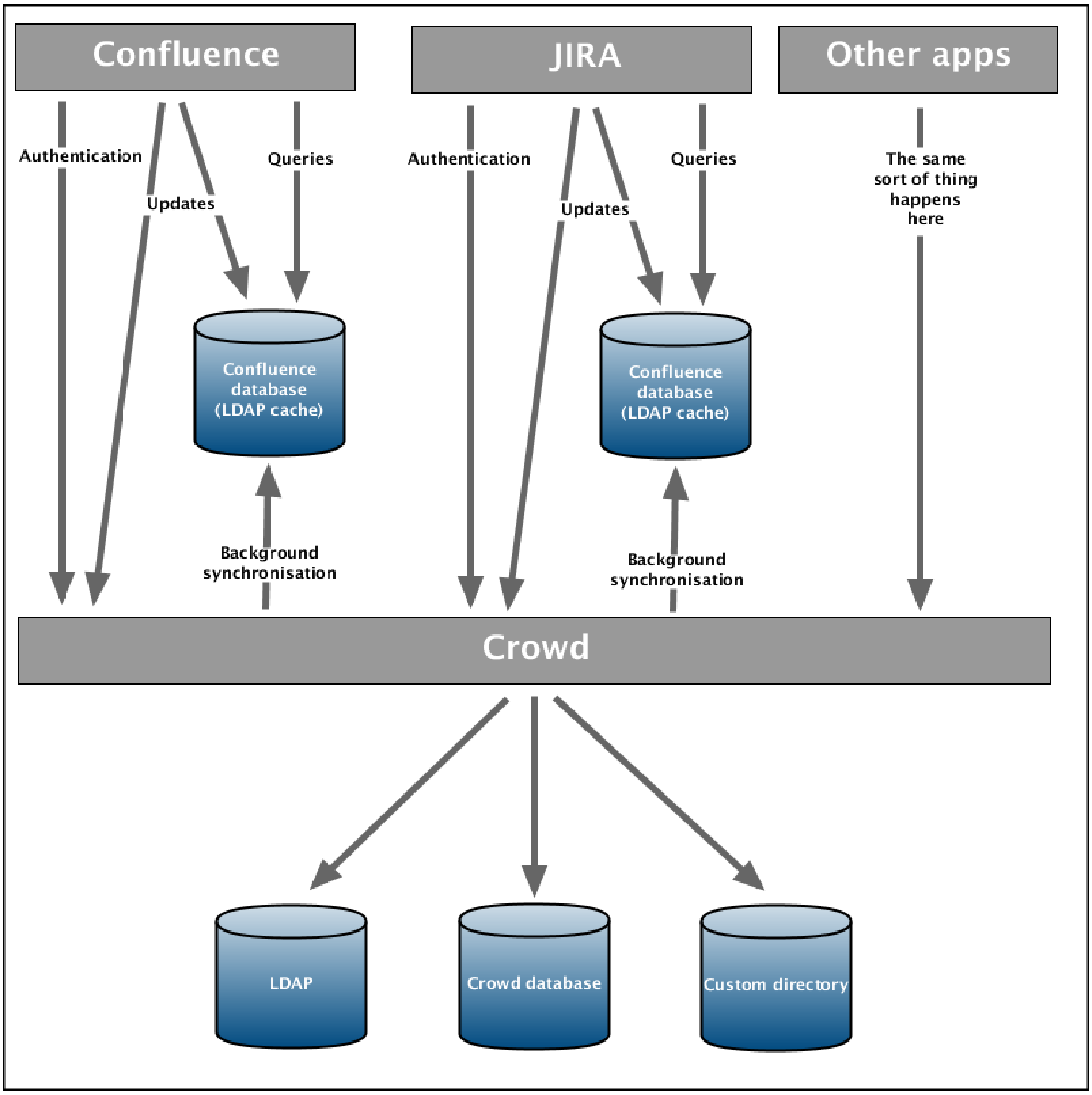

Confluence
JIRA
Other apps
Authentication
Updates
Queries
Authentication
Updates
Queries
The same sort of thing happens here
Confluence database (LDAP cache)
Confluence database (LDAP cache)
Background synchronisation
Background synchronisation
Crowd
LDAP
Crowd database
Custom directory

Diagram above: Confluence, JIRA and other applications connecting to Crowd for user management.

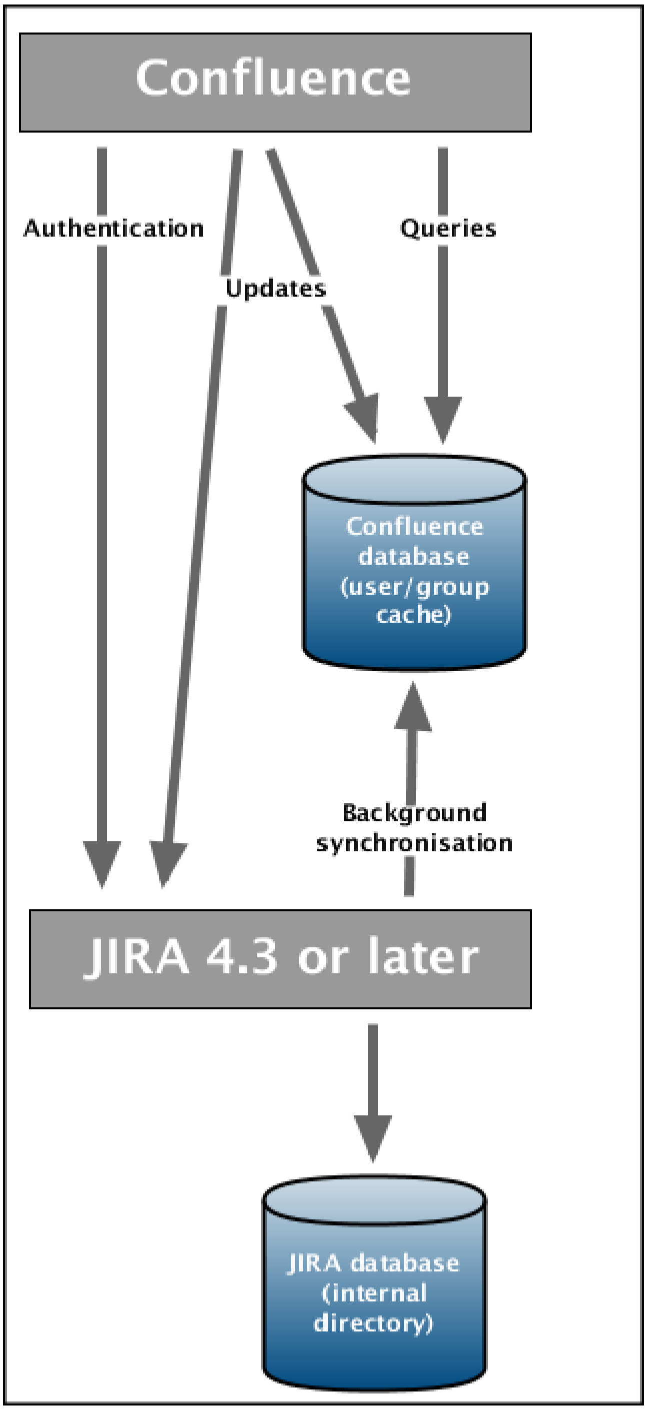

Confluence
Authentication
Updates
Queries
Confluence database (user/group cache)
Background synchronisation
JIRA 4.3 or later
JIRA database (internal directory)

Diagram above: Confluence connecting to JIRA for user management.

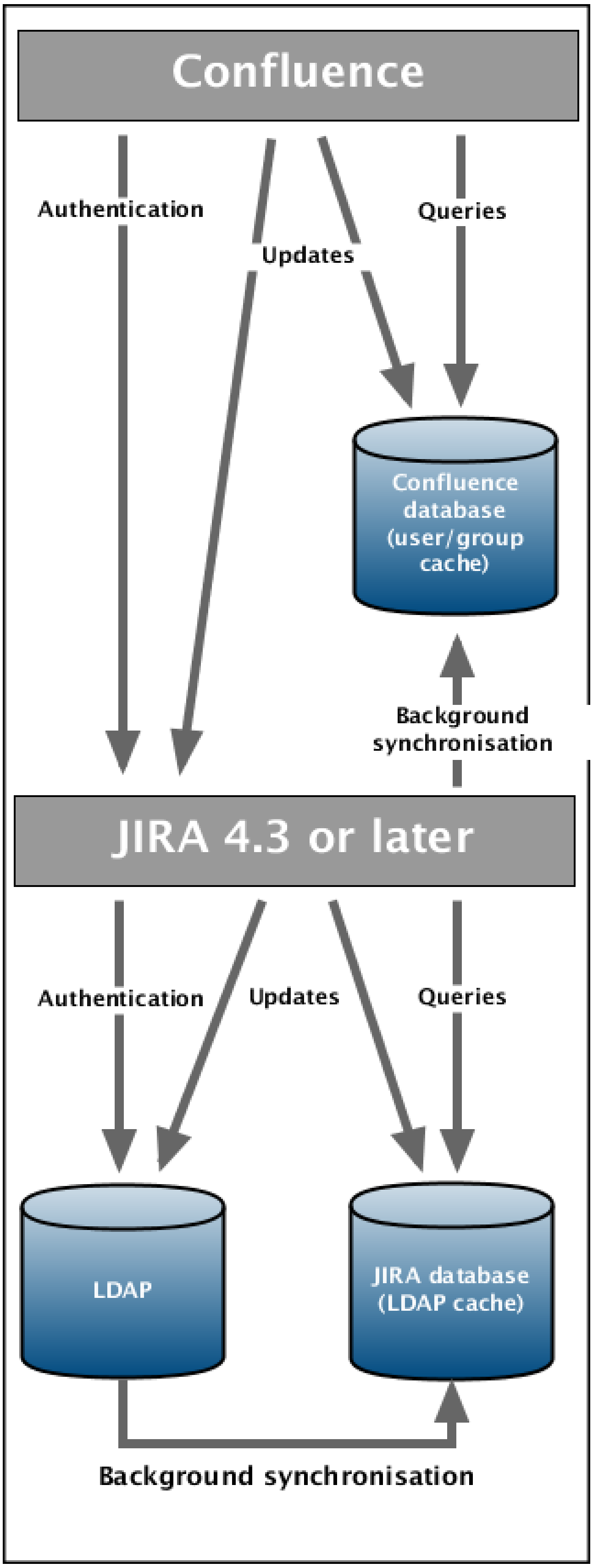

Confluence
Authentication
Updates
Queries
Confluence database (user/group cache)
Background synchronisation
JIRA 4.3 or later
Authentication
Updates
Queries
LDAP
JIRA database (LDAP cache)
Background synchronisation

Diagram above: Confluence connecting to JIRA for user management, with JIRA in turn connecting to LDAP.

RELATED TOPICS

Configuring User Directories

- Configuring the Internal Directory

- Connecting to an LDAP Directory
- Connecting to an Internal Directory with LDAP Authentication
- Connecting to Crowd or JIRA for User Management
- Connecting to JIRA 4.2 or Earlier for User Management
- Managing Multiple Directories
- Managing Nested Groups
- Synchronising Data from External Directories
- Diagrams of Possible Configurations for User Management
- User Management Limitations and Recommendations
- Requesting Support for External User Management

Administrators Guide Home Confluence Documentation Home

Reverting from Crowd or JIRA to Internal User Management

If your Confluence site currently uses JIRA or Crowd for user management, you can revert to internal user management as described below. If your Confluence instance has only a few users, it is easier to recreate the users and groups in Confluence manually. If you have a large number of users and groups, it is more efficient to migrate the relevant users and groups into the Confluence Internal directory.

> ⚠ Both options provided below will reset the affected users' passwords. When done, be sure to notify them to use the 'Reset My Password' link on the Confluence log in page before they attempt to log in.

On this page:

> ⚠ *The information on this page does not apply to Atlassian OnDemand sites with multiple apps. If you are using Confluence-only OnDemand, the information does apply.*

Option 1 – Manually Recreate Users and Groups in Confluence

Use this option if you have only a few users and groups.

1. Log in to Confluence as a Confluence system administrator.
2. Go to the user directories administration screen and move the **internal** directory to the top of the list of directories, by clicking the arrows in the '**Order**' column.
3. Make sure that you have at least one user from the **internal** directory in each of the `confluence-users` and `confluence-administrators` groups.
4. Make sure that you have a username in the **internal**directory with Confluence system administrator permissions.
    - If you do not have such a user, add a new one now, and log out of Confluence.
    - Log back in as the user you just added, and go back to the user directories administration screen.
5. Disable the '**Atlassian Crowd**' directory.
6. Manually add the required users and groups in Confluence. They will be added to the internal directory, because you have moved it to the top of the list of directories.
    - If you have assigned Confluence permissions to a group which exists in JIRA, you must create a group in Confluence with the same name.
    - If a user who exists in JIRA has created content or has had permissions assigned to them in Confluence, you must also create that user in Confluence.
7. Add the users to the required groups.

Option 2 – Transfer Crowd/JIRA Users and Groups to the Confluence Database

Use this option to migrate External Application (Crowd or JIRA) users into the Confluence database. You need a knowledge of SQL to perform this task.

The SQL commands given below are tailored for **MySQL**. If you are using a database other than MySQL, you will need to modify the SQL to work in your database.

Step 1. Create Backups

Creating backups is the only way to restore your data if something goes wrong.

1. From Confluence, create a full XML site backup including attachments.
2. Stop Confluence.
3. Make a backup copy of the Confluence home and installation directories.
4. Repeat the above steps for your External Application.
5. From your MySQL administration tool, create a database backup for the Crowd/JIRA and Confluence databases.

Step 2. Replace Confluence User Management

Use the SQL below to move groups and users from your External Application to Confluence by transferring table content. The SQL provided is specific to MySQL and must be modifed for other databases.

Find the IDs for your Directories

1. Run the following command and take note of the resulting number. It will be referenced throughout the following instructions as <Confluence Internal ID>.

   ```
   select id from cwd_directory where directory_name='Confluence Internal
   Directory';
   ```

2. From the User Directories administration page, find the name of the directory who's users/groups you want to move. Run the following command and take note of the resulting number. It will be referenced throughout the following instructions as <External Application ID>.

   ```
   select id from cwd_directory where directory_name='<External Directory
   Name>';
   ```

Move Groups to Confluence

1. It is possible that you have several groups in your Internal Directory that have the same name as groups in your External Application. To find these, run:

   ```
   select distinct a.id, a.directory_id, a.group_name, d.directory_name
   from cwd_group a join cwd_group b on a.group_name=b.group_name join
   cwd_directory d on d.id=a.directory_id where a.directory_id !=
   b.directory_id;
   ```

   a. If you have results from the previous query, for each of the group names that have duplicates, find the id for the group in the Confluence Internal Directory (<internal group id>) and the External Application (<external group id>). Run the following:

```
update cwd_group_attribute set group_id=<internal group id>,
directory_id=<Confluence Internal Id> where group_id=<external
group id>;
update cwd_membership set child_group_id=<internal group id> where
child_group_id=<external group id>;
update cwd_membership set parent_id=<internal group id> where
parent_id=<external group id>;
delete from cwd_group where id=<external group id>;
```

2. Move all the groups in the External Application to the Confluence Internal Directory.

```
update cwd_group set directory_id=<Confluence Internal ID> where
directory_id=<External Application ID>;
```

Move Users to Confluence

1. It is possible that you have several users in your Internal Directory that have the same name as users in your External Application. To find these, run:

```
select distinct a.id, a.directory_id, a.user_name, d.directory_name
from cwd_user a join cwd_user b on a.user_name=b.user_name join
cwd_directory d on d.id=a.directory_id where a.directory_id !=
b.directory_id;
```

   a. If you have results from the previous query, for each of the user names that have duplicates, find the id for the user in the Confluence Internal Directory (<internal user id>) and the External Application (<external user id>). Run the following:

```
update cwd_membership set child_user_id=<internal user id> where
child_user_id=<external user id>;
update cwd_user_credential_record set user_id=<internal user id>
where user_id=<external user id>;
update cwd_user_attribute set user_id=<internal user id>,
directory_id=<Confluence Internal ID> where user_id=<external user
id>;
delete from cwd_user where id=<external user id>;
```

2. Move all the users in the External Application to the Confluence Internal Directory.

```
update cwd_user set directory_id=<Confluence Internal ID> where
directory_id=<External Application ID>;
```

Delete the External Application directory

1. You need to change the order of your directories so that the Internal directory is at the top, and active.

a. If you have only two directories - the Internal and the External Application directory you are deleting, then do the following:

   ```
   update cwd_app_dir_mapping set list_index = 0 where directory_id =
   <Confluence Internal ID>;
   ```

b. If you have more than two directories, you need to rearrange them so the Internal Directory is at the top (list_index 0) and the External Application directory you are deleting is at the bottom.
   - List the directories and their order using

     ```
     select d.id, d.directory_name, m.list_index from
     cwd_directory d join cwd_app_dir_mapping m on
     d.id=m.directory_id order by m.list_index;
     ```

   - Change the list indexes so that they are in the order you want. Directory order can be rearranged using

     ```
     update cwd_app_dir_mapping set list_index = <position> where
     directory_id = <directory id>;
     ```

c. Check that the internal directory is enabled.
   - List the internal directory. An enabled directory will have its 'active' column set to 'T'

     ```
     select id, directory_name, active from cwd_directory where
     id = <Internal Directory id>;
     ```

   - If the internal directory is not active, activate it by

     ```
     update cwd_directory set active = 'T' where id = <Internal
     Directory id>;
     ```

2. When the directories are ordered correctly, delete the External Application directory from the directory order:

   ```
   delete from cwd_app_dir_operation where app_dir_mapping_id = (select id
   from cwd_app_dir_mapping where directory_id = <External Application
   ID>);
   delete from cwd_app_dir_mapping where directory_id = <External
   Application ID>;
   ```

3. The External Application directory is referenced in several other tables in the database. You need to remove the remaining references to it:

```
delete from cwd_directory_attribute where directory_id=<External
Application ID>;
delete from cwd_directory_operation where directory_id=<External
Application ID>;
```

4. All references to the External Directory should now have been removed. Delete the directory using:

```
delete from cwd_directory where id = <External Application ID>;
```

Reset passwords

1. All users who were in the External Directory you deleted, including admins, will be unable to log in. Their passwords need to be reset by choosing the 'Forgot your password?' link on the login page. Alternatively, use the instructions at Restoring Passwords To Recover Admin User Rights to reset the administrator password, then set the users' passwords for them via the Manage Users page in the administration screen.

RELATED TOPICS

Configuring User Directories

Connecting to JIRA 4.2 or Earlier for User Management

Atlassian JIRA is an issue and project tracking tool. Like Confluence, JIRA offers the ability to store its users and groups in its database. You can configure Confluence to look for its users and groups in the JIRA database. This page describes the **legacy JIRA database connector**, which provides a direct connection to the JIRA database.

When to use this option: Choose the legacy JIRA database connector if your JIRA server is **JIRA 4.2 or earlier**, for backwards compatibility with the already-existing option for Confluence to use JIRA for user management.

*If you are using **JIRA 4.3 or later**, you cannot use the legacy JIRA database connector. Instead, choose the '**Atlassian JIRA**' directory type.*

On this page:

- Connecting Confluence to JIRA
- JIRA Settings in Confluence

⚠ *The information on this page does not apply to Atlassian OnDemand sites with multiple apps. If you are using Confluence-only OnDemand, the information does apply.*

Connecting Confluence to JIRA

To connect Confluence to JIRA 4.2 or earlier:

1. Edit the Confluence `server.xml` file, to construct the datasource location, as described below.
2. Restart Confluence.
3. Choose **Browse** > **Confluence Admin**.
4. Click **User Directories** in the left-hand panel.
5. **Add** a directory and select type **Legacy Atlassian JIRA (4.2 and earlier)**. Enter the settings as

described below.

6. Save the directory settings.
7. Define the directory order by clicking the blue up- and down-arrows next to each directory on the 'User Directories' screen. Here is a summary of how the directory order affects the processing:
   - The order of the directories is the order in which they will be searched for users and groups.
   - Changes to users and groups will be made only in the first directory where the application has permission to make changes.

   For details see Managing Multiple Directories.
8. In order to use Confluence, users must be a member of the `confluence-users` group or have Confluence 'can use' permission. Follow these steps to configure your Confluence groups in JIRA:
   a. Add the `confluence-users` and `confluence-administrators` groups in JIRA.
   b. Add your own username as a member of both of the above groups.
   c. Choose one of the following methods to give your existing JIRA users access to Confluence:
      - Option 1: In JIRA, find the groups that the relevant users belong to. Add the groups as members of one or both of the above Confluence groups.
      - Option 2: Log in to Confluence using your JIRA account and go to the Confluence **Administration Console**. Click '**Global Permissions**' and assign the '**can use**' permission to the relevant JIRA groups.

JIRA Settings in Confluence

Setting	Description
Name	A meaningful name that will help you to identify this JIRA server amongst your list of directory servers. Examples: • `JIRA` • `Example Company JIRA`

Datasource Location	The JNDI name of the JIRA datasource configured in your application server. Example: `java:comp/env/jdbc/YourJiraDatasource`
	In JIRA standalone distributions (using the default application server, Tomcat 6) you can construct the datasource location as follows:
	1. Open your `<jira_install>/conf/server.xml` file in a text editor.
	2. Look for the database setup section in that file. It looks something like this:
	`<Resource auth="Container"`
	`driverClassName="com.mysql.jdbc.Driver"`
	`maxActive="20"`
	`name="*jdbc/JiraDS*"`
	`password="jirauser"`
	`type="javax.sql.DataSource"`
	`url="jdbc:mysql://localhost/jiradb?useUnicode=true&characterEncoding=UTF8"`
	`username="jirauser"`
	`validationQuery="select 1"/>`
	3. Copy the above lines (the 'Resource' section) and paste it to your Confluence's `server.xml` file (located at `<confluence_install>/conf/server.xml`), under the `Context path`. This will then expose the value of the name attribute as the JNDI resource locator.
	4. Copy the JNDI name from the `name` parameter. In this example, the datasource location is: `java:comp/env/jdbc/JiraDS`

RELATED TOPICS

Configuring User Directories

- Configuring the Internal Directory
- Connecting to an LDAP Directory
- Connecting to an Internal Directory with LDAP Authentication
- Connecting to Crowd or JIRA for User Management
- Connecting to JIRA 4.2 or Earlier for User Management
- Managing Multiple Directories
- Managing Nested Groups
- Synchronising Data from External Directories
- Diagrams of Possible Configurations for User Management
- User Management Limitations and Recommendations
- Requesting Support for External User Management

Administrators Guide Home Confluence Documentation Home

Managing Multiple Directories

This page describes what happens when you have defined more than one user directory in Confluence. For example, you may have an internal directory and you may also connect to an LDAP directory server and/or other types of user directories. When you connect to a new directory server, you also need to define the **directory order**.

Duplicate usernames across directories are not supported. If you are connecting to more than one user directory, please ensure that the usernames are unique to one directory. For example, if you have a user `jsmith` in both 'Directory1' and 'Directory2', that is an unsupported configuration.

Overview

Here is a summary of how the directory order affects the processing:

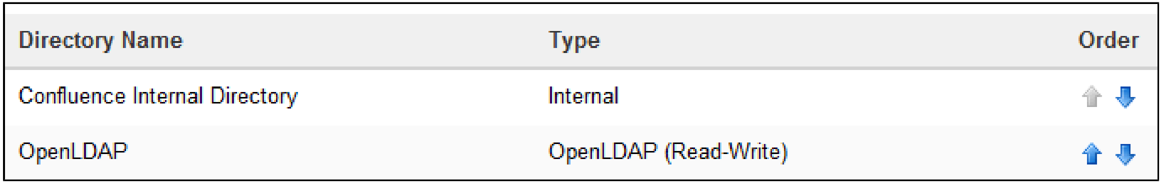
- The order of the directories is the order in which they will be searched for users and groups.
- Changes to users and groups will be made only in the first directory where the application has permission to make changes.

On this page:

⚠ *The information on this page does not apply to Atlassian OnDemand sites with multiple apps. If you are using Confluence-only OnDemand, the information does apply.*

Configuring the Directory Order

You can change the order of your directories as defined to Confluence. Select '**User Directories**' from the Confluence Administration Console and click the blue up- and down-arrows next to each directory.



Directory Name	Type	Order
Confluence Internal Directory	Internal	↑ ↓
OpenLDAP	OpenLDAP (Read-Write)	↑ ↓

Notes:

- Please read the rest of this page to understand what effect the directory order will have on authentication (login) and permissions in Confluence, and what happens when you update users and groups in Confluence.

Effect of Directory Order

This section summarises the effect the order of the directories will have on login and permissions, and on the updating of users and groups.

Login

The directory order is significant during the authentication of the user, in cases where the same user exists in multiple directories. When a user attempts to log in, the application will search the directories in the order specified, and will use the credentials (password) of the *first occurrence of the user* to validate the login attempt.

Permissions

The directory order is significant when granting the user permissions based on group membership. If the same username exists in more than one directory, the application will look for group membership only in the first directory where the username appears, based on the directory order.

Example:

- You have connected two directories: The Customers directory and the Partners directory.
- The Customers directory is first in the directory order.
- A username `jsmith` exists in both the Customers directory and the Partners directory.
- The user `jsmith` is a member of group `G1` in the Customers directory and group `G2` in the Partners directory.
- The user `jsmith` will have permissions based on membership of `G1` only, not `G2`.

Updating Users and groups

If you update a user or group via the application's administration screens, the update will be made in the first directory where the application has write permissions.

Example 1:

- You have connected two directories: The Customers directory and the Partners directory.
- The application has permission to update both directories.
- The Customers directory is first in the directory order.
- A username `jsmith` exists in both the Customers directory and the Partners directory.
- You update the email address of user `jsmith` via the application's administration screens.
- The email address will be updated in the Customers directory only, not the Partners directory.

Example 2:

- You have connected two directories: A read/write LDAP directory and the internal directory.
- The LDAP directory is first in the directory order.
- All new users will be added to the LDAP directory. It is not possible to add a new user to the internal directory.

RELATED TOPICS

Configuring User Directories

- Configuring the Internal Directory
- Connecting to an LDAP Directory
- Connecting to an Internal Directory with LDAP Authentication
- Connecting to Crowd or JIRA for User Management
- Connecting to JIRA 4.2 or Earlier for User Management
- Managing Multiple Directories
- Managing Nested Groups
- Synchronising Data from External Directories
- Diagrams of Possible Configurations for User Management
- User Management Limitations and Recommendations
- Requesting Support for External User Management

Administrators Guide Home Confluence Documentation Home

Managing Nested Groups

Some directory servers allow you to define a group as a member of another group. Groups in such a structure are called 'nested groups'. If you are using groups to manage permissions, you can create nested groups to allow inheritance of permissions from one group to its sub-groups.
This page describes how Confluence handles nested groups that exist in one or more of your directory servers.

Enabling Nested Groups

You can enable or disable support for nested groups on each directory individually. Go to the '**User Directories**' section of the Confluence Administration Console, **edit** the directory and select '**Enable Nested Groups'**. See Configuring User Directories.

Notes:

- Before enabling nested groups for a specific directory type in Confluence, please make sure that your directory server supports nested groups.
- Please read the rest of this page to understand what effect nested groups will have on authentication (login) and permissions in Confluence, and what happens when you update users and groups in Confluence.

On this page:

⚠ *The information on this page does not apply to Atlassian OnDemand sites with multiple apps. If you are using Confluence-only OnDemand, the information does apply.*

Effect of Nested Groups

This section summarises the effect nested groups will have on login and permissions, and on the viewing and updating of users and groups.

Login

When a user logs in, they will be allowed access to the application if they belong to an authorised group or any of its sub-groups.

Permissions

The user will be allowed access to a function if they belong to a group that has the necessary permissions, or if they belong to any of its sub-groups.

Viewing Lists of Group Members

If you ask to view the members of a group, you will see all users who are members of the group and all users belonging its sub-groups, consolidated into one list. We call this a '**flattened**' list.

You cannot view or edit the nested groups themselves. You will not be able to see that one group is a member of another group.

Adding and Updating Group Memberships

If you add a user to a group, the user is added to the named group and not to any other groups.

If you try to remove a user from a flattened list, the following will happen:

- If the user is a member of the top group in the hierarchy (tree) of groups contained in the flattened list, the user will be removed from the group.
- Otherwise, you will see an error message stating that the user is not a direct member of the group.

Examples

Example 1: User is Member of Sub-Group

Let's assume that the following two groups exist in your directory server:

- `staff`
- `marketing`

Memberships:

- The `marketing` group is a member of the `staff` group.
- User `jsmith` is a member of `marketing`.

You will see that `jsmith` is a member of both `marketing` and `staff`. You will not see that the two groups are nested. If you assign permissions to the `staff` group, then `jsmith` will get those permissions.

Example 2: Sub-Groups as Members of the 'jira-developers' group

In an LDAP directory server, we have groups '**engineering-group**' and '**techwriters-group**'. We want to grant both groups developer-level access to our JIRA site.

- Add a group called '**jira-developers**'.
- Add the '**engineering-group**' as a sub-group of '**jira-developers**'.
- Add the '**techwriters-group**' as a sub-group of '**jira-developers**'.

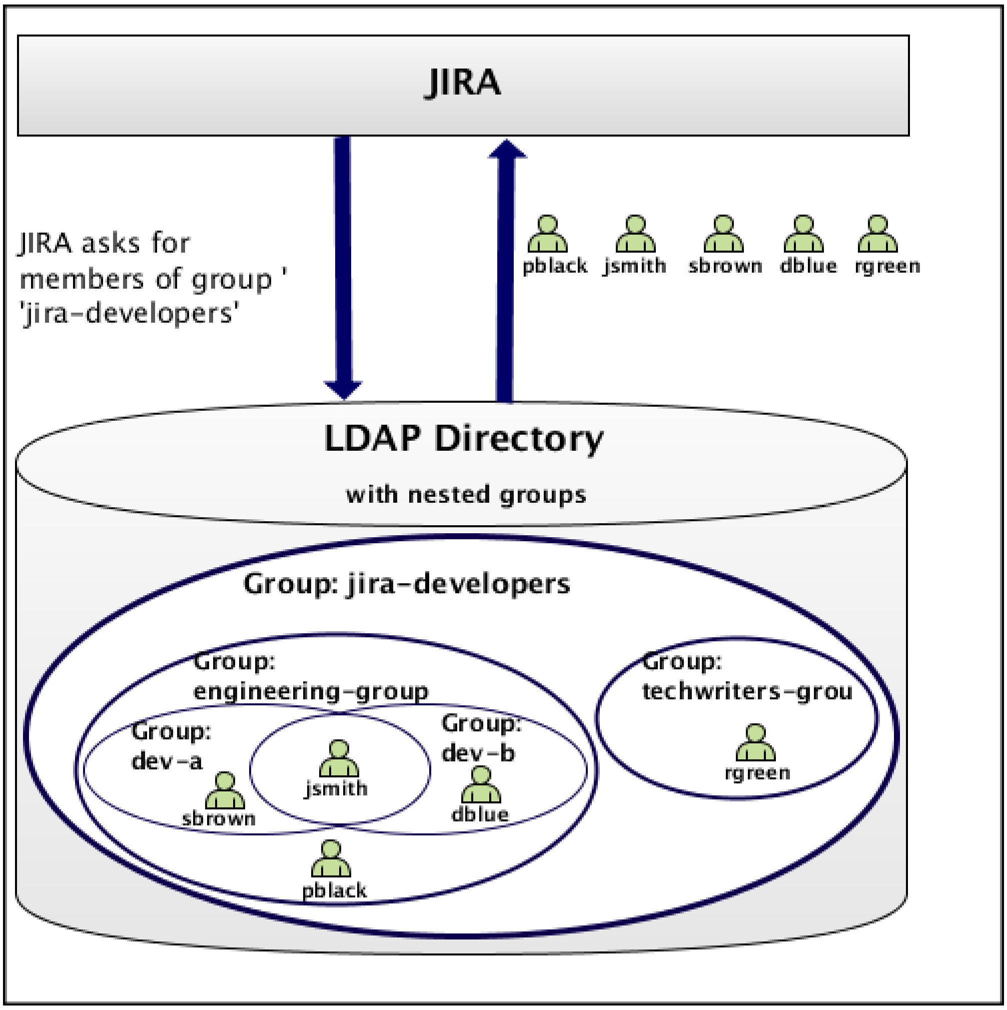
Group memberships are now:

- **jira-developers** — sub-groups: **engineering-group**, **techwriters-group**
- **engineering-group** — sub-groups: **dev-a**, **dev-b**; users: **pblack**
- **dev-a** — users: **jsmith**, **sbrown**
- **dev-b** — users: **jsmith**, **dblue**
- **techwriters-group** — users: **rgreen**

When JIRA requests a list of users in the '**jira-developers**' group, it will receive the following list:

- **pblack**
- **jsmith**
- **sbrown**
- **dblue**
- **rgreen**

Diagram: Sub-groups as members of the 'jira-developers' group



Example 3: Sub-Groups as Members of the 'confluence-users' group

In an LDAP directory server, we have groups '**engineering-group**' and '**payroll-group**'. We want to grant both groups access to our Confluence site.

- Add a group called '**confluence-users**'.
- Add the '**engineering-group**' as a sub-group of '**confluence-users**'.
- Add the '**payroll-group**' as a sub-group of '**confluence-users**'.

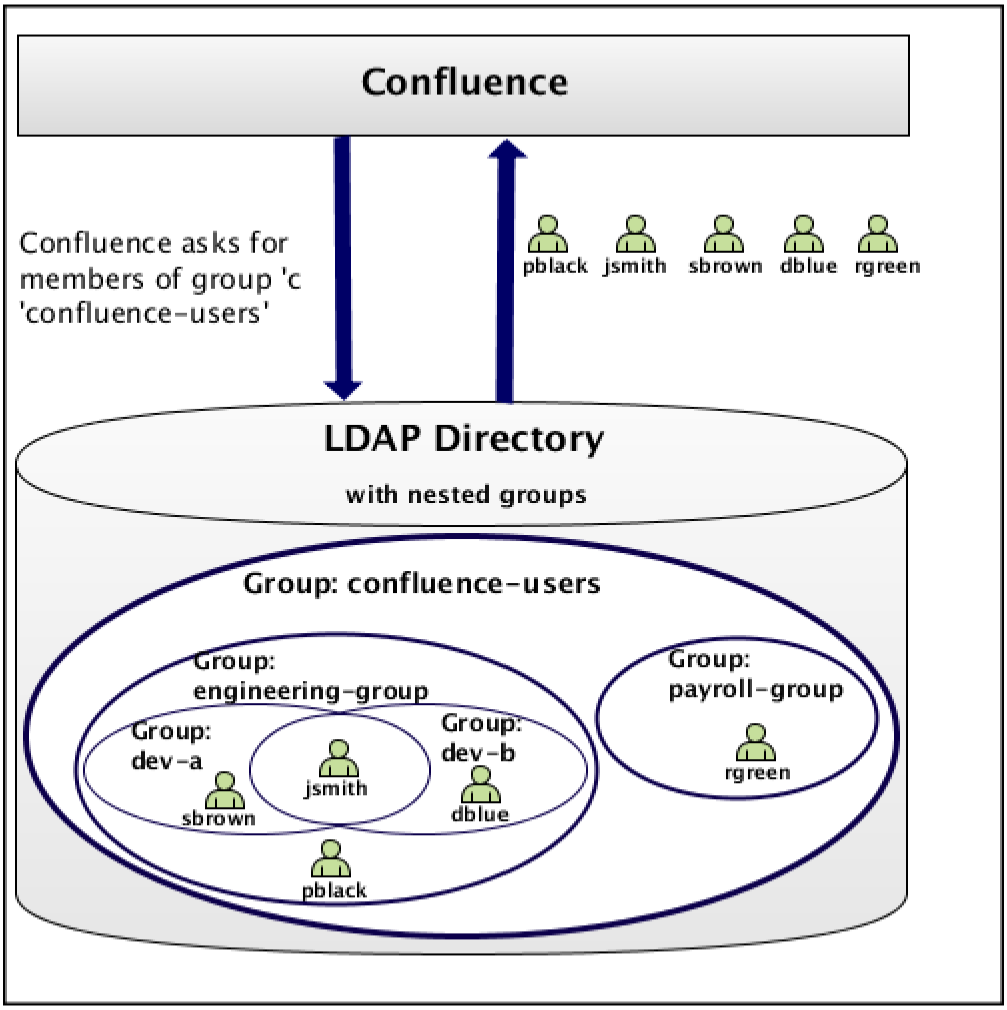
Group memberships are now:

- **confluence-users** — sub-groups: **engineering-group**, **payroll-group**
- **engineering-group** — sub-groups: **dev-a**, **dev-b**; users: **pblack**
- **dev-a** — users: **jsmith**, **sbrown**
- **dev-b** — users: **jsmith**, **dblue**
- **payroll-group** — users: **rgreen**

When Confluence requests a list of users in the '**confluence-users**' group, it will receive the following list:

- **pblack**
- **jsmith**
- **sbrown**
- **dblue**
- **rgreen**

Diagram: Sub-groups as members of the 'confluence-users' group



Notes

- **Possible impact on performance.** Enabling nested groups may result in slower user searches.
- **Definition of nested groups in LDAP.** In an LDAP directory, a nested group is defined as a child group entry whose DN (Distinguished Name) is referenced by an attribute contained within a parent group entry. For example, a parent group '**Group One**' might have an `objectClass=group` attribute and one or more `member=DN` attributes, where the DN can be that of a user *or* that of a group elsewhere in the LDAP tree:

```
member=CN=John Smith,OU=Users,OU=OrgUnitA,DC=sub,DC=domain
member=CN=Group Two,OU=OrgUnitBGroups,OU=OrgUnitB,DC=sub,DC=domain
```

RELATED TOPICS

Configuring User Directories

- Configuring the Internal Directory
- Connecting to an LDAP Directory
- Connecting to an Internal Directory with LDAP Authentication
- Connecting to Crowd or JIRA for User Management
- Connecting to JIRA 4.2 or Earlier for User Management
- Managing Multiple Directories
- Managing Nested Groups
- Synchronising Data from External Directories
- Diagrams of Possible Configurations for User Management

- User Management Limitations and Recommendations
- Requesting Support for External User Management

Administrators Guide Home Confluence Documentation Home

Synchronising Data from External Directories

For certain directory types, Confluence stores a cache of directory information (users and groups) in the application database, to ensure fast recurrent access to user and group data. A synchronisation task runs periodically to update the internal cache with changes from the external directory.

On this page:

⚠ *The information on this page does not apply to Atlassian OnDemand sites with multiple apps. If you are using Confluence-only OnDemand, the information does apply.*

Affected Directory Types

Data caching and synchronisation apply to the following user directory types:

- **LDAP** (Microsoft Active Directory and all supported LDAP directories) where permissions are set to **read only**.
- **LDAP** (Microsoft Active Directory and all supported LDAP directories) where permissions are set to **read only, with local groups**.
- **LDAP** (Microsoft Active Directory and all supported LDAP directories) where permissions are set to **read/write**.
- **Atlassian Crowd**.
- **Atlassian JIRA**.

Data caching and synchronisation do not occur for the following user directory types:

- **LDAP** (Microsoft Active Directory and all supported LDAP directories) where permissions are set to **authentication only, with local groups**.
- **Internal Directory with LDAP Authentication**.
- **Internal Directory**.

How it Works

Here is a summary of the caching functionality:

- The caches are held in the application database.
- When you connect a new external user directory to the application, a synchronisation task will start running in the background to copy all the required users, groups and membership information from the external directory to the application database. This task may take a while to complete, depending on the size and complexity of your user base.
- Note that a user will not be able to log in until the synchronisation task has copied that user's details into the cache.
- A periodic synchronisation task will run to update the database with any changes made to the external directory. The default synchronisation interval, or polling interval, is one hour (60 minutes). You can change the synchronisation interval on the directory configuration screen.
- You can manually synchronise the cache if necessary.

- If the external directory permissions are set to read/write: Whenever an update is made to the users, groups or membership information via the application, the update will also be applied to the cache and the external directory immediately.
- All authentication happens via calls to the external directory. When caching information from an external directory, the application database does not store user passwords.
- All other queries run against the internal cache.

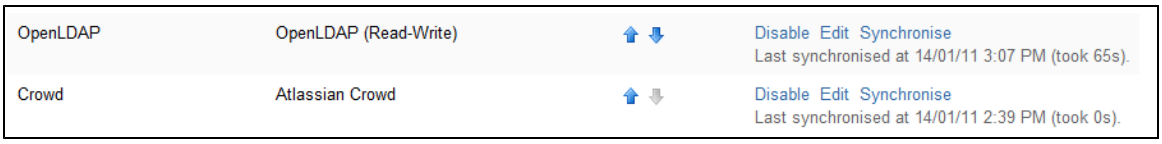
Finding the Time Taken to Synchronise

The '**User Directories**' screen shows information about the last synchronisation operation, including the length of time it took.

Manually Synchronising the Cache

You can manually synchronise the cache by clicking '**Synchronise**' on the '**User Directories**' screen. If a synchronisation operation is already in progress, you cannot start another until the first has finished.

Screen snippet: User directories, showing information about synchronisation



OpenLDAP	OpenLDAP (Read-Write)	↑ ↓	Disable Edit Synchronise Last synchronised at 14/01/11 3:07 PM (took 65s).
Crowd	Atlassian Crowd	↑ ↓	Disable Edit Synchronise Last synchronised at 14/01/11 2:39 PM (took 0s).

Configuring the Synchronisation Interval

Note: The option to configure the synchronisation interval for Crowd and JIRA directories is available in **Confluence 3.5.3 and later**. Earlier versions of Confluence allow you to configure the interval for LDAP directories only.

You can set the '**Synchronisation Interval**' on the directory configuration screen. The synchronisation interval is the period of time to wait between requests for updates from the directory server.

The length you choose for your synchronisation interval depends on:

- The length of time you can tolerate stale data.
- The amount of load you want to put on the application and the directory server.
- The size of your user base.

If you synchronise more frequently, then your data will be more up to date. The downside of synchronising more frequently is that you may overload your server with requests.

If you are not sure what to do, we recommend that you start with an interval of 60 minutes (this is the default setting) and reduce the value incrementally. You will need to experiment with your setup.

RELATED TOPICS

Configuring User Directories

- Configuring the Internal Directory
- Connecting to an LDAP Directory
- Connecting to an Internal Directory with LDAP Authentication
- Connecting to Crowd or JIRA for User Management
- Connecting to JIRA 4.2 or Earlier for User Management
- Managing Multiple Directories
- Managing Nested Groups
- Synchronising Data from External Directories
- Diagrams of Possible Configurations for User Management
- User Management Limitations and Recommendations

- Requesting Support for External User Management

Administrators Guide Home Confluence Documentation Home

Diagrams of Possible Configurations for User Management

The aim of these diagrams is to help people understand each directory type at a glance. We have kept the diagrams simple and conceptual, with just enough information to be correct.

Some things that we do **not** attempt to show:

- In most cases, we do not attempt to show that you can have multiple directory types mapped to Confluence at the same time. We illustrate that fact in just the first two LDAP diagrams.
- We have not included a diagram for Confluence's legacy connection to JIRA database.
- We do not attempt to show all of the possible configurations and layered connections that are available now that you can use JIRA as a directory manager.

On this page:

⚠ *The information on this page does not apply to Atlassian OnDemand sites with multiple apps. If you are using Confluence-only OnDemand, the information does apply.*

Confluence Internal Directory

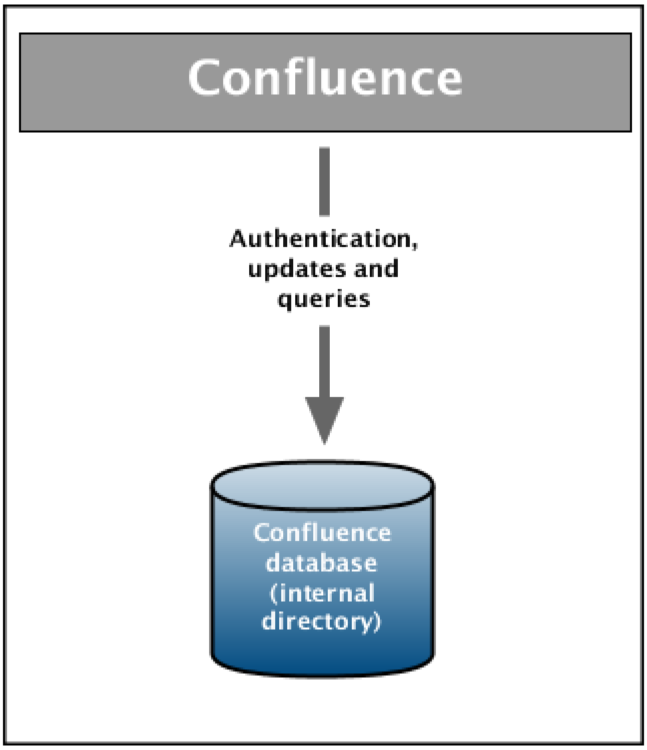

Confluence
Authentication, updates and queries
Confluence database (internal directory)

Diagram above: Confluence using its internal directory for user management.

Confluence with Read/Write Connection to LDAP

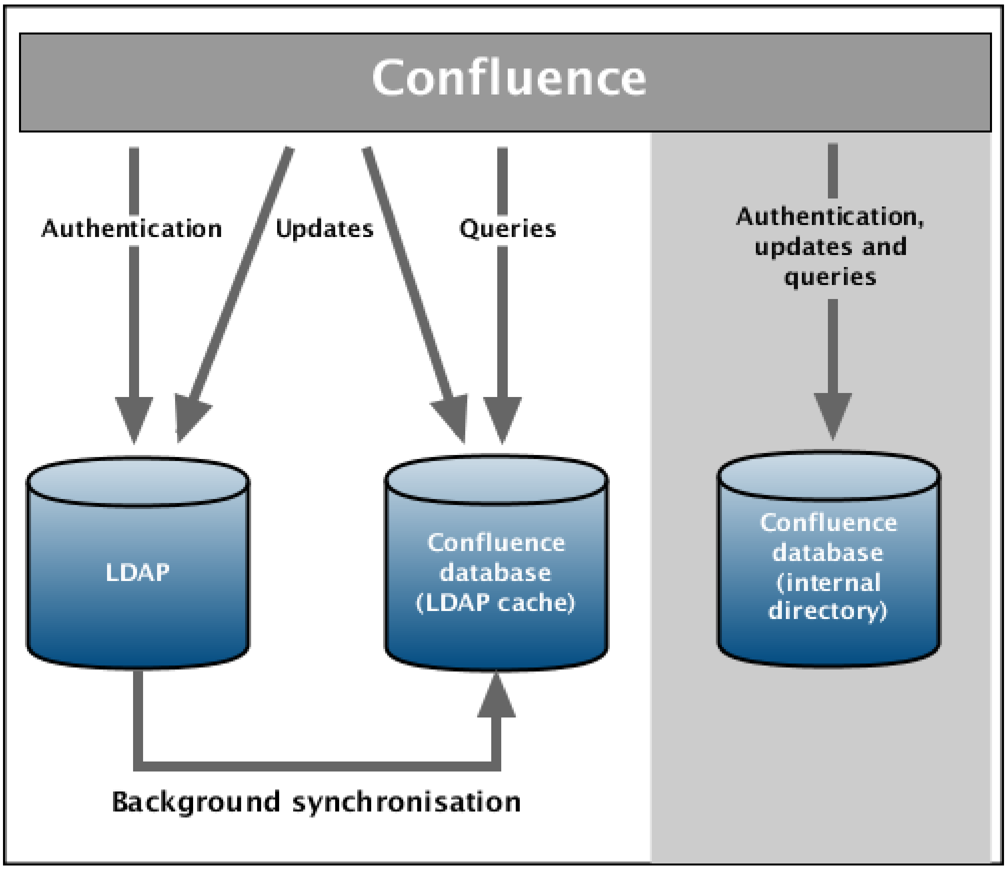

Confluence
Authentication
Updates
Queries
Authentication, updates and queries
LDAP
Confluence database (LDAP cache)
Confluence database (internal directory)
Background synchronisation

Diagram above: Confluence connecting to an LDAP directory.

Confluence with Read-Only Connection to LDAP, with Local Groups

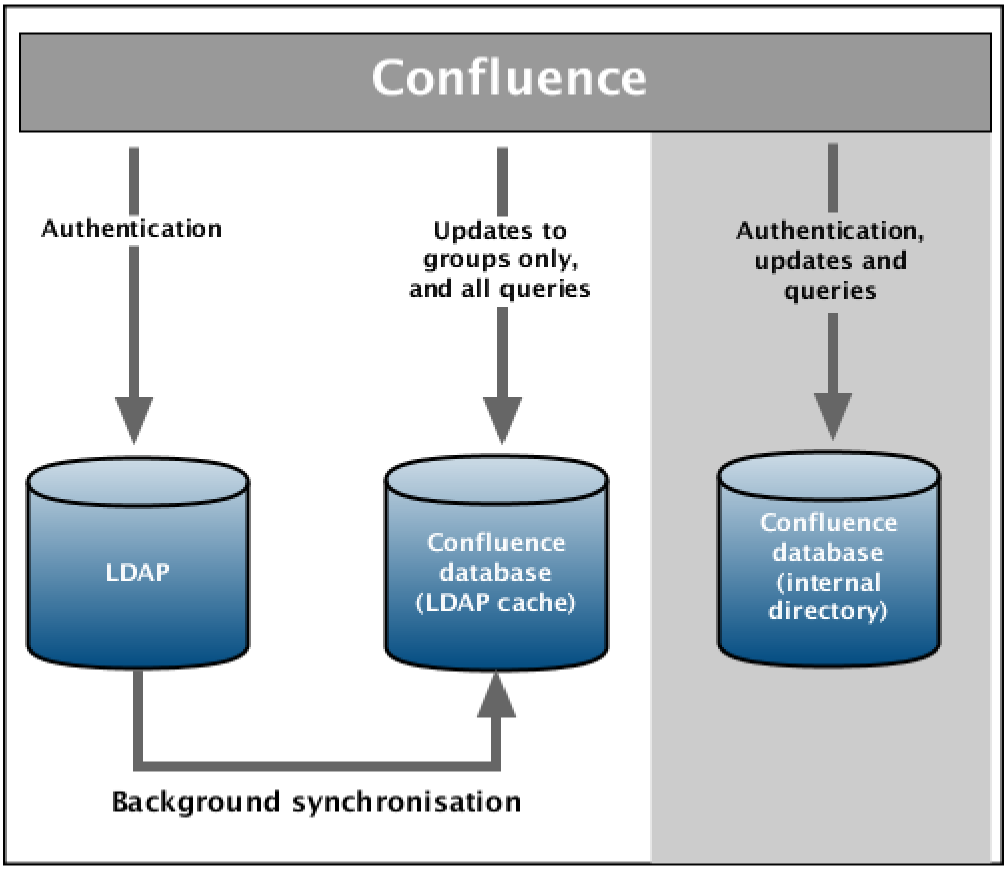

Confluence
Authentication
Updates to groups only, and all queries
Authentication, updates and queries
LDAP
Confluence database (LDAP cache)
Confluence database (internal directory)
Background synchronisation

Diagram above: Confluence connecting to an LDAP directory with permissions set to read only and local groups.

Confluence Internal Directory with LDAP Authentication

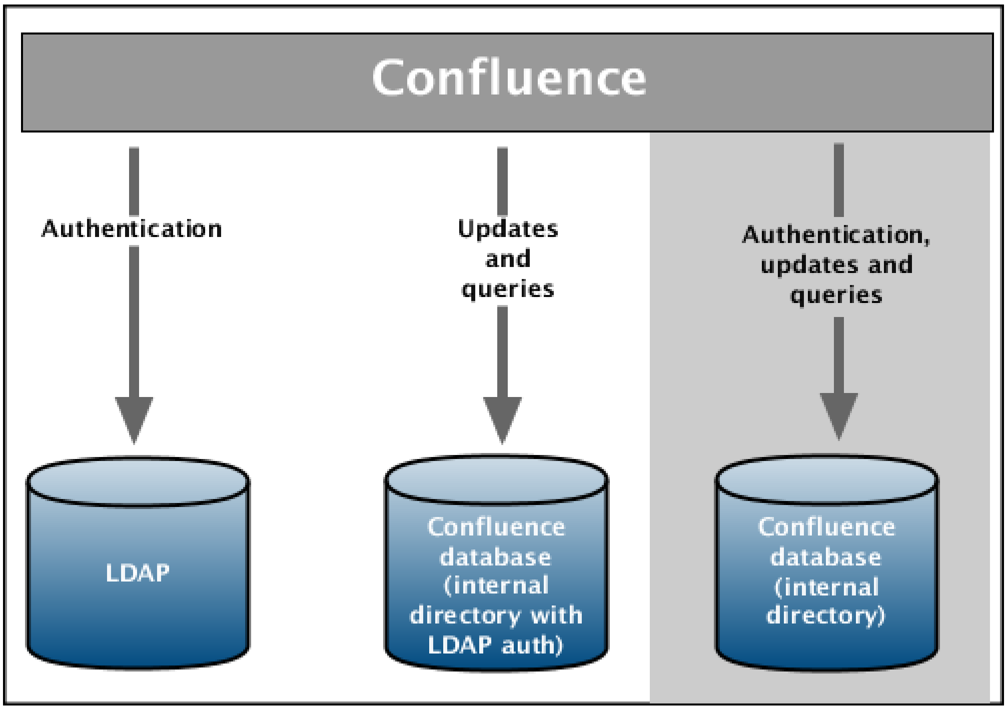

Confluence
Authentication
Updates and queries
Authentication, updates and queries
LDAP
Confluence database (internal directory with LDAP auth)
Confluence database (internal directory)

Diagram above: Confluence connecting to an LDAP directory for authentication only.

Confluence with LDAP Authentication, Copy Users on First Login

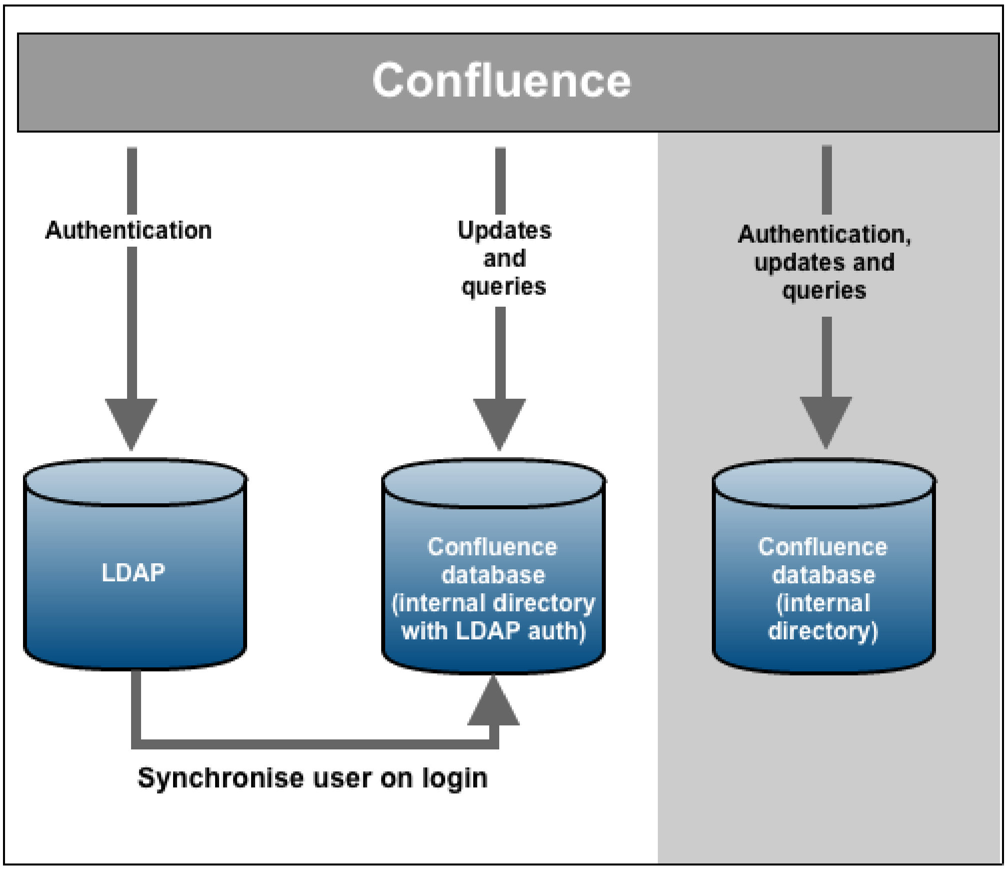

Confluence
Authentication
Updates and queries
Authentication, updates and queries
LDAP
Confluence database (internal directory with LDAP auth)
Confluence database (internal directory)
Synchronise user on login

Diagram above: Confluence connecting to an LDAP directory for authentication only, with each user *synchronised with the internal directory that is using LDAP authentication when they log in to Confluence.*

Confluence Connecting to JIRA

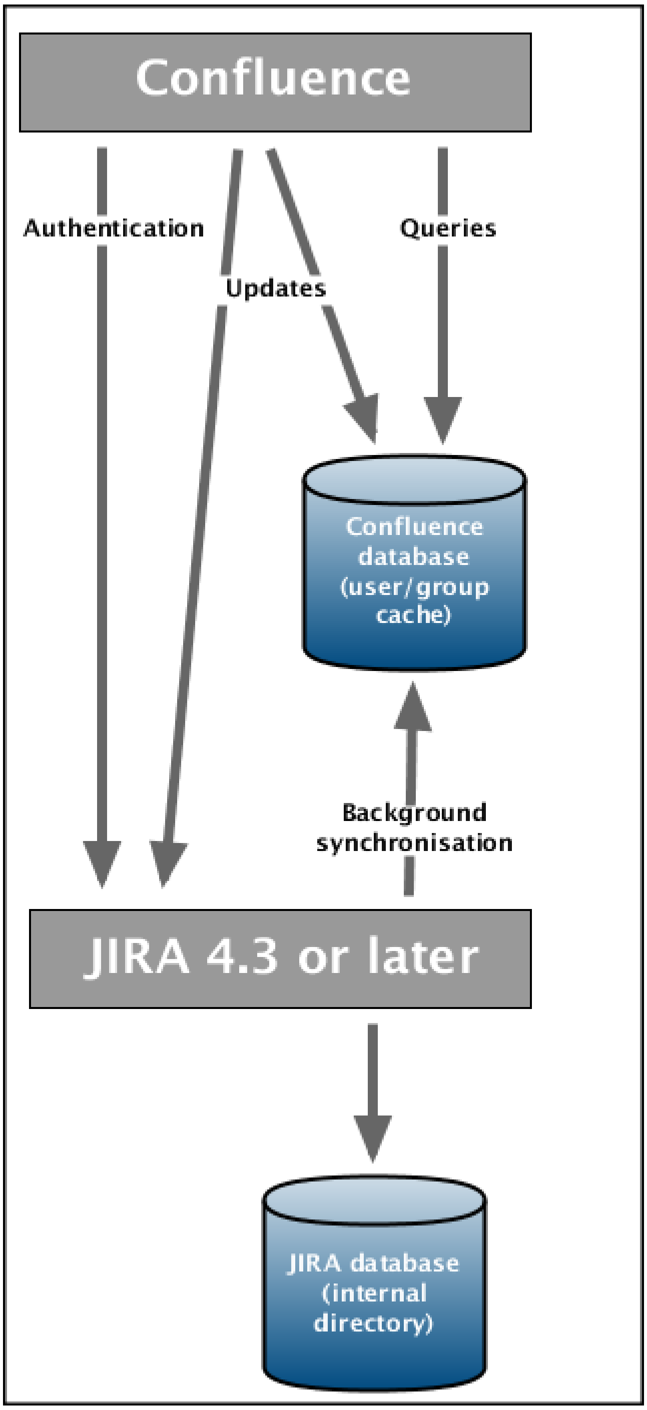

Confluence
Authentication
Updates
Queries
Confluence database (user/group cache)
Background synchronisation
JIRA 4.3 or later
JIRA database (internal directory)

Diagram above: Confluence connecting to JIRA for user management.

Confluence Connecting to JIRA and JIRA Connecting to LDAP

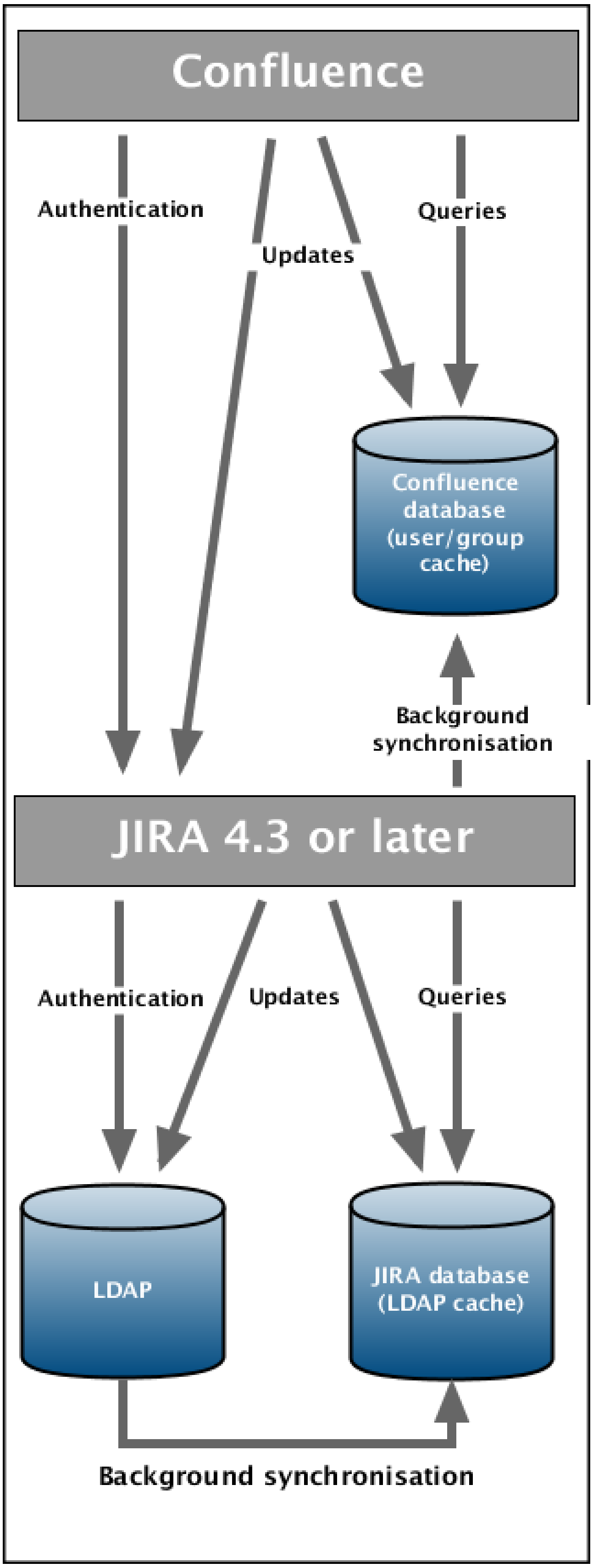

Confluence
Authentication
Updates
Queries
Confluence database (user/group cache)
Background synchronisation
JIRA 4.3 or later
Authentication
Updates
Queries
LDAP
JIRA database (LDAP cache)
Background synchronisation

Diagram above: Confluence connecting to JIRA for user management, with JIRA in turn connecting to LDAP.

Confluence and JIRA Connecting to Crowd

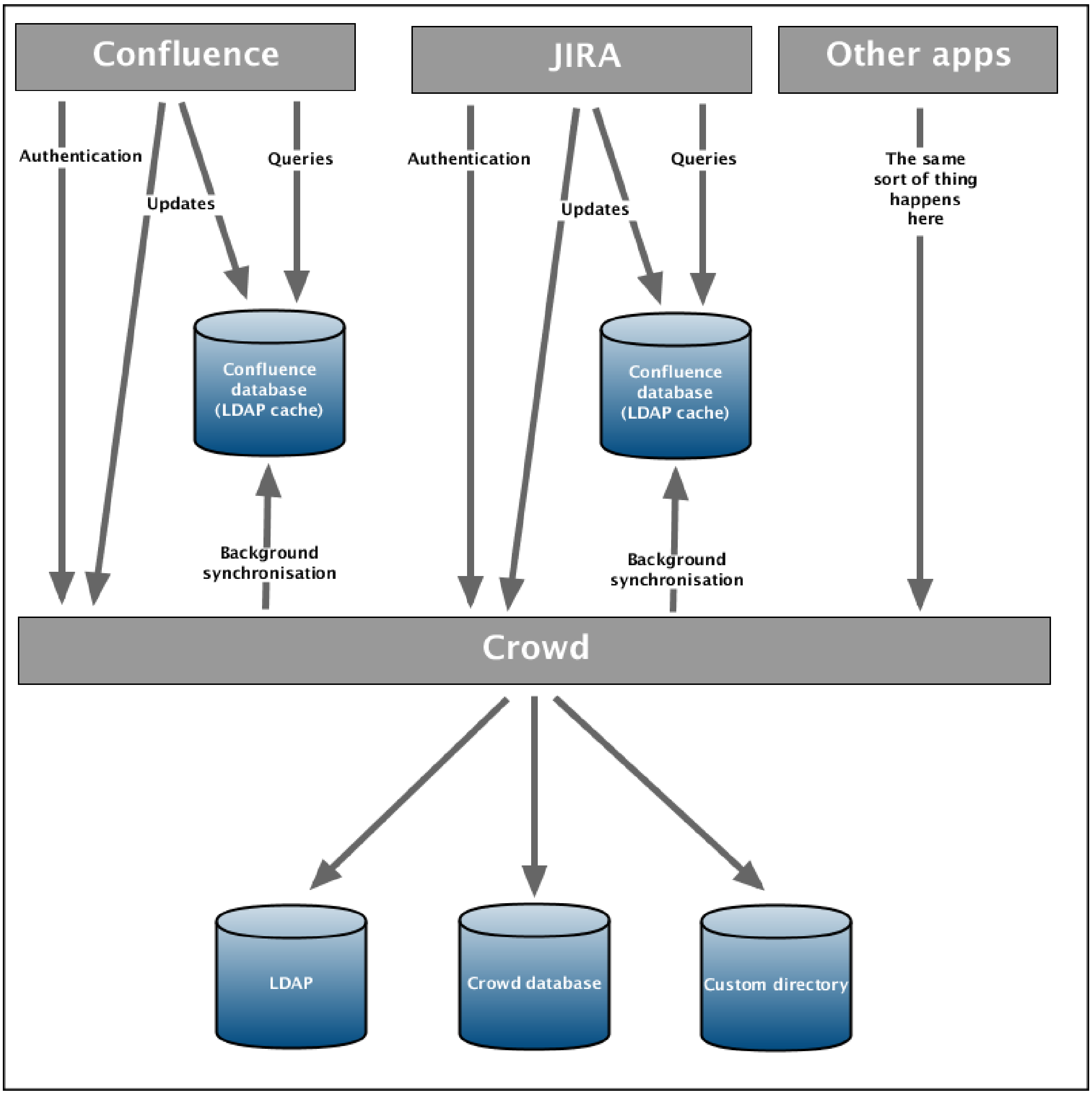

Confluence
JIRA
Other apps
Authentication
Updates
Queries
Authentication
Updates
Queries
The same sort of thing happens here
Confluence database (LDAP cache)
Confluence database (LDAP cache)
Background synchronisation
Background synchronisation
Crowd
LDAP
Crowd database
Custom directory

Diagram above: Confluence, JIRA and other applications connecting to Crowd for user management.

RELATED TOPICS

Configuring User Directories

- Configuring the Internal Directory
- Connecting to an LDAP Directory
- Connecting to an Internal Directory with LDAP Authentication
- Connecting to Crowd or JIRA for User Management
- Connecting to JIRA 4.2 or Earlier for User Management
- Managing Multiple Directories
- Managing Nested Groups
- Synchronising Data from External Directories
- Diagrams of Possible Configurations for User Management
- User Management Limitations and Recommendations
- Requesting Support for External User Management

Administrators Guide Home Confluence Documentation Home

User Management Limitations and Recommendations

This page describes the optimal configurations and limitations that apply to user management in Confluence.

On this page:

⚠ *The information on this page does not apply to Atlassian OnDemand sites with multiple apps. If you are using Confluence-only OnDemand, the information does apply.*

General Recommendations

- **Duplicate usernames across directories are not supported**. If you are connecting to more than one user directory, please ensure that the usernames are unique to one directory. For example, if you have a user `jsmith` in both 'Directory1' and 'Directory2', that is an unsupported configuration.
- **Be careful when deleting users in remote directories**. If you are connecting to an LDAP directory, a Crowd directory or a JIRA directory, please take care when deleting users from the remote directory. If you delete a user that is associated with data in Confluence, this will cause problems in Confluence.

Recommendations for Connecting to LDAP

Please consider the following limitations and recommendations when connecting to an LDAP user directory.

Optimal Number of Users and Groups in your LDAP Directory

The connection to your LDAP directory provides powerful and flexible support for connecting to, configuring and managing LDAP directory servers. To achieve optimal performance, a background synchronisation task loads the required users and groups from the LDAP server into the application's database, and periodically fetches updates from the LDAP server to keep the data in step. The amount of time needed to copy the users and groups rises with the number of users, groups, and group memberships. For that reason, we recommended a maximum number of users and groups as described below.

This recommendation affects connections to LDAP directories:

- Microsoft Active Directory
- All other LDAP directory servers

The following LDAP configurations are **not** affected:

- Internal directories with LDAP authentication
- LDAP directories configured for 'Authentication Only, Copy User On First Login'

Please choose one of the following solutions, depending on the number of users, groups and memberships in your LDAP directory.

Your environment	Recommendation

Up to 10 000 (ten thousand) users, 1000 (one thousand) groups, and 20 (twenty) groups per user	Choose the '**LDAP**' or '**Microsoft Active Directory**' directory type. You can make use of the full synchronisation option. Your application's database will contain all the users and groups that are in your LDAP server.
More than the above	Use LDAP filters to reduce the number of users and groups visible to the synchronisation task.

Our Test Results

We performed internal testing of synchronisation with an AD server on our local network consisting of 10 000 users, 1000 groups and 200 000 memberships.

We found that the initial synchronisation took about 5 minutes. Subsequent synchronisations with 100 modifications on the AD server took a couple of seconds to complete.

Please keep in mind that a number of factors come into play when trying to tune the performance of the synchronisation process, including:

- **Size of userbase.** Use LDAP filters to keep this to the minimum that suits your requirements.
- **Type of LDAP server.** We currently support change detection in AD, so subsequent synchronisations are much faster for AD than for other LDAP servers.
- **Network topology.** The further away your LDAP server is from your application server, the more latent LDAP queries will be.
- **Database performance.** As the synchronisation process caches data in the database, the performance of your database will affect the performance of the synchronisation.
- **JVM heap size.** If your heap size is too small for your userbase, you may experience heavy garbage collection during the synchronisation process which could in turn slow down the synchronisation.

Redundant LDAP is Not Supported

The LDAP connections do not support the configuration of two or more LDAP servers for redundancy (automated failover if one of the servers goes down).

Specific Notes for Connecting to Active Directory

When the application synchronises with Active Directory (AD), the synchronisation task requests only the changes from the LDAP server rather than the entire user base. This optimises the synchronisation process and gives much faster performance on the second and subsequent requests.

On the other hand, this synchronisation method results in a few limitations:

1. **Externally moving objects out of scope or renaming objects causes problems in AD.** If you move objects out of scope in AD, this will result in an inconsistent cache. We recommend that you do not use the external LDAP directory interface to move objects out of the scope of the sub-tree, as defined on the application's directory configuration screen. If you do need to make structural changes to your LDAP directory, manually synchronise the directory cache after you have made the changes to ensure cache consistency.
2. **Synchronising between AD servers is not supported.** Microsoft Active Directory does not replicate the uSNChanged attribute across instances. For that reason, we do not support connecting to different AD servers for synchronisation. (You can of course define multiple different directories, each pointing to its own respective AD server.)
3. **Synchronising with AD servers behind a load balancer is not supported.** As with synchronising between two different AD servers, Microsoft Active Directory does not replicate the uSNChanged attribute across instances. For that reason, we do not support connecting to different AD servers even when they are load balanced. You will need to select one server (preferably one that is local) to synchronise with instead of using the load balancer.

4. **You must restart the application after restoring AD from backup.** On restoring from backup of an AD server, the uSNChanged timestamps are reverted to the backup time. To avoid the resulting confusion, you will need to flush the directory cache after a Active Directory restore operation.
5. **Obtaining AD object deletions requires administrator access.** Active Directory stores deleted objects in a special container called cn=Deleted Objects. By default, to access this container you need to connect as an administrator and so, for the synchronisation task to be aware of deletions, you must use administrator credentials. Alternatively, it is possible to change the permissions on the cn=Deleted Objects container. If you wish to do so, please see this Microsoft KB Article.
6. **The User DN used to connect to AD must be able to see the uSNChanged attribute.** The synchronisation task relies on the uSNChanged attribute to detect changes, and so must be in the appropriate AD security groups to see this attribute for all LDAP objects in the subtree.

Recommendations for Connecting to JIRA for User Management

Please consider the following limitations and recommendations when connecting to a JIRA server for user management.

Single Sign-On Across Multiple Applications is Not Supported

When you connect to JIRA for user management, you will not have single sign-on across the applications connected in this way. JIRA, when acting as a directory manager, does not support SSO.

Custom Application Connectors are Not Supported

JIRA, Confluence, FishEye, Crucible and Bamboo can connect to a JIRA server for user management. Custom application connectors will need to use the new REST API.

Custom Directories are Not Supported

Earlier versions of JIRA supported OSUser Providers. It was therefore possible write a special provider to obtain user information from any external user directory. This is no longer the case.

Optimal Number of Users and Applications

Please consider the following limitations when connecting to a JIRA server for user management:

- Maximum 500 users.
- Maximum 5 connected applications.

Recommendations

Your environment	Recommendation
If **all** the following are true: • You have fewer than 500 users. • You want to share user and group management across just a few applications, such as one JIRA server and one Confluence server, or two JIRA servers. • You do not need single sign-on (SSO) between JIRA and Confluence, or between two JIRA servers. • You do not have custom application connectors. Or, if you do have them, you are happy to convert them to use the new REST API. • You are happy to shut down all your servers when you need to upgrade JIRA.	Your environment meets the optimal requirements for using JIRA for user management.

If **one or more** of the following are true: • You have more than 500 users. • You want to share user and group management across more than 5 applications. • You need single sign-on (SSO) across multiple applications. • You have custom applications integrated via the Crowd SOAP API, and you cannot convert them to use the new REST API. • You are not happy to shut down all your servers when you need to upgrade JIRA.	We recommend that you install Atlassian Crowd for user management and SSO.
If you are considering creating a custom directory connector to define your own storage for users and groups...	Please see if one of the following solutions will work for you: • If you have written a custom provider to support a specific LDAP schema, please check the supported LDAP schemas to see if you can use one of them instead. • If you have written a custom provider to support nested groups, please consider enabling nested groups in the supported directory connectors instead. • If you have written a custom provider to connect to your own database, please consider loading the data into the application's database instead. • If you need to keep the custom directory connection, please consider whether Atlassian Crowd meets your requirements. See the documentation on Creating a Custom Directory Connector.

RELATED TOPICS

Connecting to an LDAP Directory
Connecting to Crowd or JIRA for User Management
Configuring User Directories

Requesting Support for External User Management

This page gives guidelines on how to request help from the Atlassian support team if you are having problems with external user management. External user management includes connections to Active Directory, other LDAP servers, Atlassian Crowd or Atlassian JIRA for user management. The information on this page is provided in addition to the more general page on Troubleshooting Problems and Requesting Technical Support.

The cause of such problems may be:

- The LDAP server is not responding.
- The application password is incorrectly configured, causing the LDAP server or other directory to return an authentication error.
- Other LDAP settings are incorrectly configured.

On this page:

> ⚠ *The information on this page does not apply to Atlassian OnDemand sites with multiple apps. If you are using Confluence-only OnDemand, the information does apply.*

Troubleshooting the Connection to your External User Directory

The configuration screen for external directories in Confluence has a '**Test Settings**' button. This will help you to diagnose problems with user management in Active Directory and other LDAP servers.

To test your directory connection:

1. Choose **Browse** > **Confluence Admin**.
2. Click '**User Directories**' in the left-hand panel.
3. **Edit** the relevant directory.
4. Click '**Test Settings**'.
5. The results of the test will appear at the top of the screen.

Please refer to our knowedge base articles for troubleshooting user management and login issues.

If the above resources do not help, continue below.

Problems During Initial Setup

Raise a support request and include the following information.

- Download an LDAP browser to make sure you have the right settings in your LDAP directory. Atlassian recommends LDAP Studio. Include screenshots of your user and group DNs.
- If you can start up Confluence and access the Administration Console, review your directory settings. See Connecting to an LDAP Directory. Attach screenshots of all your settings.

Complex Authentication or Performance Problems

Raise a support request and include the following information.

Confluence Server

Log in to Confluence and access the Administration Console.

- Take a screenshot of the '**System Information**' screen, or save the page as HTML.
- Take a screenshot of the '**Global Permissions**' screen, if people are having problems with logging in.
- Go to '**Space Admin**' for the relevant space and take a screenshot of the '**Permissions**' page, if you are having problems with space or page permissions.

Confluence Configuration Files

- If you have implemented a custom authenticator or in any way modified `seraph-config.xml` or `seraph-paths.xml`, please provide the modified file.

User Management System

- Include the name and version of your LDAP server.
- Does your LDAP server use dynamic or static groups?
- Review your directory settings. See Connecting to an LDAP Directory. Attach screenshots of all your settings.

Diagnostics

- Enable profiling. See Performance Tuning.
- Enable detailed user management logging, by editing `confluence/WEB-INF/classes/log4j.properties`.
  Change this section:

```
###
# Atlassian User
###
#log4j.logger.com.atlassian.user=DEBUG
#log4j.logger.com.atlassian.confluence.user=DEBUG
#log4j.logger.bucket.user=DEBUG
#log4j.logger.com.atlassian.seraph=DEBUG
#log4j.logger.com.opensymphony.user=DEBUG
```

Remove the '#' signs at the beginning of the lines, so that it looks like this:

```
###
# Atlassian User
###
log4j.logger.com.atlassian.user=DEBUG
log4j.logger.com.atlassian.confluence.user=DEBUG
log4j.logger.bucket.user=DEBUG
log4j.logger.com.atlassian.seraph=DEBUG
log4j.logger.com.opensymphony.user=DEBUG
```

- After enabling both the above, please attempt a Confluence LDAP account login and attach a copy of the log files that are produced when the problem occurs. To do this, locate your install directory or exploded WAR directory, then zip the full `/logs` subdirectory into a single file for us to examine.The logs subdirectory is located in your Confluence Home directory.

RELATED TOPICS

Troubleshooting Problems and Requesting Technical Support
Configuring User Directories

- Configuring the Internal Directory
- Connecting to an LDAP Directory
- Connecting to an Internal Directory with LDAP Authentication
- Connecting to Crowd or JIRA for User Management
- Connecting to JIRA 4.2 or Earlier for User Management
- Managing Multiple Directories
- Managing Nested Groups
- Synchronising Data from External Directories
- Diagrams of Possible Configurations for User Management
- User Management Limitations and Recommendations
- Requesting Support for External User Management

Administrators Guide Home Confluence Documentation Home

Confluence User Management

This section describes how to manage users and groups in Confluence. To learn how to configure external user management in Confluence, see Configuring User Directories.

> ⚠ *The information on this page does not apply to Atlassian OnDemand sites with multiple apps. If you are using Confluence-only OnDemand, the information does apply.*

Searching For and Managing Users

If you are a Confluence Administrator, you can add users, assign them to groups and edit their user details.

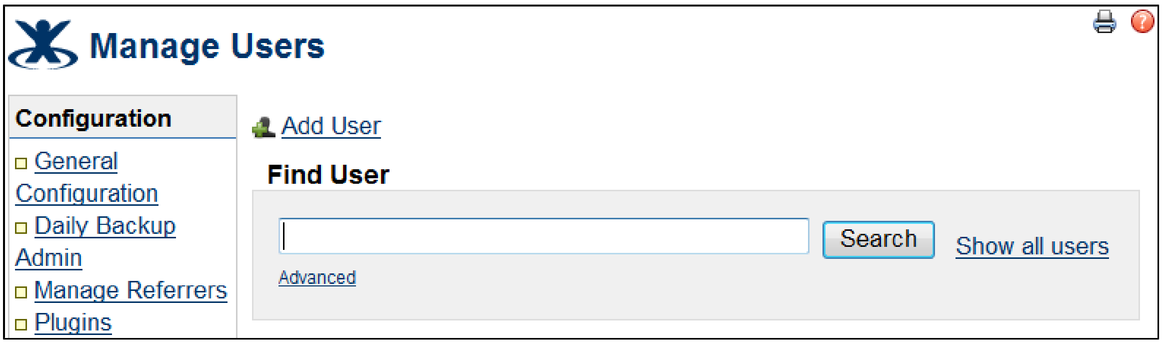
On this page:

⚠ *The information on this page does not apply to Atlassian OnDemand sites with multiple apps. If you are using Confluence-only OnDemand, the information does apply.*

Accessing the User Management Screen

To search for and manage users:

1. Go to the user management screen for the user concerned. There are two ways to do this:
   - Either,
     - Go to the user's Profile and click the '**Administer User**' link on the user's profile screen. (This link is available in Confluence 2.8.2 and later.)
   - Or, Choose **Browse** > **Confluence Admin**.
     - Select '**Manage Users**' in the left-hand panel.
     - The '**Manage Users**' screen appears, as shown below. You can now choose to list all users or you can search for a specific user.

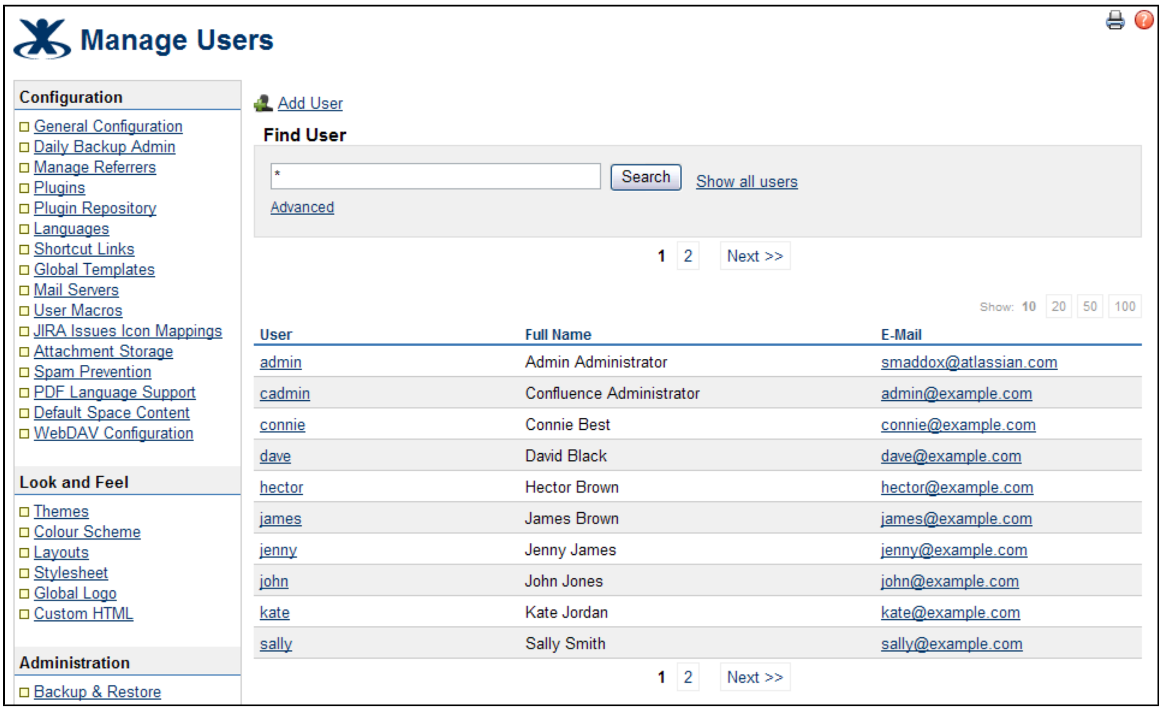


Screenshot above: Managing users

Listing All Users

To list all users:

1. Open the '**Manage Users**' screen as described above.
2. Click the '**Show all users**' link. All members of the confluence-users group are listed in alphabetical order, by username. If there are more users than can fit on one page, the results will be divided into multiple pages.
3. To move to another page of results, click the numbered links, '**Next**' or '**Previous**' near the top or bottom of the page.
4. To specify how many results should be shown per page, click a number '**10**', '**20**', '**50**' or '**100**' near the top of the page.



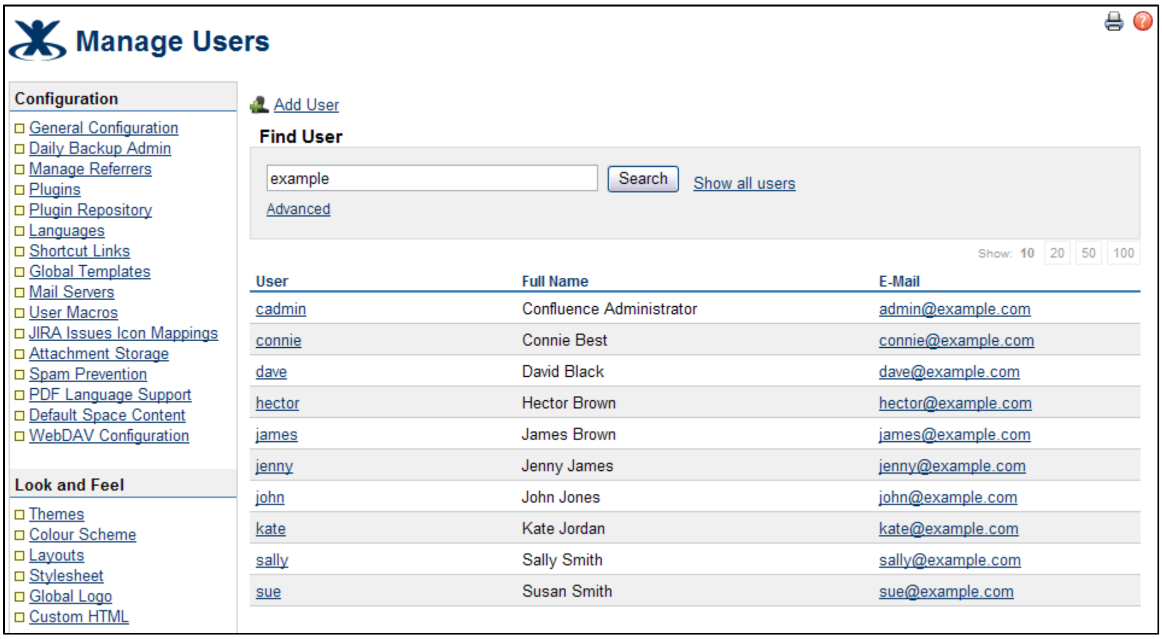
User	Full Name	E-Mail
admin	Admin Administrator	smaddox@atlassian.com
cadmin	Confluence Administrator	admin@example.com
connie	Connie Best	connie@example.com
dave	David Black	dave@example.com
hector	Hector Brown	hector@example.com
james	James Brown	james@example.com
jenny	Jenny James	jenny@example.com
john	John Jones	john@example.com
kate	Kate Jordan	kate@example.com
sally	Sally Smith	sally@example.com

Screenshot above: Listing all users

Using the Simple User Search

To search for a specific user via the simple user search:

1. Open the '**Manage Users**' screen as described above.
2. If the '**Simple**' link is showing, click it. (If you see the 'Advanced' link and no 'Simple' link, then you're fine. The simple search is already active.)
3. The simple user search screen will appear, as shown below.
4. Type some information about the user into the 'Search' textbox. You can type all or part of their username, full name or email address.
5. Click the '**Search**' button.
6. Confluence will display a list of matching users. Click the link on a username to see and edit the details for that user.



Manage Users

Configuration

- □ General Configuration
- □ Daily Backup Admin
- □ Manage Referrers
- □ Plugins
- □ Plugin Repository
- □ Languages
- □ Shortcut Links
- □ Global Templates
- □ Mail Servers
- □ User Macros
- □ JIRA Issues Icon Mappings
- □ Attachment Storage
- □ Spam Prevention
- □ PDF Language Support
- □ Default Space Content
- □ WebDAV Configuration

Look and Feel

- □ Themes
- □ Colour Scheme
- □ Layouts
- □ Stylesheet
- □ Global Logo
- □ Custom HTML

Add User

Find User

example [Search] Show all users

Advanced

Show: 10 20 50 100

User	Full Name	E-Mail
cadmin	Confluence Administrator	admin@example.com
connie	Connie Best	connie@example.com
dave	David Black	dave@example.com
hector	Hector Brown	hector@example.com
james	James Brown	james@example.com
jenny	Jenny James	jenny@example.com
john	John Jones	john@example.com
kate	Kate Jordan	kate@example.com
sally	Sally Smith	sally@example.com
sue	Susan Smith	sue@example.com

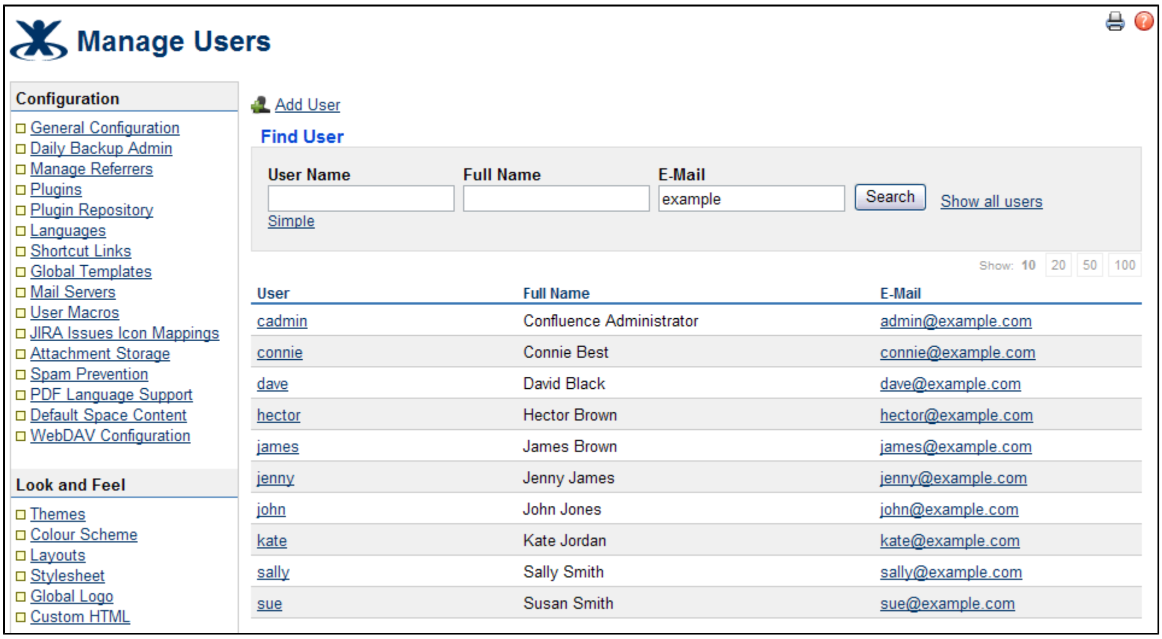
Screenshot above: Simple user search

Using the Advanced User Search

The advanced user search allows you to specify the field in which your search term appears, i.e. username, full name or email address. You may find this useful if you need to limit the number of users appearing in the search results.

To search via the advanced user search:

1. Open the '**Manage Users**' screen as described above.
2. If the '**Advanced**' link is showing, click it. (If you see the 'Simple' link and no 'Advanced' link, then you're fine. The advanced search is already active.)
3. The advanced user search screen will appear, as shown below.
4. Complete one or more of the following fields:
   - **User Name** — Enter all or part of the person's username i.e. their login id, e.g. 'joe', or 'bloggs'.
   - **Full Name** — Enter all or part of the person's name, e.g. 'joe bloggs', or 'bloggs', or 'joe'.
   - **E-Mail** — Enter all or part of the person's email address, e.g. 'acme'
5. Click the '**Search**' button.
6. Confluence will display a list of matching users. Click the link on a username to see and edit the details for that user.



Manage Users

Configuration

- □ General Configuration
- □ Daily Backup Admin
- □ Manage Referrers
- □ Plugins
- □ Plugin Repository
- □ Languages
- □ Shortcut Links
- □ Global Templates
- □ Mail Servers
- □ User Macros
- □ JIRA Issues Icon Mappings
- □ Attachment Storage
- □ Spam Prevention
- □ PDF Language Support
- □ Default Space Content
- □ WebDAV Configuration

Look and Feel

- □ Themes
- □ Colour Scheme
- □ Layouts
- □ Stylesheet
- □ Global Logo
- □ Custom HTML

Add User

Find User

User Name:
Full Name:
E-Mail: example

User	Full Name	E-Mail
cadmin	Confluence Administrator	admin@example.com
connie	Connie Best	connie@example.com
dave	David Black	dave@example.com
hector	Hector Brown	hector@example.com
james	James Brown	james@example.com
jenny	Jenny James	jenny@example.com
john	John Jones	john@example.com
kate	Kate Jordan	kate@example.com
sally	Sally Smith	sally@example.com
sue	Susan Smith	sue@example.com

Screenshot above: Advanced user search

Notes

- **Multiple user directories:** You may define multiple user directories in Confluence, so that Confluence looks in more than one place for its users and groups. For example, you may use the default Confluence **internal directory** and also connect to an **LDAP** directory server. In such cases, you can define the **directory order** to determine where Confluence looks first when processing users and groups. Here is a summary of how the directory order affects the processing:
  - The order of the directories is the order in which they will be searched for users and groups.
  - Changes to users and groups will be made only in the first directory where the application has permission to make changes.

  See Managing Multiple Directories.
- **Crowd and the user search:** If you are using Atlassian's Crowd for user management, you will need Crowd 1.5.1 or later to use the 'Simple' option in the user search. If your version of Crowd does not support the simple user search, you will see only the 'Advanced' search form.

RELATED TOPICS

No content found for label(s) confluence-usermanagement.

administrators guide home Confluence Documentation Home

Adding Users

There are a number of ways to add users to Confluence:

- **By public signup**: If public signup is enabled on your Confluence site, people can add themselves as users of the site. See below.
- **Via an invitation URL:** Administrators with Confluence Administrator or System Administrator permissions can send people an invitation URL. See below.
- **By adding users manually**: Administrators with Confluence Administrator or System Administrator permissions can add new users. See below.
- **Via an external user directory**: See Configuring User Directories.

Choosing public or private signup

You can set your signup mode to public or private at the same time as adding or inviting new users to the site.

You need Confluence Administrator or System Administrator permissions to change the signup mode.

To choose public or private signup:

1. Click **Add Users** on the dashboard.
   Or take the longer route: Choose **Browse** > **Confluence Admin**. Click **Users** > **Add User**.
2. Choose the signup mode:
   a. **Private**: There will not be a 'Sign Up' link on the Confluence screens. People can sign up if an administrator sends them the **Invitation URL**. Administrators can add users manually too.
   b. **Public**: A 'Sign Up' link will appear on the Confluence screens. People can click the link to add their own usernames. In addition, people can sign up if an administrator sends them the **Invitation URL**, and administrators can add users manually.

On this page:

Related pages:

- User Management
- Confluence Administrator's Guide

⚠ *The information on this page does not apply to Atlassian OnDemand sites with multiple apps. If you are using Confluence-only OnDemand, the information does apply.*

Inviting people to sign up via a URL

You can invite new users to the site by sending them a signup URL. This option is available in both public and private signup modes. When someone visits the URL in a browser, a Confluence signup screen will appear.

To invite people to sign up:

1. Click **Add Users** on the dashboard.
   Or take the longer route: Choose **Browse** > **Confluence Admin**. Click **Users** > **Add User**.
2. Copy the **Invitation URL** and paste it into an email message, or onto a page on your extranet.

Resetting the signup URL

If your signup mode is private, the invitation URL will include a security token, like this:

```
http://confluence.example.com/signup.action?token=d513a04456312c47
```

You can change the URL at any time, by clicking **Reset**. The previous URL will become unusable. People will no longer be able to use the previous URL to sign up. Instead, they will see an error message that the signup token has expired.

The reset option is available only in **private** signup mode.

Enabling and disabling notifications about user signup

By default, Confluence will send an email notification to all Confluence administrators whenever someone signs up to the Confluence site, either by clicking the 'Sign Up' link or by clicking the invitation URL sent by an administrator. The notification is enabled by default.

To disable this notification:

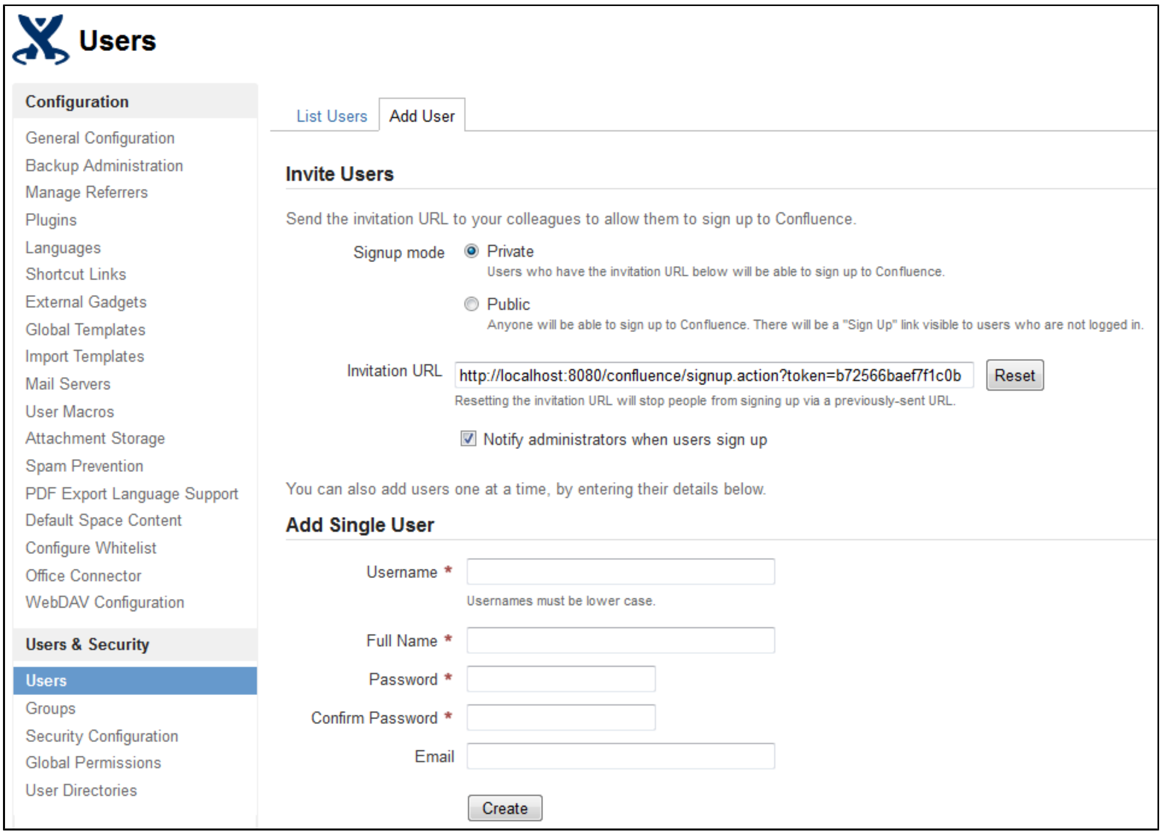
1. Click **Add Users** on the dashboard.
   Or take the longer route: Choose **Browse** > **Confluence Admin**. Click **Users** > **Add User**.
2. Remove the tick from **Notify administrators when users sign up**.

Adding users manually

To add a new user:

1. Click **Add Users** on the dashboard.
   Or take the longer route: Choose **Browse** > **Confluence Admin**. Click **Users** > **Add User**.
2. Enter the user's details: username, password, name and email address.
3. Click **Create**.

Screenshot: Adding and inviting users



Invite Users

Send the invitation URL to your colleagues to allow them to sign up to Confluence.

Signup mode ● Private
Users who have the invitation URL below will be able to sign up to Confluence.
○ Public
Anyone will be able to sign up to Confluence. There will be a "Sign Up" link visible to users who are not logged in.

Invitation URL http://localhost:8080/confluence/signup.action?token=b72566baef7f1c0b
Resetting the invitation URL will stop people from signing up via a previously-sent URL.

☑ Notify administrators when users sign up

You can also add users one at a time, by entering their details below.

Add Single User

Username *
Usernames must be lower case.
Full Name *
Password *
Confirm Password *
Email

Notes

You may define multiple user directories in Confluence, so that Confluence looks in more than one place for its users and groups. For example, you may use the default Confluence **internal directory** and also connect to an **LDAP** directory server. In such cases, you can define the **directory order** to determine where Confluence looks first when processing users and groups. Here is a summary of how the directory order affects the processing:

- The order of the directories is the order in which they will be searched for users and groups.
- Changes to users and groups will be made only in the first directory where the application has permission to make changes.

See Managing Multiple Directories.

Adding a Group

A group is a collection of users. Administrators create groups so that the administrator can assign permissions to a number of people at once. For example, it is quicker to give group 'X' access to Confluence, rather than giving every team member access individually.

> ⚠ *The information on this page does not apply to Atlassian OnDemand sites with multiple apps. If you are using Confluence-only OnDemand, the information does apply.*

To add a new group:

1. Choose **Browse** > **Confluence Admin**.
2. Click **Manage Groups** in the left-hand panel.
3. Click **Add Group**.
4. Enter a name for your group and click **Save**.

You are now ready to start adding users to the group.

Notes

- **Multiple user directories:** You may define multiple user directories in Confluence, so that Confluence looks in more than one place for its users and groups. For example, you may use the default Confluence **internal directory** and also connect to an **LDAP** directory server. In such cases, you can define the **directory order** to determine where Confluence looks first when processing users and groups. Here is a summary of how the directory order affects the processing:
  - The order of the directories is the order in which they will be searched for users and groups.
  - Changes to users and groups will be made only in the first directory where the application has permission to make changes.

  See Managing Multiple Directories.

Related Topics

No content found for label(s) managing-groups.

Adding or Removing Users in Groups

If you are a Confluence Administrator, you can add users and groups, and assign users to groups in order to determine their permissions.

This page tells you how to add a user to a group or remove a user from a group. For an overview of users and groups, please refer to Users and Groups and Confluence User Management.

You can edit group membership in two places:

- From the group management screen.
- From the user management screen for a particular user.

Both methods are described below.

On this page:

The information on this page does not apply to Atlassian OnDemand sites with multiple apps. If you are using Confluence-only OnDemand, the information does apply.

Adding and Removing Members via the Group Management Screen

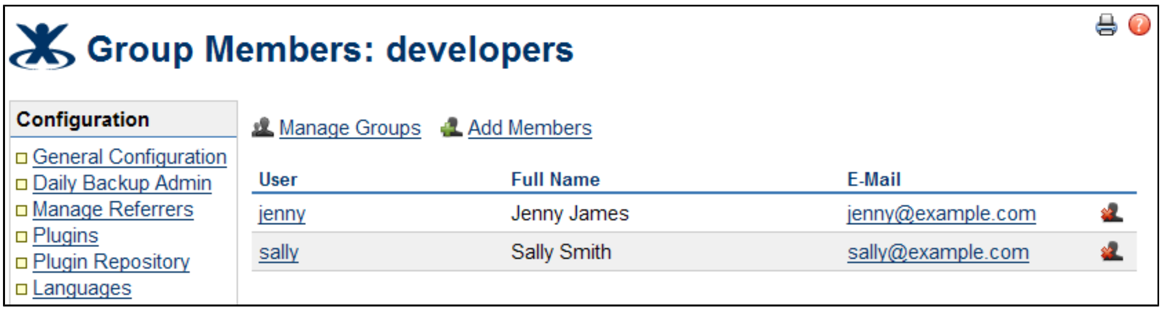
This is the recommended method, available in **Confluence 2.10** and later. It allows you to manage the group membership for a number of users at the same time.

To add members to a group:

1. Choose **Browse** > **Confluence Admin**.
2. Select '**Manage Groups**' in the left-hand panel.
3. The '**Manage Groups**' screen appears, showing a list of groups. Select the group to which you want to add users.
4. The '**Group Members**' screen appears, showing the users who belong to the selected group. (See screenshot below.) Click the '**Add Members**' link.
5. The '**Add Members**' screen appears, as shown below. Type in the usernames of the people you want to add to the group. You can also search for and select users by clicking the icon, as described in Searching for Users.
6. When you have added the required username(s), click the '**Add**' button to add the member(s) to the group.

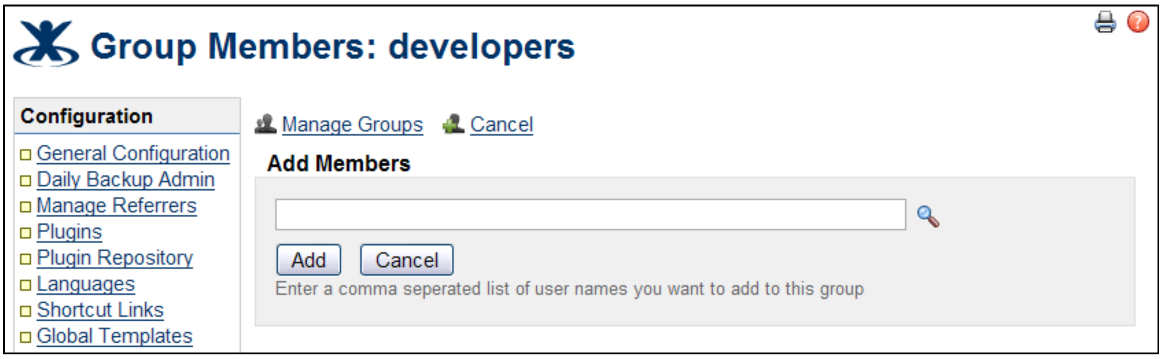
To remove members from a group:

1. Choose **Browse** > **Confluence Admin**.
2. Select '**Manage Groups**' in the left-hand panel.
3. The '**Manage Groups**' screen appears, showing a list of groups. Select the group from which you want to remove the user.
4. The '**Group Members**' screen appears, showing the users who belong to the selected group. (See screenshot below.) Click the 'Remove user from group' icon next to the user whose group membership you want to remove.



User	Full Name	E-Mail
jenny	Jenny James	jenny@example.com
sally	Sally Smith	sally@example.com

Screenshot above: Group members



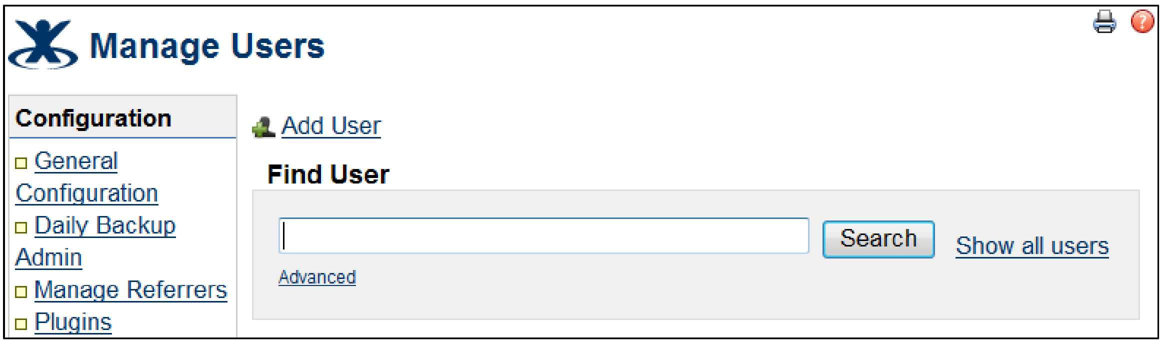
Screenshot above: Adding members

Editing Group Membership from the User Management Screen

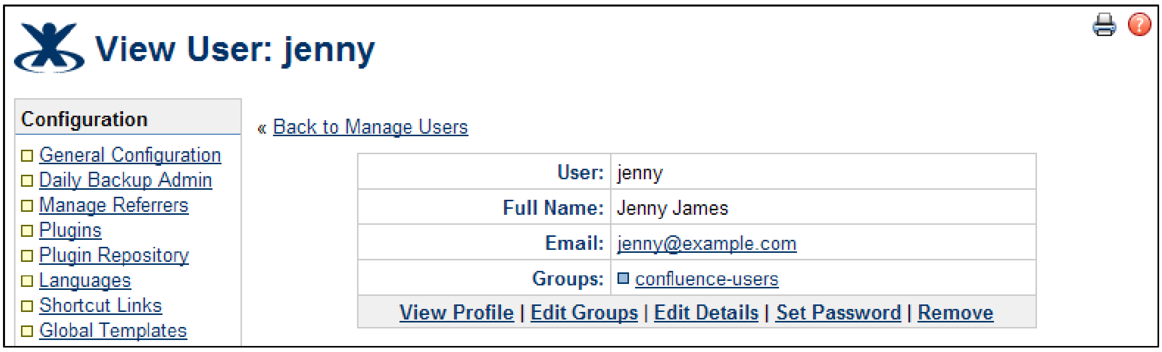
You can update a user's group membership from the user management screen. This functionality allows you to update one user at a time.

To add a user to a group or remove a user from a group:

1. Go to the user management screen for the user concerned. There are two ways to do this:
    - Either,
        - Go to the user's Profile and click the '**Administer User**' link on the user's profile screen. (This link is available in Confluence 2.8.2 and later.)
    - Or, Choose **Browse** > **Confluence Admin**.
        - Select '**Manage Users**' in the left-hand panel.
        - The '**Manage Users**' screen appears, as shown below. You can now choose to '**Show all users**' or you can search for a specific user by entering all or part of the person's username, full name or email address. (For more details about the user search, see Searching For and Managing Users.)
        - Click the link on the username you want to edit.
2. Now you should be able to see the user's current details, with links allowing you to edit the user's details and groups. See the screenshot showing a user's details below.
3. Click '**Edit Groups**'. This will display two lists of groups, as shown in the screenshot below. Update the user's group membership as follows:
    - '**Not a member of groups**' — This box shows all groups to which the user does not belong. To add the user to a group, select a group and click '**Join**'. Hold the Ctrl key down and click to select more than one group.
    - '**Member of groups**' — This box shows all groups to which the user belongs. Select a group and click '**Leave**' to remove the user from the group.

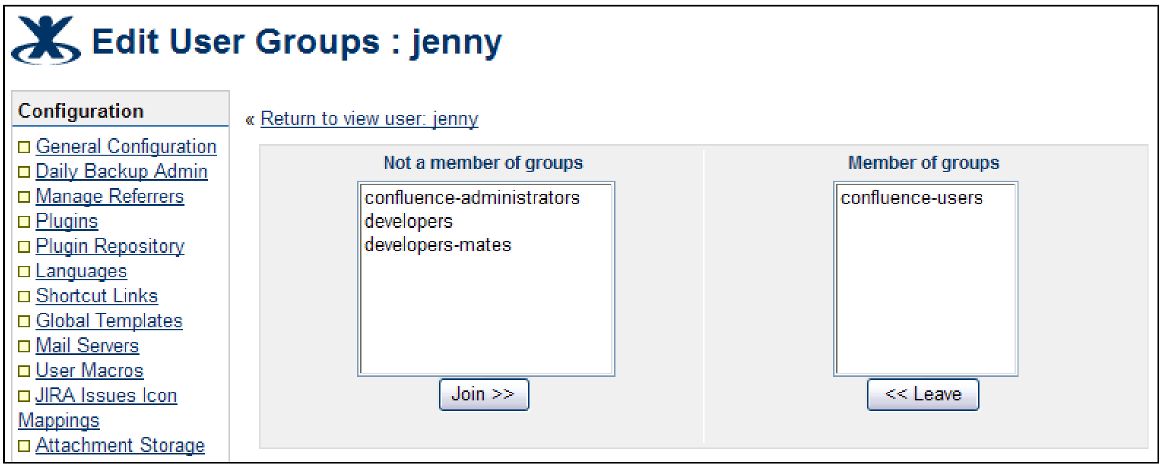


Screenshot above: Managing users



User:	jenny
Full Name:	Jenny James
Email:	jenny@example.com
Groups:	confluence-users

Screenshot above: User details



Not a member of groups	Member of groups
confluence-administrators developers developers-mates	confluence-users

Screenshot above: Editing a user's groups

Notes

- **Multiple user directories:** You may define multiple user directories in Confluence, so that Confluence looks in more than one place for its users and groups. For example, you may use the default Confluence **internal directory** and also connect to an **LDAP** directory server. In such cases, you can define the **directory order** to determine where Confluence looks first when processing users and groups. Here is a summary of how the directory order affects the processing:
  - The order of the directories is the order in which they will be searched for users and groups.
  - Changes to users and groups will be made only in the first directory where the application has permission to make changes.

  See Managing Multiple Directories.

RELATED TOPICS

No content found for label(s) confluence-usermanagement.

Administrators Guide Home Confluence Documentation Home

Changing Usernames

A **username** is the name used to log into Confluence, eg. `jsmith`.

Currently, there is no straightforward method for changing a username and its associated content, to that of another user. The only practicable method currently available is to execute direct SQL queries on your database. There is a feature request to facilitate this process via a web interface and you can vote for it to improve its chances of being implemented. Be aware, however, that no matter what method you use to change usernames in Confluence, there is **no support** provided for this process. The instructions below provide suggested guidelines on how to change a username via SQL queries, although this may vary depending on your database.

The information on this page does not apply to Atlassian OnDemand sites with multiple apps. If you are using Confluence-only OnDemand, the information does apply.

Instructions For Changing Usernames

This document is for use with 3.5. If using an earlier version, please see the 3.4 version of the page.

The following SQL commands are only tested for MySQL and PostgreSQL Databases. If you have any other database please contact your DBA to determine the equivalent queries.

Usernames can only be changed through direct update to the Confluence database.

1. If you have a database administrator, request that they approve the database-related steps described below
2. If you are using JIRA user management, Revert from JIRA To Internal User Management
3. Backup Confluence
4. If you are using MySQL, make sure you are not running in safe updates mode:

```
set sql_safe_updates=0;
```

5. Create a `usermigration`table:

```
create table usermigration
(
oldusername varchar(255),
newusername varchar(255)
)
```

6. Usernames that will be changed must be placed in the `usermigration`table with their current and planned usernames:

```
insert into usermigration (oldusername, newusername)
values ('oldusername', 'newusername');
```

7. Run the following SQL commands:
   a. If you have command line access to your database, download the scripts for PostgreSQL or MySQL then run them against your database:

PostgreSQL

```
$ psql -f PostgreSQLChangeUsernames.sql your_database_name
```

MySQL

```
$ mysql your_database_name < MySQLChangeUsernames.sql
```

b. Otherwise, run the following:
   i. If your DB administration tool does not support multiple SQL queries, these must be entered individually:

PostgreSQL

```
update attachments
set creator = newusername from usermigration u
where creator = u.oldusername;

update attachments
set lastmodifier = newusername from usermigration u
where lastmodifier = u.oldusername;

update content
set creator = newusername from usermigration u
where creator = u.oldusername;

update content
set lastmodifier = newusername from usermigration u
where lastmodifier = u.oldusername;

update content
set username = newusername from usermigration u
where username = u.oldusername;

update content_label
set owner = newusername from usermigration u
where owner = u.oldusername;

update content_perm
set creator = newusername from usermigration u
where creator = u.oldusername;

update content_perm
set lastmodifier = newusername from usermigration u
where lastmodifier = u.oldusername;

update content_perm
set username = newusername from usermigration u
where username = u.oldusername;

update contentlock
set creator = newusername from usermigration u
where creator = u.oldusername;
```

```
update contentlock
set lastmodifier = newusername from usermigration u
where lastmodifier = u.oldusername;

update cwd_user
set lower_user_name = lower(newusername) from usermigration
u
where lower_user_name = lower(u.oldusername);

update cwd_user
set user_name = newusername from usermigration u
where user_name = u.oldusername;

update extrnlnks
set creator = newusername from usermigration u
where creator = u.oldusername;

update extrnlnks
set lastmodifier = newusername from usermigration u
where lastmodifier = u.oldusername;

update follow_connections
set followee = newusername from usermigration u
where followee = u.oldusername;

update follow_connections
set follower = newusername from usermigration u
where follower = u.oldusername;

update label
set owner = newusername from usermigration u
where owner = u.oldusername;

update links
set creator = newusername from usermigration u
where creator = u.oldusername;

update links
set lastmodifier = newusername from usermigration u
where lastmodifier = u.oldusername;

update notifications
set creator = newusername from usermigration u
where creator = u.oldusername;

update notifications
set lastmodifier = newusername from usermigration u
where lastmodifier = u.oldusername;

update notifications
set username = newusername from usermigration u
where username = u.oldusername;

update pagetemplates
set creator = newusername from usermigration u
where creator = u.oldusername;

update pagetemplates
set lastmodifier = newusername from usermigration u
where lastmodifier = u.oldusername;
```

```
update remembermetoken
set username = newusername from usermigration u
where username = u.oldusername;

update spacegroups
set creator = newusername from usermigration u
where creator = u.oldusername;

update spacegroups
set lastmodifier = newusername from usermigration u
where lastmodifier = u.oldusername;

update spacepermissions
set creator = newusername from usermigration u
where creator = u.oldusername;

update spacepermissions
set lastmodifier = newusername from usermigration u
where lastmodifier = u.oldusername;

update spacepermissions
set permusername = newusername from usermigration u
where permusername = u.oldusername;

update spaces
set creator = newusername from usermigration u
where creator = u.oldusername;

update spaces
set lastmodifier = newusername from usermigration u
where lastmodifier = u.oldusername;

update trackbacklinks
set creator = newusername from usermigration u
where creator = u.oldusername;
```

```
update trackbacklinks
set lastmodifier = newusername from usermigration u
where lastmodifier = u.oldusername;
```

MySQL

```
update ATTACHMENTS a, usermigration u
set a.creator = u.newusername
where a.creator = u.oldusername;

update ATTACHMENTS a, usermigration u
set a.lastmodifier = u.newusername
where a.lastmodifier = u.oldusername;

update CONTENT a, usermigration u
set a.creator = u.newusername
where a.creator = u.oldusername;

update CONTENT a, usermigration u
set a.lastmodifier = u.newusername
where a.lastmodifier = u.oldusername;

update CONTENT a, usermigration u
set a.username = u.newusername
where a.username = u.oldusername;

update CONTENTLOCK a, usermigration u
set a.creator = u.newusername
where a.creator = u.oldusername;

update CONTENTLOCK a, usermigration u
set a.lastmodifier = u.newusername
where a.lastmodifier = u.oldusername;

update CONTENT_LABEL a, usermigration u
set a.owner = u.newusername
where a.owner = u.oldusername;

update CONTENT_PERM a, usermigration u
set a.creator = u.newusername
where a.creator = u.oldusername;

update CONTENT_PERM a, usermigration u
set a.lastmodifier = u.newusername
where a.lastmodifier = u.oldusername;

update CONTENT_PERM a, usermigration u
set a.username = u.newusername
where a.username = u.oldusername;

update CWD_USER a, usermigration u
set a.lower_user_name = LOWER(u.newusername)
where a.lower_user_name = LOWER(u.oldusername);

update CWD_USER a, usermigration u
set a.user_name = u.newusername
where a.user_name = u.oldusername;
```

```
update EXTRNLNKS a, usermigration u
set a.creator = u.newusername
where a.creator = u.oldusername;

update EXTRNLNKS a, usermigration u
set a.lastmodifier = u.newusername
where a.lastmodifier = u.oldusername;

update FOLLOW_CONNECTIONS a, usermigration u
set a.followee = u.newusername
where a.followee = u.oldusername;

update FOLLOW_CONNECTIONS a, usermigration u
set a.follower = u.newusername
where a.follower = u.oldusername;

update LABEL a, usermigration u
set a.owner = u.newusername
where a.owner = u.oldusername;

update LINKS a, usermigration u
set a.creator = u.newusername
where a.creator = u.oldusername;

update LINKS a, usermigration u
set a.lastmodifier = u.newusername
where a.lastmodifier = u.oldusername;

update NOTIFICATIONS a, usermigration u
set a.creator = u.newusername
where a.creator = u.oldusername;

update NOTIFICATIONS a, usermigration u
set a.lastmodifier = u.newusername
where a.lastmodifier = u.oldusername;

update NOTIFICATIONS a, usermigration u
set a.username = u.newusername
where a.username = u.oldusername;

update PAGETEMPLATES a, usermigration u
set a.creator = u.newusername
where a.creator = u.oldusername;

update PAGETEMPLATES a, usermigration u
set a.lastmodifier = u.newusername
where a.lastmodifier = u.oldusername;

update REMEMBERMETOKEN a, usermigration u
set a.username = u.newusername
where a.username = u.oldusername;

update SPACEGROUPS a, usermigration u
set a.creator = u.newusername
where a.creator = u.oldusername;

update SPACEGROUPS a, usermigration u
set a.lastmodifier = u.newusername
where a.lastmodifier = u.oldusername;
```

```
update SPACEPERMISSIONS a, usermigration u
set a.creator = u.newusername
where a.creator = u.oldusername;

update SPACEPERMISSIONS a, usermigration u
set a.lastmodifier = u.newusername
where a.lastmodifier = u.oldusername;

update SPACEPERMISSIONS a, usermigration u
set a.permusername = u.newusername
where a.permusername = u.oldusername;

update SPACES a, usermigration u
set a.creator = u.newusername
where a.creator = u.oldusername;

update SPACES a, usermigration u
set a.lastmodifier = u.newusername
where a.lastmodifier = u.oldusername;

update TRACKBACKLINKS a, usermigration u
set a.creator = u.newusername
where a.creator = u.oldusername;
```

```
update TRACKBACKLINKS a, usermigration u
set a.lastmodifier = u.newusername
where a.lastmodifier = u.oldusername;
```

ii. Reassign user preferences in the OS_PROPERTYENTRY table. Usernames in the OS_PROPERTYENTRY table need to be prefixed with 'CWD_'.

PostgreSQL

```
update os_propertyentry
set entity_name = 'CWD_' || newusername from usermigration u
where entity_name = 'CWD_' || u.oldusername;
```

MySQL

```
update OS_PROPERTYENTRY a, usermigration u
set a.entity_name = concat('CWD_', u.newusername)
where a.entity_name = concat('CWD_', u.oldusername);
```

iii. Reassign personal spaces and settings associated with the old username to the new username. The tilda (~) is required as it is prepended to the space key of all personal spaces:

PostgreSQL

```
update spaces
set spacekey = '~' || newusername from usermigration u
where spacekey = '~' || u.oldusername;

update bandana
set bandanacontext = '~' || newusername from usermigration u
where bandanacontext = '~' || u.oldusername;
```

MySQL

```
update SPACES a, usermigration u
set a.spacekey = concat('~', u.newusername)
where a.spacekey = concat('~', u.oldusername);

update BANDANA a, usermigration u
set a.bandanacontext = concat('~', u.newusername)
where a.bandanacontext = concat('~', u.oldusername);
```

8. Each username is associated with a full name. For example, username 'jsmith' may have a full name of 'John M Smith'. If this fullname needs to be changed, modify the `first_name`, `lower_first_name`, `last_name` and `lower_last_name` in the `cwd_user` table. Ensure the `lower_` columns are merely copies of their normal counterparts but with all letters in lower case. Then modify the `display_name` and `lower_display_name` columns so that they are the `first_name` and `last_name` columns or the `lower_first_name` and `lower_last_name` columns put together but separated by a space.

Rebuild the Indexes

After all the updates, it's necessary to Rebuild the Indexes from Scratch

All old usernames in Confluence should now be replaced with the new usernames from the `usermigration` table.

RELATED TOPICS

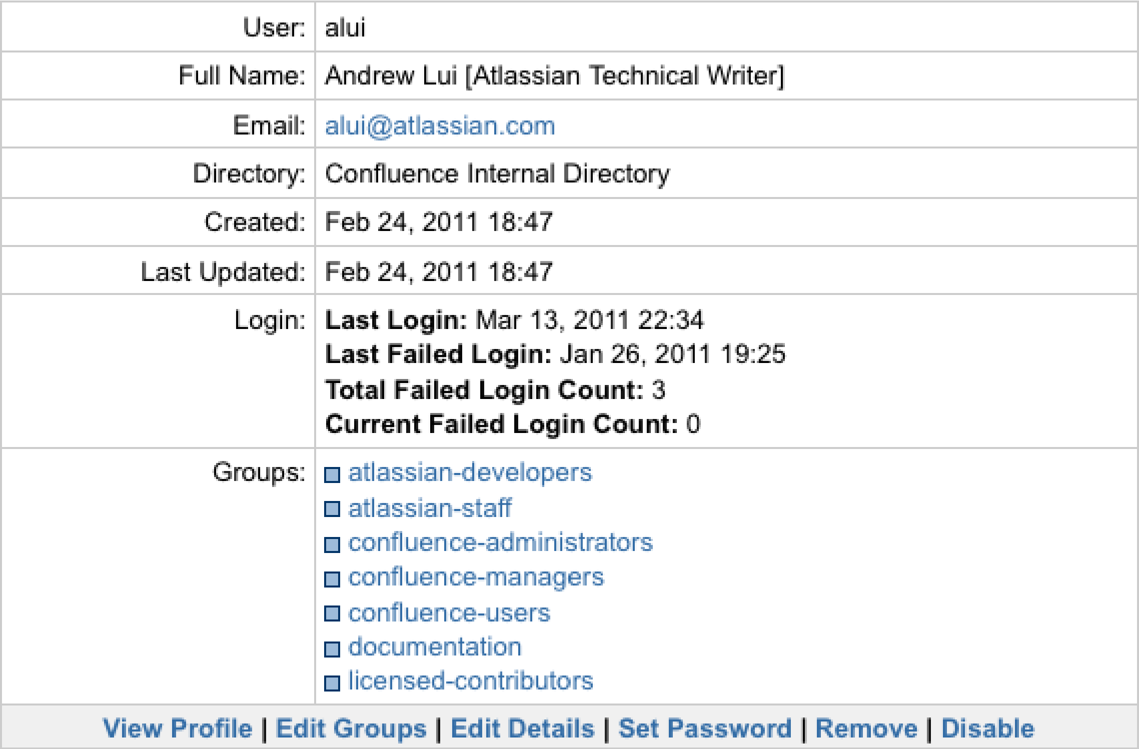
No content found for label(s) confluence-usermanagement.

Administrators Guide Home Confluence Documentation Home

Editing User Details

To update a user's details:

1. First, go to the user management screen for the user concerned. There are two ways to do this:
    - Either,
        - Go to the user's Profile and click the '**Administer User**' link on the user's profile screen.
    - Or, Choose **Browse** > **Confluence Admin**.
        - Select the link '**Manage Users**' in the left-hand panel.
        - Locate the user by doing a search on the username or the groups to which they belong.
        - Click the user link.
2. Now you should be able to see the user's current details and links allowing you to edit them.
    - **View Profile** — View the user's profile.
    - **Edit Groups** — Add or remove this user from a group.
    - **Edit Details** — Change details such as the user's name, email address, contact details and team or department information.
      Changing a user's username is not supported. See Changing Usernames for information.
    - **Set Password** — Edit the user's password details.
    - **Remove** — You can remove a user permanently if the user has not added or edited any content on the site.
    - **Disable** — You can disable (i.e. deactivate) access for a user who has already added or edited any content on the site.



User:	alui
Full Name:	Andrew Lui [Atlassian Technical Writer]
Email:	alui@atlassian.com
Directory:	Confluence Internal Directory
Created:	Feb 24, 2011 18:47
Last Updated:	Feb 24, 2011 18:47
Login:	**Last Login:** Mar 13, 2011 22:34 **Last Failed Login:** Jan 26, 2011 19:25 **Total Failed Login Count:** 3 **Current Failed Login Count:** 0
Groups:	atlassian-developers atlassian-staff confluence-administrators confluence-managers confluence-users documentation licensed-contributors

View Profile | **Edit Groups** | **Edit Details** | **Set Password** | **Remove** | **Disable**

Screenshot above: User details

> *The information on this page does not apply to Atlassian OnDemand sites with multiple apps. If you are using Confluence-only OnDemand, the information does apply.*

Notes

- **Multiple user directories:** You may define multiple user directories in Confluence, so that Confluence looks in more than one place for its users and groups. For example, you may use the default Confluence **internal directory** and also connect to an **LDAP** directory server. In such cases, you can define the **directory order** to determine where Confluence looks first when processing users and groups. Here is a summary of how the directory order affects the processing:
  - The order of the directories is the order in which they will be searched for users and groups.
  - Changes to users and groups will be made only in the first directory where the application has permission to make changes.

  See Managing Multiple Directories.

RELATED TOPICS

No content found for label(s) managing-users.

Administrators Guide Home Confluence Documentation Home

Global Groups Overview

There are two special default groups in Confluence:

1. **confluence-administrators**: This is a group of 'super-users' who can access the 'Administration Console' and perform site-wide administration. Members of this group can also see all spaces in the Confluence instance.
   Any user who is a member of this group has site-wide administration powers, regardless of any other setting. The settings on the Global Permissions screen do **not** affect the powers allowed to members of this group.
2. **confluence-users**: This is the default group for all new users. Permissions you assign to this group will be assigned to all newly signed-up users of Confluence.

> **Confluence Administrator permission and confluence-administrators group are not related**
>
> Going by the names, you would think the 'confluence-administrators' group and the 'Confluence Administrator' permission are related – but they are not. To resolve confusion, we want to make explicit that granting a user or group 'Confluence Administrator' permission is *not* the same as granting them membership to the 'confluence-administrators' group. Granting the 'Confluence Administrator' permission enables access to only a subset of the administrative functions. Granting membership to the 'confluence-administrators' group, on the other hand, gives complete access.

> *The information on this page does not apply to Atlassian OnDemand sites with multiple apps. If you are using Confluence-only OnDemand, the information does apply.*

> ⚠ **Confluence Administrator permission and confluence-administrators group are not related**
>
> Going by the names, you would think the 'confluence-administrators' group and the 'Confluence Administrator' permission are related – but they are not. To resolve confusion, we want to make explicit that granting a user or group 'Confluence Administrator' permission is *not* the same as granting them membership to the 'confluence-administrators' group. Granting the 'Confluence Administrator' permission enables access to only a subset of the administrative functions. Granting membership to the 'confluence-administrators' group, on the other hand, gives complete access.

Other user groups : A Confluence administrator can also group users together into user groups for more convenient administration. Once created, groups become available at the space and page levels to allow for flexible access control. A user in one of these groups will automatically be granted all permissions granted to the group.

Anonymous users : Confluence treats all users who do not log in when they access Confluence as being 'anonymous'. You can grant anonymous '**Use Confluence**' permission via the Global Permissions screen. This will allow non-registered users to access pages and spaces in Confluence. A space administrator can then further control anonymous access per space via the space permissions.

Related Topics

No content found for label(s) confluence-usermanagement.

Administrators Guide Home Confluence Documentation Home

Global Permissions Overview

Permissions determine the actions which a user is allowed to perform within Confluence. Global permissions are one of the levels of permission provided by Confluence.

In order to assign these permissions, you must already have the global 'Confluence Administrator' or 'System Administrator' permission (described below). You can then assign global permissions to groups, individual users and anonymous users. Further permissions are granted from the space administration screens.

On this page:

Related pages:

- Searching For and Managing Users
- Enabling or Disabling Public Signup
- Global Groups Overview
- Confluence Administrator's Guide

⚠ *Some functionality described on this page is restricted in **Confluence OnDemand**.*

Overview of the global permissions

Global permissions control access across the whole Confluence site. Here is a list:

Global Permission	Description
Can Use	This is the most basic permission that allows users to access the site. ℹ Users with this permission count towards the number of users allowed by your license. See the information on removing/deactivating users.
Attach Files to User Profile	This allows the user to upload files to be stored in their user profile. ℹ This feature was made obsolete by the introduction of personal spaces in Confluence 2.2. Hence, this permission is no longer relevant. Attachments can be accessed from a user profile view (for example, an image within the 'About Me' field of a profile view) by attaching these files to a page within that user's personal space and referencing them using appropriate wiki markup code.
Update User Status	This allows the user to update their user status message, which can be seen on the user's profile, pages in their personal space and on various activity streams accessible to other Confluence users.
Personal Space	This permission allows the user to create a personal space.
Create Space(s)	This permission allows users to create new spaces within your Confluence site. When a space is created, the creator automatically has the 'Admin' permission f or that space and can perform space-wide administrative functions.
Confluence Administrator	This permission allows users to access the 'Administration Console' that controls site-wide administrative functions. Users with this permission can perform most, but not all, of the Confluence administrative functions. See the comparison of 'System Administrator' and 'Confluence Administrator' below.
System Administrator	This permission allows users to access the 'Administration Console' that controls site-wide administrative functions. Users with this permission can perform all the Confluence administrative functions, including the ones which the 'Confluence Administrator' permission does not allow. See the comparison of 'System Administrator' and 'Confluence Administrator' below. Refer also to the note about the 'confluence-administrators' group belo w.

The first system administrator is defined during installation

During the initial configuration of Confluence, the Setup Wizard asks for the username of the System Administrator. This user will have the 'System Administrator' permission and will be a member of the 'confluence-administrators' group.

Comparing the System Administrator with the Confluence Administrator Permission

Confluence recognises two levels of administrator:

- **System Administrator** – Users with this permission can perform all the Confluence administrative functions, including the ones which the 'Confluence Administrator' permission does not allow.
- **Confluence Administrator** – Users with this permission can perform most, but not all, of the Confluence administrative functions.

✅ **Tip:** The two-tier administration is useful when you want to delegate some administrator privileges to project managers or team leaders. You can give 'Confluence Administrator' permission to users who should be able to perform most administrative functions, but should not be able to perform functions that can compromise the security of the Confluence system.

The following functions are excluded from the 'Confluence Administrator' permission:

Administration Screen	Excluded from Confluence Administrator permission
General Configuration	The following functionality is disallowed: • Server Base URL • Remote API plugin • Public Signup • Connection Timeouts
Security Configuration	The following functionality is disallowed: • External user management • Append wildcards to user and group searches • Anti XSS Mode • Enable Custom Stylesheets for Spaces • Show system information on the 500 page • Maximum RSS Items • XSRF Protection
Plugins	The following functionality is disallowed: • Upgrade • Install • Confluence Upgrade Check
Daily Backup Admin	This function is disallowed entirely.
Mail Servers	This function is disallowed entirely.
User Macros	This function is disallowed entirely.

Attachment Storage	This function is disallowed entirely.
Layouts	This function is disallowed entirely.
Custom HTML	This function is disallowed entirely.
Backup & Restore	This function is disallowed entirely.
Logging and Profiling	This function is disallowed entirely.
Cluster Configuration	This function is disallowed entirely.
Scheduled Jobs	This function is disallowed entirely.
Application Links	This function is disallowed entirely.

Comparing the Administrator Permissions with the confluence-administrators Group

The 'confluence-administrators' group defines a set of 'super-users' who can access the Administration Console and perform site-wide administration. Members of this group can also see the content of all pages and spaces in the Confluence instance, regardless of space permissions. They cannot immediately see the pages for which they are excluded by page restrictions without knowing the direct URL to the page (restrictions can be removed by members of the confluence-administrators group in the Space Admin screen if need be). For example, they will not see restricted pages displayed by the children macro. But they are able to access restricted pages directly using the page URL. The settings on the 'Global Permissions' screen do not affect the powers allowed to members of this group.

Granting the 'System Administrator' or 'Confluence Administrator' permission to a user will *not* automatically grant the user access to all spaces in the site. These permissions will only give access to the Administration Console.

Be aware, however, that users with 'System Administrator' can add themselves to the 'confluence-administrators' group and become a super-user.

> **Confluence Administrator permission and confluence-administrators group are not related**
>
> Going by the names, you would think the 'confluence-administrators' group and the 'Confluence Administrator' permission are related – but they are not. To resolve confusion, we want to make explicit that granting a user or group 'Confluence Administrator' permission is *not* the same as granting them membership to the 'confluence-administrators' group. Granting the 'Confluence Administrator' permission enables access to only a subset of the administrative functions. Granting membership to the 'confluence-administrators' group, on the other hand, gives complete access.

Read more about global groups.

Updating Global Permissions

To view the global permissions for a group or user:

1. Choose **Browse** > **Confluence Admin**.
2. Select **Global Permissions** in the **Security** section of the left-hand panel. The **View Global Permissions** screen appears.

Add or edit group and user permissions as follows:

To add permissions for a group:

1. First add the group to Confluence, if you have not already done so.
2. Click **Edit Permissions**. The 'Edit Global Permissions' screen appears, as shown below.
3. Enter the group name in the **Grant browse permission to** box in the 'Groups' section. You can search for the group name.
4. Click **Add**.
5. The group will appear in the list and you can now edit its permissions.

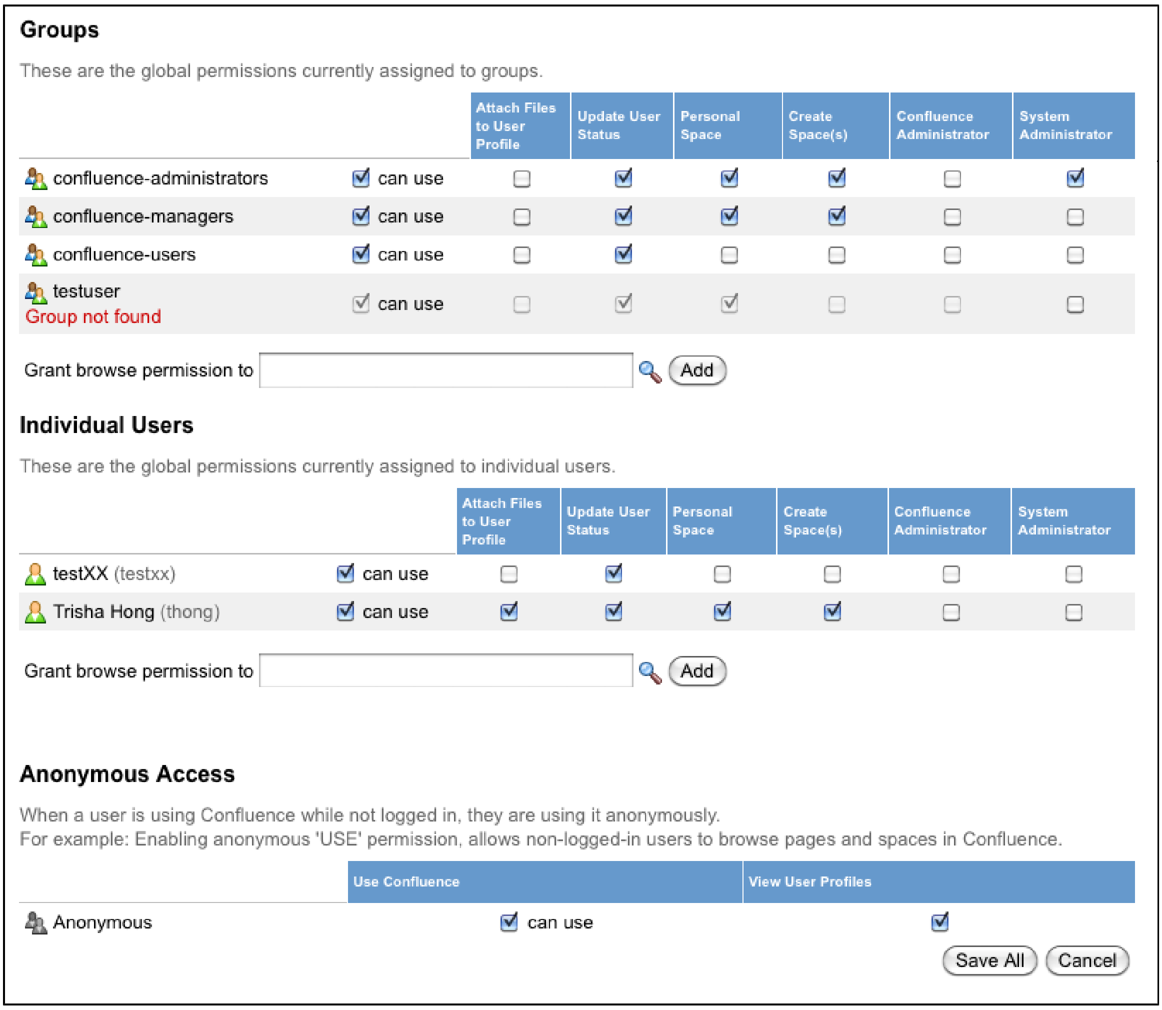
To add permissions for a specific user:
(Consider adding the user to a group and then assigning the permissions to the group, as described above, instead of assigning permissions to the specific user.)

1. First add the user to Confluence, if you have not already done so.
2. Click **Edit Permissions**. The 'Edit Global Permissions' screen appears, as shown below.
3. Enter the username in the **Grant browse permission to** box in the 'Individual Users' section. You can search for the username.
4. Click **Add**.
5. The username will appear in the list and you can now edit its permissions.

To add or edit the permissions for a user or group:

1. Select, or clear, the check box under the relevant permission in the row for the relevant user/group. A selected check box indicates that the permission is granted.
2. To allow anonymous access to your Confluence site, select the 'Use Confluence' and 'View User Profile' options in the 'Anonymous Access' section.
   ℹ For more information about these permissions, refer to Setting up Anonymous Access.
3. Click **Save All** to save your changes.

Screenshot: Editing global permissions



Groups

These are the global permissions currently assigned to groups.

		Attach Files to User Profile	Update User Status	Personal Space	Create Space(s)	Confluence Administrator	System Administrator
confluence-administrators	☑ can use	□	☑	☑	☑	□	☑
confluence-managers	☑ can use	□	☑	☑	☑	□	□
confluence-users	☑ can use	□	☑	□	□	□	□
testuser Group not found	☑ can use	□	☑	☑	□	□	□

Grant browse permission to Add

Individual Users

These are the global permissions currently assigned to individual users.

		Attach Files to User Profile	Update User Status	Personal Space	Create Space(s)	Confluence Administrator	System Administrator
testXX (testxx)	☑ can use	□	☑	□	□	□	□
Trisha Hong (thong)	☑ can use	☑	☑	☑	☑	□	□

Grant browse permission to Add

Anonymous Access

When a user is using Confluence while not logged in, they are using it anonymously.
For example: Enabling anonymous 'USE' permission, allows non-logged-in users to browse pages and spaces in Confluence.

	Use Confluence	View User Profiles
Anonymous	☑ can use	☑

Error messages you may see

Confluence will let you know if there is a problem with some permissions. In rare situations, you may see the following error messages below a permission:

- 'User/Group not found' — This message may appear if your LDAP repository is unavailable, or if the user/group has been deleted after the permission was created.
- 'Case incorrect. Correct case is: xxxxxx' — This message may appear if the upper/lower case in the permission does not match the case of the username or group name. If you see a number of occurrences of this message, you should consider running the routine supplied to fix the problem.

Removing a Group

To remove a group:

1. Choose **Browse** > **Confluence Admin**.
2. Select '**Manage Groups**' in the left panel. A list of all existing groups is displayed along with links to remove them.
3. Click '**Remove**' beside the group you want to remove. You will need to confirm your action before the group is deleted.

> ⚠ *The information on this page does not apply to Atlassian OnDemand sites with multiple apps. If you are using Confluence-only OnDemand, the information does apply.*

Notes

- **Multiple user directories:** You may define multiple user directories in Confluence, so that Confluence looks in more than one place for its users and groups. For example, you may use the default Confluence **internal directory** and also connect to an **LDAP** directory server. In such cases, you can define the **directory order** to determine where Confluence looks first when processing users and groups. Here is a summary of how the directory order affects the processing:
  - The order of the directories is the order in which they will be searched for users and groups.
  - Changes to users and groups will be made only in the first directory where the application has permission to make changes.

  See Managing Multiple Directories.

RELATED TOPICS

No content found for label(s) other-settings.

Administrators Guide Home Confluence Documentation Home

Removing or Deactivating a User

If you are a Confluence Administrator, you can remove and deactivate users.

You can **remove** a user from Confluence if they have not yet added or edited any content on the site. Such content includes pages and blog posts, and edits and comments on existing pages.

You can **deactivate**, or disable, a user, including one who has contributed content.

- Deactivated users can no longer log in to Confluence.
- Deactivating a user will not remove the content created by them from the site.
- Deactivated users do not count towards your license count. (See the notes below.)

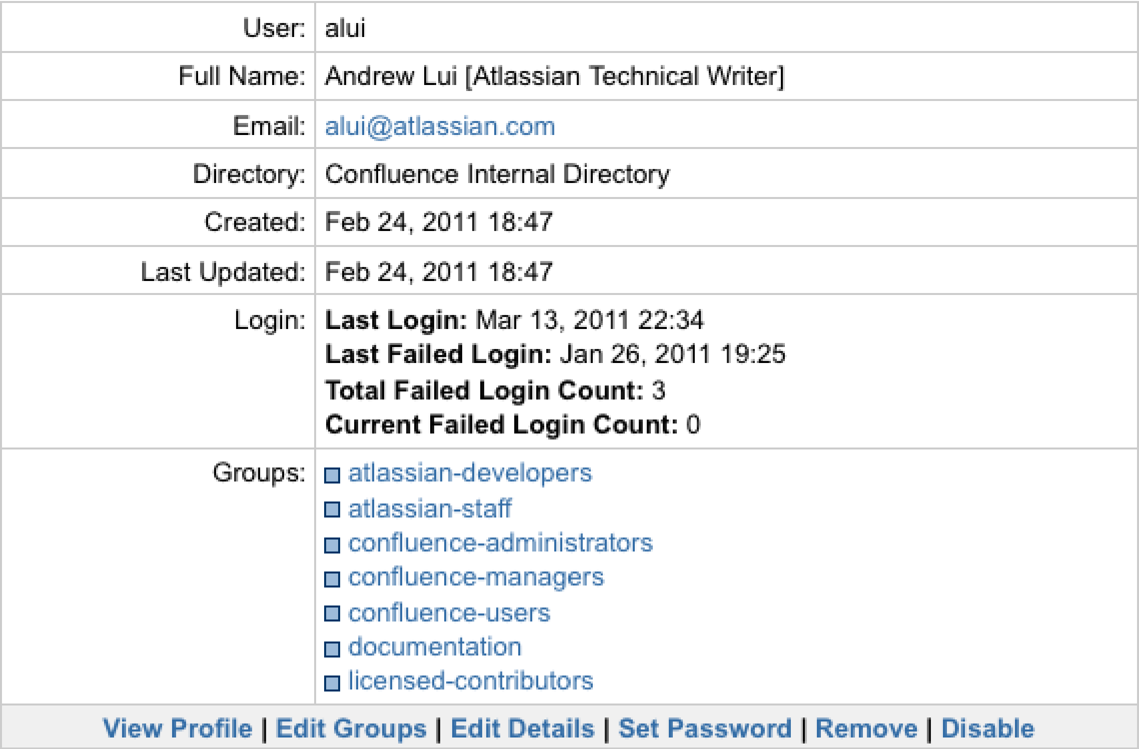
> ⚠ *The information on this page does not apply to Atlassian OnDemand sites with multiple apps. If you are using Confluence-only OnDemand, the information does apply.*

To remove a user:

1. Go to the user's Profile and click the '**Administer User**' link.
2. Click '**Remove**'.

To deactivate a user:

1. Go to the user's Profile and click the '**Administer User**' link.
2. Click '**Disable**'.



User:	alui
Full Name:	Andrew Lui [Atlassian Technical Writer]
Email:	alui@atlassian.com
Directory:	Confluence Internal Directory
Created:	Feb 24, 2011 18:47
Last Updated:	Feb 24, 2011 18:47
Login:	**Last Login:** Mar 13, 2011 22:34 **Last Failed Login:** Jan 26, 2011 19:25 **Total Failed Login Count:** 3 **Current Failed Login Count:** 0
Groups:	■ atlassian-developers ■ atlassian-staff ■ confluence-administrators ■ confluence-managers ■ confluence-users ■ documentation ■ licensed-contributors

View Profile | **Edit Groups** | **Edit Details** | **Set Password** | **Remove** | **Disable**

Screenshot above: Viewing user details

Notes

- The '**Administer User**' link is only visible if you are logged in as an administrator.
- You can also remove or disable users using the Administration Console.
- You can edit the groups that a user belongs to if you don't wish to prevent their access to Confluence completely.
- **Multiple user directories:** You may define multiple user directories in Confluence, so that Confluence looks in more than one place for its users and groups. For example, you may use the default Confluence **internal directory** and also connect to an **LDAP** directory server. In such cases, you can define the **directory order** to determine where Confluence looks first when processing users and groups. Here is a summary of how the directory order affects the processing:
    - The order of the directories is the order in which they will be searched for users and groups.
    - Changes to users and groups will be made only in the first directory where the application has permission to make changes.

  See Managing Multiple Directories.
- **Number of users and your license.** The Confluence 'License Details' screen tells you how many users your Confluence instance is licensed to support, and how many are currently registered. See Viewing and Editing License Details. The number of registered users includes only users who have the 'Can Use' global permission. Deactivated users, as described above, are not included.

Related Topics

No content found for label(s) confluence-usermanagement.

Administrators Guide Home Confluence Documentation Home

Setting up Anonymous Access

You can enable anonymous access (also known as public access) to your site by granting the 'Use Confluence' permission to 'Anonymous' users.

This user category has been created for convenient administration of users who have not logged into the site.

Permissions assigned to this group apply to all anonymous users of the site.

> ⚠ *The information on this page does not apply to Atlassian OnDemand sites with multiple apps. If you are using Confluence-only OnDemand, the information does apply.*

Enabling Anonymous Access

To enable anonymous access to your site,

1. Choose **Browse** > **Confluence Admin**.
2. Click '**Global Permissions**' in the left-hand panel.
3. Click '**Edit Permissions**'.
4. In the 'Anonymous Access' section, select the '**can use**' check box to enable anonymous access to the content on your site.
5. If you selected the '**can use**' check box in the previous step and want to allow anonymous access to user profile views, select the check box in the '**View User Profiles**' section.
   Note: You cannot grant the 'View User Profiles' permission independently of the 'Use Confluence' permission.
6. Click '**Save All**'.
7. You can now grant further permissions from the **space administration screens** to control the viewing and editing privileges of anonymous users. See Space Permissions Overview

Disabling Anonymous Access

To disable anonymous access to your site, clear the '**can use**' check box and the '**View User Profiles**' check box, then click '**Save All**'.

RELATED TOPICS

No content found for label(s) managing-users.

Administrators Guide Home Confluence Documentation Home

Viewing members of a group

To view the members of a group:

1. Choose **Browse** > **Confluence Admin**.
2. Click **Manage Groups** in the left-hand panel. This will list all the existing groups on the site.
3. Click a group name to display all the users in the group.

> ⚠ *The information on this page does not apply to Atlassian OnDemand sites with multiple apps. If you are using Confluence-only OnDemand, the information does apply.*

Notes

- **Multiple user directories:** You may define multiple user directories in Confluence, so that Confluence looks in more than one place for its users and groups. For example, you may use the default Confluence **internal directory** and also connect to an **LDAP** directory server. In such cases, you can define the **directory order** to determine where Confluence looks first when processing users and groups. Here is a summary of how the directory order affects the processing:
  - The order of the directories is the order in which they will be searched for users and groups.
  - Changes to users and groups will be made only in the first directory where the application has

permission to make changes.

See Managing Multiple Directories.

Related Topics

No content found for label(s) managing-groups.

Administrators Guide Home Confluence Documentation Home

Restoring Passwords To Recover Admin User Rights

Use this document if you are unable to log in to Confluence as administrator. The most common reason for using these instructions is if you have lost the administration password for your Confluence site.

Before you Start

Please note the following before you start:

- The following instructions include example SQL that should work on MySQL and PostgreSQL. You may need to customise the queries for other databases or for your installation.
- We strongly recommend testing the queries on a test database before modifying your production database.

New user management in Confluence 3.5 and later

- Confluence now uses the `CWD_USER` table in the database to store and refer to its users.
- When you imported your backup on upgrade from Confluence 3.4.9 or earlier, the upgrade process copied the users from the `OS_USER` table (for upgrades from versions older than 2.7) or the `USERS` table (for versions 2.7 to 3.4) into the `CWD_USER` table.
- The new user management framework also introduced user directories. Making modifications to users in the database will only fully work for users in Confluence's Internal Directory. The instructions below include extra steps for instances in which the user management has been delegated to external sources (via LDAP, Crowd or JIRA).

Please refer to the older documentation if you are still using OSUser or AtlassianUser.

Using Crowd for SSO

- If Confluence is configured for SSO through Crowd, you will only be able to authenticate as users from the Crowd server.
- This document covers how to recover administration rights from the local 'Confluence Internal Directory' only. However, you will not be able to authenticate as a local Confluence administrator while Crowd SSO is enabled. Please refer to Integrating Crowd with Atlassian Confluence for details on how to configure or disable Crowd SSO.

On this page:

⚠ *The information on this page does not apply to Atlassian OnDemand sites with multiple apps. If you are using Confluence-only OnDemand, the information does apply.*

Step 0. Get access to the database

If you are using the embedded HSQL database, you can find the files containing your database in `<confluence-home-directory>/database`. When you shut down Confluence, the SQL will be written to a '.script' or '.log' file in that directory to which you can append the SQL described below.

If you are using a proper production database, connect to the database with your normal tools. You will need to have permission to run queries and update data in the database.

Step 1. Identify Administrator

To find out which usernames have admin privileges, connect to your database using a database admin tool such as DBVisualiser. Please download a database admin tool now if you do not have one installed already. Then connect to your database and retrieve the list of administrator usernames and IDs with:

```
select u.id, u.user_name from cwd_user u
join cwd_membership m on
u.id=m.child_user_id join cwd_group g on
m.parent_id=g.id join cwd_directory d on
d.id=g.directory_id
where g.group_name =
'confluence-administrators' and
d.directory_name='Confluence Internal
Directory';
```

If there are multiple results, choose one ID/username combination to use for the following steps.
If there are no results, skip down to 'If No Local Users Exist' in Step 2.

Step 2. Replace Administrator Password

Confluence does not store passwords in plain text in the database, but uses hashes computed from the original password. You will need to insert a hash, rather than the plain password, over the existing password in the database. Below is the hash for the password `admin`

```
x61Ey612Kl2gpFL56FT9weDnpSo4AV8j8+qx2AuTHdRyY036xxzTTrw10Wq3+4qQyB+XURPWx1ONxp3Y3pB37A==
```

For an External Database

To change the password to `admin` for a given username:

1. Shut down Confluence.
2. Connect to your database.
3. Run the following SQL:

```
update cwd_user set credential =
'x61Ey612Kl2gpFL56FT9weDnpSo4AV8j8+qx2AuTHdRyY036xxzTTrw10Wq3+4qQyB+XUR
PWx1ONxp3Y3pB37A=='
where id=<id from Stage 1>;
```

For the Evaluation Embedded HSQL Database

To change the password to `admin` for a given username:

1. Shut down Confluence.
2. Open `<confluence-home>/database/confluencedb.script`, or `confluencedb.log` if the .script file looks empty.
3. Search for:

   ```
   INSERT INTO CWD_USER VALUES(
   ```

4. Keep searching until you find the appropriate user, then replace their password with the hash value above.
5. Save the file.
6. Restart Confluence.

If No Local Users Exist

There may be no administrators in your Internal Directory. If this is the case, you need to add one:

1. Add a new admin user by running:

   ```
   insert into cwd_user(id, user_name, lower_user_name, active,
   created_date, updated_date, first_name, lower_first_name, last_name,
   lower_last_name, display_name, lower_display_name, email_address,
   lower_email_address, directory_id, credential) values (1212121,
   'admin', 'admin', 'T', '2009-11-26 17:42:08', '2009-11-26 17:42:08',
   'A. D.', 'a. d.', 'Ministrator', 'ministrator', 'A. D. Ministrator',
   'a. d. ministrator', 'admin@example.com', 'admin@example.com', (select
   id from cwd_directory where directory_name='Confluence Internal
   Directory'),
   'x61Ey612Kl2gpFL56FT9weDnpSo4AV8j8+qx2AuTHdRyY036xxzTTrw10Wq3+4qQyB+XUR
   PWx1ONxp3Y3pB37A==');
   ```

2. Add new groups by running:

```
insert into cwd_group(id, group_name, lower_group_name, active, local,
created_date, updated_date, description, group_type, directory_id)
values (
'888888','confluence-administrators','confluence-administrators','T','F
','2011-03-21 12:20:29','2011-03-21 12:20:29',NULL,'GROUP',(select id
from cwd_directory where directory_name='Confluence Internal
Directory'));
insert into cwd_group(id, group_name, lower_group_name, active, local,
created_date, updated_date, description, group_type, directory_id)
values (
'999999','confluence-users','confluence-users','T','F','2011-03-21
12:20:29','2011-03-21 12:20:29',NULL,'GROUP',(select id from
cwd_directory where directory_name='Confluence Internal Directory'));
```

3. Add group memberships into cwd_membership:

```
insert into cwd_membership (id, parent_id, child_user_id) values
(888888, (select id from cwd_group where group_name='confluence-users'
and directory_id=(select id from cwd_directory where
directory_name='Confluence Internal Directory')), 1212121);
insert into cwd_membership (id, parent_id, child_user_id) values
(999999, (select id from cwd_group where
group_name='confluence-administrators' and directory_id=(select id from
cwd_directory where directory_name='Confluence Internal Directory')),
1212121);
```

⚠ If using an Oracle database, use **sysdate** instead of a string for the **`created_date`** column.

Step 3. Put the Internal Directory in First Position

Start Confluence, and try logging in with the username of the user you updated/created and the password 'admin'. If this works, skip to Step 4. Otherwise, your Internal Directory does not have high enough priority.

To put your Internal Directory in first position:

1. Find the directory names and their order:

```
select d.id, d.directory_name, m.list_index from cwd_directory d join
cwd_app_dir_mapping m on d.id=m.directory_id;
```

2. Take note of the ID with list_index 0, and the list_index and ID of the Confluence Internal Directory.
3. Switch the order of the directories:

```
update cwd_app_dir_mapping set list_index = 0 where directory_id =
<Internal Directory id>;
update cwd_app_dir_mapping set list_index = <Noted Internal Directory
list_index> where directory_id = <Directory id that had list_index 0>;
```

4. Check to see if the directory is active (the 'active' column should be set to 'T'):

```
select id, directory_name, active from cwd_directory where id =
<Internal Directory id>;
```

5. If necessary, activate the directory:

```
update cwd_directory set active = 'T' where id = <Internal Directory
id>;
```

Step 4. Clean Up

To tidy up:

1. Start Confluence.
2. Log in with your modified/created username and use password `admin`
3. Change your password. **Do not leave your password as admin, or your instance will not be secure**.
4. If you created a new user in Stage 2, create a new admin via the UI and delete the admin you created in Stage 2.
5. If you followed Stage Three, go to Confluence Administration > User Directories and rearrange your directories so they are correctly configured again.

Notes

- Learn more about the password hash algorithm Confluence is using.

Resetting the Login Count for a User

Confluence records the number of failed logins attempts made against each user account. When the login attempts exceed a preset number (see Configuring Captcha for Failed Logins), the user will prompted to authenticate using CAPTCHA until they successfully log in.

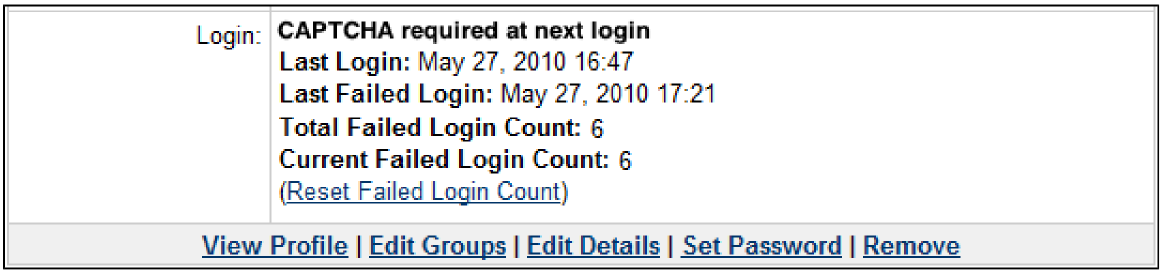
If you are a Confluence Administrator, you can manually reset the failed login count for a user.

> ⚠ *The information on this page does not apply to Atlassian OnDemand sites with multiple apps. If you are using Confluence-only OnDemand, the information does apply.*

To reset the failed login count for a user,

1. Choose **Browse** > **Confluence Admin**.
2. Select '**Manage Users**' in the left-hand panel. The '**Manage Users**' screen appears, as shown below.
3. Search for the desired user and click the user in the search results. The 'View User' screen will be displayed.
4. Click the '**Reset Failed Login Count**' for the user. The 'Current Failed Login Count' will be reset to 0.

Screenshot: Resetting failed login count for a user



Login: **CAPTCHA required at next login**
Last Login: May 27, 2010 16:47
Last Failed Login: May 27, 2010 17:21
Total Failed Login Count: 6
Current Failed Login Count: 6
(Reset Failed Login Count)

View Profile | Edit Groups | Edit Details | Set Password | Remove

Disabling the Built-In User Management

By selecting the '**External user management**' option in Confluence, you can disable the group and user management screens in Confluence. You need system administrator permissions to set this option.

⚠ Setting this option currently has no effect. Please see the notes below.

You will find it useful to select external user management under the following circumstances:

- When Crowd's directory permissions are configured so that Confluence cannot update the Crowd directories, then Confluence's external user management setting **must** be turned on. Otherwise, a 'System Error' will occur when Confluence attempts to write data into Crowd. For more information about integrating Crowd with Confluence, see Connecting to Crowd or JIRA for User Management.
- If you are using JIRA for user management, we recommend that you turn on Confluence's external user management setting. This centralises user management in JIRA. See Connecting to Crowd or JIRA for User Management and Connecting to JIRA 4.2 or Earlier for User Management.

> ⚠ *The information on this page does not apply to Atlassian OnDemand sites with multiple apps. If you are using Confluence-only OnDemand, the information does apply.*

To disable management of users and groups within Confluence:

1. Choose **Browse** > **Confluence Admin**.
2. Click '**Security Configuration**' in the left-hand panel.
3. The '**Edit Security Configuration**' screen will appear. Click '**Edit**'.
4. Tick the '**External user management**' check box.
5. Click '**Save**'.

Notes

- Please refer to the following bugs and improvement requests:
  - CONF-16709 – When the External User Management check box is ticked, the group and user management screens are still functional.
  - CONF-21158 – Enabling both public signup and external user management renders a blank screen during signup.
  - CONF-9830 – This is a request to rename this feature to better reflect its functionality.

RELATED TOPICS

No content found for label(s) external-usermanagement.

Administrators Guide Home Confluence Documentation Home

Integrating Confluence with Other Applications

You can integrate Confluence with other applications using **Application Links.** The Application Links feature allows you to link Confluence to applications like Atlassian's JIRA. Linking two applications allows you to share information and access one application's functions from within the other. For example, if you linked your Confluence server with a JIRA server, you could view JIRA issues in a Confluence page via the JIRA Issues Macro.

> *The information on this page does not apply to Confluence OnDemand.*

Getting Started

The Application Links quick start guide provides instructions on how to set up the most common application link configuration.

Administrator's Guide

The administrator's guide is for administrators who want to configure application links for their applications. The guide contains information on adding a new application link, configuring the authentication for an application link, setting up project links and more.

Developer Resources

These resources are for developers who want to develop with the Application Links plugin. Take a look at the Development Hub.

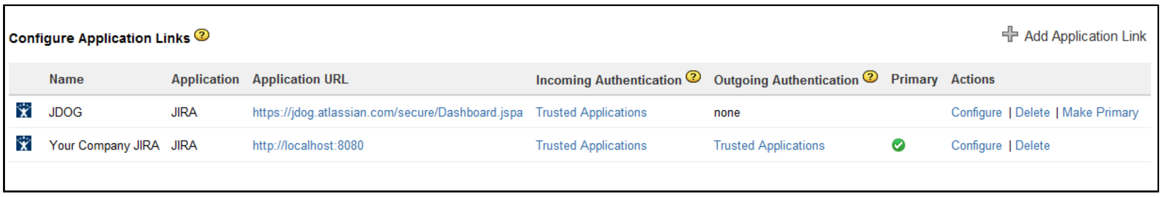
Related Topics

- Configuring Application Links
- Confluence and JIRA

Configuring Application Links

An application link is a trust relationship between two applications. Linking two applications allows you to share information and to access one application's functions from within the other.

> *The information on this page does not apply to Confluence OnDemand.*



Configure Application Links ?

	Name	Application	Application URL	Incoming Authentication ?	Outgoing Authentication ?	Primary	Actions
	JDOG	JIRA	https://jdog.atlassian.com/secure/Dashboard.jspa	Trusted Applications	none		Configure | Delete | Make Primary
	Your Company JIRA	JIRA	http://localhost:8080	Trusted Applications	Trusted Applications	✓	Configure | Delete

Screenshot above: Application links for a Confluence server

Notes

- In the above screenshot, the column titled '**Incoming Authentication**' is visible in Confluence 3.5.1 and later. The column does not appear in Confluence 3.5.

Related Topics

- Adding an Application Link
- Configuring Authentication for an Application Link
- Editing an Application Link
- Making an Application Link the Primary Link
- Relocating an Application Link

- Upgrading an Application Link
- Deleting an Application Link
- Configuring Project Links across Applications

Adding an Application Link

This page describes how to add a new application link in Confluence. The process for adding an application link is different depending on whether the application that you are linking Confluence to, supports Application Links (i.e. has Application Links installed) or not.

If you are linking Confluence to an application that does not have Application Links, you will need to do additional configuration in that application. This is because Application Links in Confluence will not be able to automatically configure authentication in your remote application.

Please read the appropriate set of instructions below:

- Linking to an application that supports Application Links.
- Linking to an application that does not support Application Links.

On this page:

⚠ *The information on this page does not apply to Confluence OnDemand.*

Adding an Application Link to an Application That Supports Application Links

Before you begin:

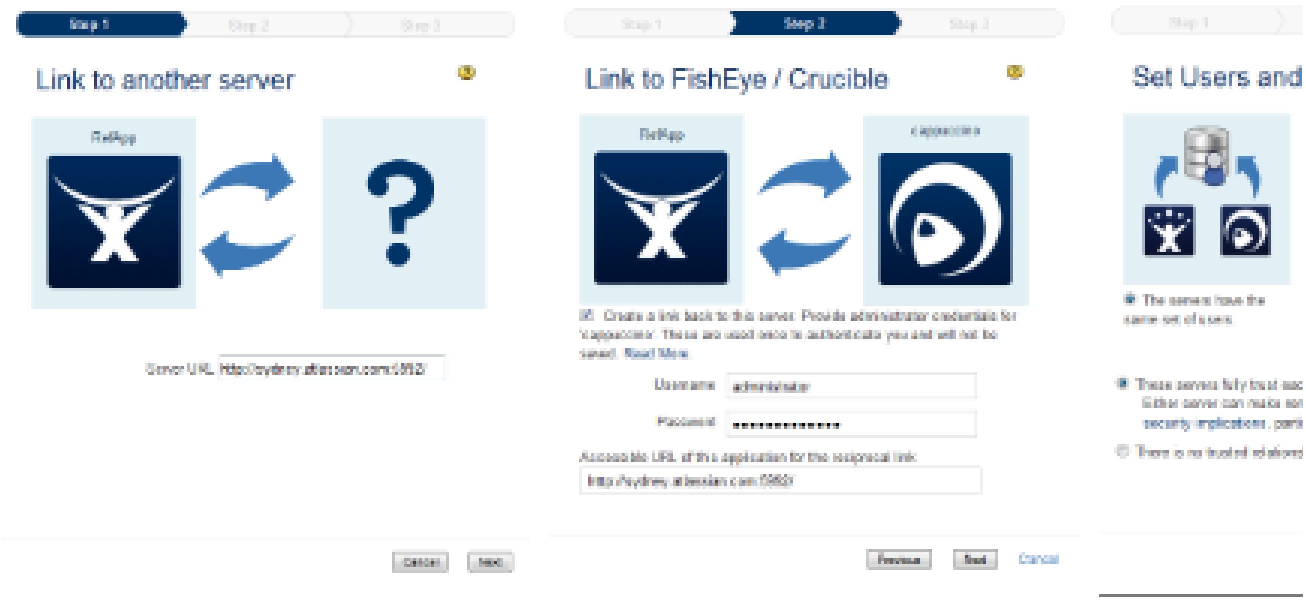
- Make sure that the base URL is set correctly in Confluence. See Configuring the Server Base URL for instructions.
- Make sure that the base URL is set correctly in the application which you intend to link to. See the appropriate instructions: JIRA instructions | FishEye/Crucible instructions | Bamboo instructions). This is required for synchronisation to work correctly.

To link to an application that supports Application Links:

1. Log in as a system administrator and go to the administration page. Click 'Application Links' in the administration menu. The 'Configure Application Links' page will appear, showing the application links that have been set up.
2. Click '**Add Application Link**'. Step 1 of the link wizard will appear.
3. Enter the **server URL** of the application that you want to link to (the 'remote application').
4. Click the '**Next**' button. Step 2 of the link wizard will appear.
5. Enter the following information:
   - '**Create a link back to this server**' – Tick this check box if you want to create a two-way link between the remote application and your application. If you want to do this, you will need to enter the username and password of an administrator for the remote application.
     Note: These credentials are only used to authenticate you to the remote applicaiton, so that Application Links can make the changes required for the new link. The credentials are not saved.
   - '**Reciprocal Link URL**' – The URL you give here will override the base URL specified in your remote application's administration console, for the purposes of the application links connection. Application Links will use this URL to access the remote application.
6. Click the '**Next**' button. Step 3 of the link wizard will appear.
7. Enter the information required to configure authentication for your application link:

- '**The servers have the same set of users**' or '**The servers have different sets of users**' – Select one of these options depending on how you manage users between the two applications.
- '**These servers fully trust each other**' – Tick this check box if you know that the code in both applications will behave itself at all times and are sure each application will maintain the security of its private key.
  For more information about configuring authentication, see Configuring Authentication for an Application Link.

8. Click the '**Create**' button to create the application link.



Step 1

Step 2

Screenshots above: Adding an application link to an application that supports Application Links (click to view full-sized images)

Adding an Application Link to an Application That Does Not Support Application Links

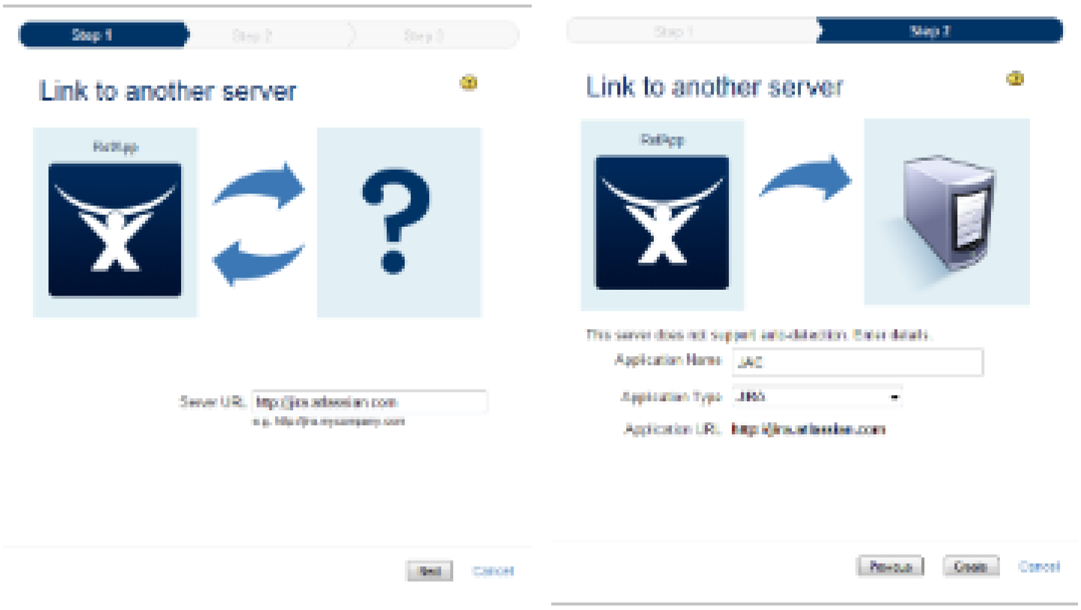
Before you begin:

- Make sure that the base URL is set correctly in Confluence. See Configuring the Server Base URL for instructions.
- Make sure that the base URL is set correctly in the application which you intend to link to. See the appropriate instructions: JIRA instructions | FishEye/Crucible instructions | Bamboo instructions). This is required for synchronisation to work correctly.

To link to an application that does not support Application Links:

1. Log in as a system administrator and go to the administration page. Click 'Application Links' in the administration menu. The 'Configure Application Links' page will appear, showing the application links that have been set up.
2. Click '**Add Application Link**'. Step 1 of the 'Link to another server' dialogue will be displayed.
3. Enter the server URL of the application that you want to link to, in the '**Server URL**' field. Click the '**Next**' button. Step 2 of the 'Link to another server' dialogue will be displayed.
4. Fill out the fields, as follows:
   - '**Application Name**' — Enter the name by which this remote application will be referred to, in your application.
   - '**Application Type**' — Select the type of application that you are linking to: Bamboo, FishEye/Crucible, JIRA, Confluence, Subversion.
   - '**Application URL**' — This will be set to the server URL you entered in the previous step and will not be editable.

5. Click the '**Create**' button to create the application link. The 'Configure Application Links' page will be displayed, listing all of the application links that have currently been set up for your application including the one you just added.
6. Configure the desired authentication type (Trusted Applications, OAuth, basic HTTP, none) for your new application link. See Configuring Authentication for an Application Link.
7. In your application that does not support Application Links, configure the same type of authentication that you configured for your application link's *outgoing* authentication (in the previous step). For example, if you configured outgoing Trusted Applications authentication in your Application-Links-enabled application, you also need log into your non-Application-Links application and manually configure Trusted Applications (see the relevant administrator's documentation for the application).



Server URL: http://jira.atlassian.com
e.g. http://jira.mycompany.com

This server does not support auto-detection. Enter details.
Application Name: JAC
Application Type: JIRA
Application URL: http://jira.atlassian.com

Step 1 Step 2

Screenshots above: Adding an application link to an application that supports Application Links (click to view full-sized images)

Notes

Related Topics

- Making an Application Link the Primary Link
- Configuring Authentication for an Application Link
- Configuring Project Links across Applications

Configuring Authentication for an Application Link

Configuring authentication for an application link is essentially defining the level of trust between Confluence and the application that it is linked to.

On this page:

⚠ *The information on this page does not apply to Confluence OnDemand.*

Choosing Authentication for an Application Link

The level of authentication that you should configure for your application link depends on a number of factors.

- **Do the two applications you are linking trust each other?** i.e. are you sure that the code in the application will behave itself at all times and that the application will maintain the security of its private key?
- **Do the two applications you are linking share the same user base or not?**
- **Do you have administrative access to the application you are linking to?**

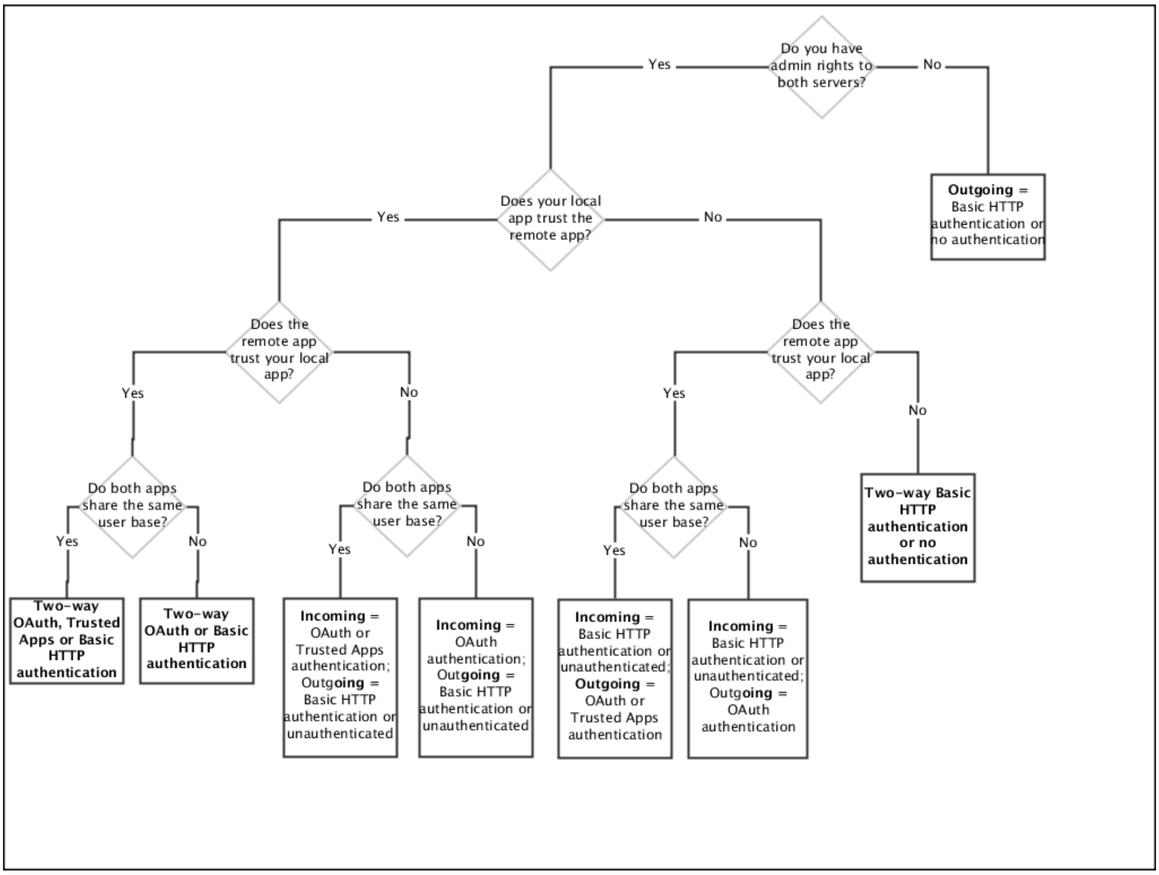
Common scenarios include:

- If the two applications you are linking **trust each other** and **share the same user base**, configure **two-way authentication using Trusted Applications** for both incoming and outgoing authentication. For example, you may link your internal Confluence server to an internal JIRA server.
- If the two applications you are linking **trust each other** but **do not share the same user base**, configure **two-way authentication using OAuth** for both incoming and outgoing authentication. For example, you may link your internal Confluence server to an external (customer-facing) JIRA server.
- If you **do not have administrative rights to the application that you are linking to** (e.g. linking to a public FishEye server), configure a **one-way outgoing link** authenticated using **basic HTTP authentication or do not configure any authentication** for the link. For example, you may link your external Confluence server to a partner organisation's Confluence server. An unauthenticated link will still allow the local application to render hyperlinks to the remote application or query anonymously-accessible APIs.

The flowchart below provides a guide to what authentication you should configure for your application link.

Read the following topics for information on how to configure authentication for an application link:

- Configuring Basic HTTP Authentication for an Application Link
- Configuring OAuth Authentication for an Application Link
- Configuring Trusted Applications Authentication for an Application Link
- Incoming and Outgoing Authentication


Do you have admin rights to both servers?
Yes
No
Outgoing = Basic HTTP authentication or no authentication
Does your local app trust the remote app?
Yes
No
Does the remote app trust your local app?
Yes
No
Does the remote app trust your local app?
Yes
No
Two-way Basic HTTP authentication or no authentication
Do both apps share the same user base?
Yes
No
Do both apps share the same user base?
Yes
No
Do both apps share the same user base?
Yes
No
Two-way OAuth, Trusted Apps or Basic HTTP authentication
Two-way OAuth or Basic HTTP authentication
Incoming = OAuth or Trusted Apps authentication; Outgoing = Basic HTTP authentication or unauthenticated
Incoming = OAuth authentication; Outgoing = Basic HTTP authentication or unauthenticated
Incoming = Basic HTTP authentication or unauthenticated; Outgoing = OAuth or Trusted Apps authentication
Incoming = Basic HTTP authentication or unauthenticated; Outgoing = OAuth authentication

Flowchart above: Determining what authentication to configure for an Application Link

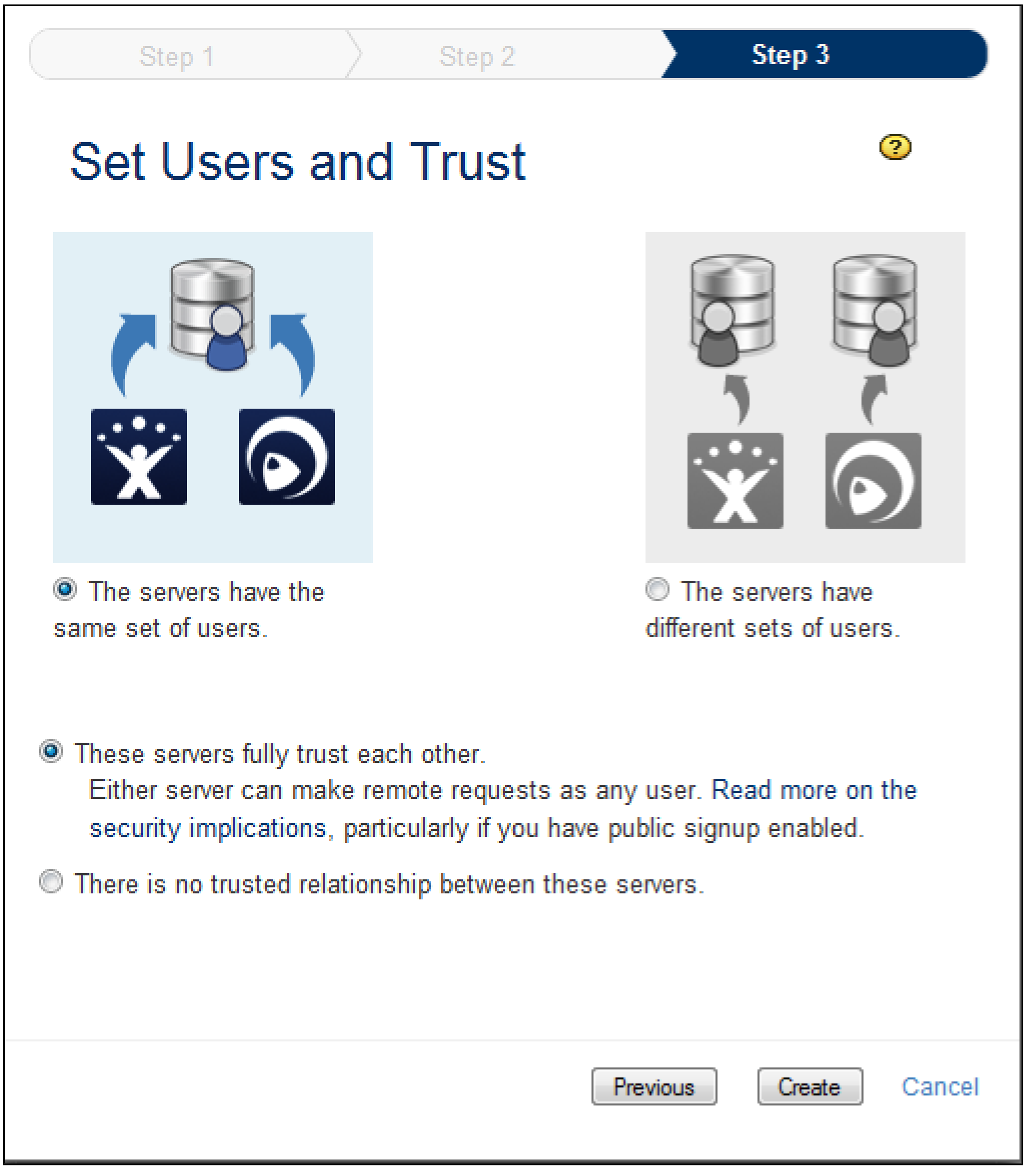
Security Implications for each Authentication Type

If you configure **Trusted Applications authentication** for your application (i.e. your servers have the same set of users and they fully trust each other), please be aware of the following security implications:

- Trusted applications are a **potential security risk**. When you configure Trusted Applications authentication, you are allowing one application to access another as any user. This allows all of the built-in security measures to be bypassed. Do not configure a trusted application unless you know that all code in the application you are trusting will behave itself at all times, and you are sure that the application will maintain the security of its private key.

If you configure **OAuth authentication** for your application (i.e. your servers have different sets of users and they fully trust each other), please be aware of the following security implications:

- Adding an OAuth consumer requires the transmission of sensitive data. To prevent 'man-in-the-middle' attacks, it is recommended that you **use SSL** for your applications while configuring OAuth authentication.
- Do not link to an application using OAuth authentication, unless you **trust all code in the application** to behave itself at all times. OAuth consumers are a potential security risk to the applications that they are linked to.



● The servers have the same set of users.

○ The servers have different sets of users.

● These servers fully trust each other.
Either server can make remote requests as any user. Read more on the security implications, particularly if you have public signup enabled.

○ There is no trusted relationship between these servers.

Screenshot above: Configuring authentication during application link setup

About Primary Authentication Types

You can configure multiple authentication types for each application link. When a feature makes a request using an Application Link, it will use one of the configured authentication types. If more than one authentication type is configured, it will by default use the authentication type that is marked as the primary authentication type. The default authentication type is indicated by the green tick ✓ next to the authentication type on the list application link screen.

You **cannot** configure which authentication type is the primary authentication type. The primary authentication type is determined automatically by Application Links and depends on a weight defined by each authentication type method. However, every feature that uses Application Links can also choose to use a specific authentication type and might not use the default primary authentication type.

About Impersonating and Non-Impersonating Authentication Types

Applications Links allows you to configure 'impersonating' and 'non-impersonating' authentication types:

- **Impersonating authentication types** make requests on behalf of the user who is currently logged in. People will see only the information that they have permission to see. This includes OAuth and Trusted Applications authentication.
- **Non-impersonating authentication types** always use a pre-configured user when making a request. Everyone logged into the system will see the same information. This includes basic HTTP authentication.

Configuring Basic HTTP Authentication for an Application Link

The instructions on this page describe how to configure **Basic HTTP authentication** for outgoing authentication and/or incoming authentication for an application link.

Basic HTTP authentication allows Confluence to provide user credentials to a remote application and vice versa. Once authenticated, one application can access specified functions on the other application on behalf of that user. For example, if you supply the credentials of a Confluence administrator on your Confluence server to a remote application, the remote application will be able to access all functions on your Confluence server that the Confluence administrator can access.

This method of authentication relies on the connection between Confluence and the remote application being secure. We recommend that you use Trusted Applications authentication or OAuth authentication for your application link instead, if possible.

On this page:

⚠ *The information on this page does not apply to Confluence OnDemand.*

Before You Begin

- The instructions assume that **both of the applications that you are linking have the Application Links plugin installed**. If the remote application that you are linking to supports Basic HTTP authentication, but does not have the Application Links plugin installed, you will need to configure Basic HTTP authentication from within the remote application (see the relevant administrator's documentation for the application). This is in addition to configuring the outgoing/incoming authentication for the application link (as described below).

- You must be a Confluence administrator to configure Basic HTTP authentication for an application link.

Configuring Basic HTTP Authentication for Outgoing Authentication

Configuring **outgoing basic http authentication** will allow Confluence to trust a remote application (i.e. allow the remote application to access specified functions in Confluence).

To configure basic http authentication for an outgoing application link:

1. Log in as a system administrator and go to the administration page. Click 'Application Links' in the administration menu. The 'Configure Application Links' page will appear, showing the application links that have been set up.
2. Click the '**Configure**' link next to the application link that you want to configure authentication for.
3. Click the '**Outgoing Authentication**' tab. The outgoing authentication page will be displayed.
4. Click the '**Basic Access**' tab.
5. Click the '**Configure**' button and enter the credentials (username and password) that the remote application will use to log into your application .
6. Click the '**Apply**' button to save your changes.

Configuring Basic HTTP Authentication for Incoming Authentication

Configuring **incoming basic http authentication** will allow the remote application that you are linking to, to trust Confluence (i.e. allow Confluence to access specified functions on the remote application it is linked to).

To configure basic http authentication for an incoming application link:

1. Log in as a system administrator and go to the administration page. Click 'Application Links' in the administration menu. The 'Configure Application Links' page will appear, showing the application links that have been set up.
2. Click the '**Configure**' link next to the application link that you want to configure authentication for.
3. Click the '**Incoming Authentication**' tab. The incoming authentication page will be displayed.
4. Click the '**Basic Access**' tab.
5. Click the '**Configure**' button and enter the credentials (username and password) that the your application will use to log in to the remote application.
6. Click the '**Apply**' button to save your changes.

Notes

Related Topics

Configuring OAuth Authentication for an Application Link
Configuring Trusted Applications Authentication for an Application Link

Configuring OAuth Authentication for an Application Link

The instructions on this page describe how to configure **OAuth** for outgoing authentication and/or incoming authentication for an application link.

OAuth is a protocol that allows a web application to share data/resources with any other OAuth-compliant external application. These external applications could be another web application (such as a JIRA installation or an iGoogle home page), a desktop application or a mobile device application, provided that they are accessible from within your network or available on the Internet.

For example, you could set up an application link between Confluence and an iGoogle page using OAuth authentication. This would allow you to view data from your Confluence server in a Confluence gadget on the iGoogle page (see Configuring Confluence Gadgets for Use in Other Applications).

A typical scenario is setting up an application link between two applications which trust each other, do not share the same set of users but both applications have the Application Links plugin installed. In this case, you would configure OAuth for both outgoing authentication and incoming authentication. See Configuring Authentication for an Application Link for other configurations.

Key OAuth Terminology

- **Service provider** — An application that shares ('provides') its resources.
- **Consumer** — An application that accesses ('consumes') a service provider's resources.
- **User** — An individual who has an account with the Service Provider.

For more information about OAuth, see Configuring OAuth as well as the OAuth specification .

On this page:

⚠ *The information on this page does not apply to Confluence OnDemand.*

Before You Begin

- Adding an OAuth consumer requires the transmission of sensitive data. To prevent 'man-in-the-middle' attacks, it is recommended that you **use SSL** for your applications while configuring OAuth authentication.
- Do not link to an application using OAuth authentication, unless you **trust all code in the application** to behave itself at all times. OAuth consumers are a potential security risk to the applications that they are linked to.
- The instructions assume that **both of the applications that you are linking have the Application Links plugin installed**. If the remote application that you are linking to supports OAuth, but does not have the Application Links plugin installed, you will need to configure OAuth from within the remote application (see the relevant administrator's documentation for the application) in addition to configuring the outgoing/incoming authentication for the application link (as described below).
- You must be a Confluence administrator to configure OAuth authentication for an application link.

Configuring OAuth for Outgoing Authentication

Configuring **outgoing OAuth authentication** will allow Confluence to access data in a remote application on behalf of a user (i.e. allow Confluence to access specified functions in the remote application).

To configure OAuth authentication for an outgoing application link:

1. Log in as a system administrator and go to the administration page. Click 'Application Links' in the administration menu. The 'Configure Application Links' page will appear, showing the application links that have been set up.
2. Click the '**Configure**' link next to the application link that you want to configure OAuth for.
3. Click the '**Outgoing Authentication**' tab. The outgoing authentication page will be displayed.
4. Click the '**OAuth**' tab.
5. If you are not currently logged in to the remote application (or you logged in to the remote application under a variant of the application's hostname, such as the IP address), a login dialogue will display.
   - Enter the '**Username**' and '**Password**' for the remote server, not your local server, and click the '**Login**' button. The remote server needs to learn the identity of your local server for the OAuth protocol to work and your admin credentials are used to store your local server's public key on the

remote server. If you are already logged into your remote server, then the appropriate changes can be made without having to log in again.

6. Click the '**Enable**' button to enable OAuth authentication for the outgoing link. Your application will be automatically set up to be the 'consumer' and the remote application as a 'service provider'.

Configuring OAuth for Incoming Authentication

Configuring **incoming OAuth authentication** will allow the remote application that you are linking to, to access data in Confluence.

To configure OAuth authentication for an incoming application link:

1. Log in as a system administrator and go to the administration page. Click 'Application Links' in the administration menu. The 'Configure Application Links' page will appear, showing the application links that have been set up.
2. Click the '**Configure**' link next to the application link that you want to configure OAuth for.
3. Click the '**Incoming Authentication**' tab. The incoming authentication page will be displayed.
4. Click the '**OAuth**' tab.
5. Click the '**Enable**' button to enable OAuth authentication for the incoming link. The remote application will be automatically set up to be the 'consumer' and your local application as a 'service provider'.

Related Topics

Configuring Basic HTTP Authentication for an Application Link
Configuring Trusted Applications Authentication for an Application Link
Configuring Confluence Gadgets for Use in Other Applications

Configuring Trusted Applications Authentication for an Application Link

The instructions on this page describe how to configure **Trusted Applications** for outgoing authentication and/or incoming authentication for an application link.

Trusted Applications authentication allows one application to allow access to specified functions on another application on behalf of any user, without the user having to log into the second application. For example, if you configure a JIRA server to trust a Confluence server, every Confluence user will see exactly the same list of issues when they view the Confluence 'JIRA Issues' macro as they see when they use the JIRA Issue Navigator as a logged-in JIRA user.

A typical scenario is setting up an application link between two applications which trust each other, have the same set of users and both have the application links plugin installed. In this case, you would configure Trusted Applications for both outgoing authentication and incoming authentication. See Configuring Authentication for an Application Link for other configurations.

On this page:

⚠ *The information on this page does not apply to Confluence OnDemand.*

Before You Begin

- Trusted applications are a **potential security risk**. When you configure Trusted Applications authentication, you are allowing one application to access another as any user. This allows all of the built-in security measures to be bypassed. Do not configure a trusted application unless you know that all code in the application you are trusting will behave itself at all times, and you are sure that the application will maintain the security of its private key.

- The instructions below assume that **both of the applications that you are linking have the Application Links plugin installed**. If the remote application that you are linking to supports Trusted Applications, but does not have the Application Links plugin installed, you will need to configure Trusted Applications from within the remote application (see the relevant administrator's documentation for the application) in addition to configuring the outgoing/incoming authentication for the application link (as described below).
- You must be a Confluence administrator to configure Trusted Applications authentication for an application link.

Configuring Trusted Applications for Outgoing Authentication

Configuring **outgoing Trusted Applications authentication** will allow the remote application to trust Confluence (i.e. allow Confluence to access specified functions and data on the remote application).

To configure Trusted Applications authentication for an outgoing application link:

1. Log in as a system administrator and go to the administration page. Click 'Application Links' in the administration menu. The 'Configure Application Links' page will appear, showing the application links that have been set up.
2. Click the '**Configure**' link next to the application link that you want to configure Trusted Applications authentication for.
3. Click the '**Outgoing Authentication**' tab. The outgoing authentication page will show, with the '**Trusted Applications**' tab displayed.
4. If you are not currently logged into the remote application (or you logged into the remote application under a variant of the application's hostname, e.g. the IP address), a login dialogue will display.
   - Enter the '**Username**' and '**Password**' for the remote server, (not your local server), and click the '**Login**' button. You need to enter the credentials for the remote server, as the remote server needs to be instructed to trust your local server for the Trusted Applications protocol to work. If you are already logged into your remote server, then the appropriate changes can be made without having to log in again.
5. Configure the settings for the Trusted Applications authentication:
   - '**IP Patterns**' — Enter the IP addresses (IPv4 only) from which the remote application will accept requests (this effectively is the IP address your local server). You can specify wildcard matches by using an asterisk (*), e.g. '`192.111.*.*`' (note, you cannot use netmasks to specify network ranges). If you are entering multiple IP addresses, separate them with commas or spaces.
     ⚠ *Please note, if you are setting up Trusted Applications between two applications that both have the Application Links plugin installed, you can leave this field blank (or explicitly use `*.*.*.*`). However, if your remote application does not have the Application Links plugin installed and you are configuring the IP Patterns in the remote application (not the Application Links plugin),* ***you must not leave this field blank nor use `*.*.*.*`****. Failure to configure IP address restrictions in this scenario is a security vulnerability, allowing an unknown site to log into your site under a user's login ID.*
     Consider the following scenarios, if you want to limit access by using this field:
     - If your local application is using a proxy server, you need to add the proxy server's IP address to this field.
     - If your local application is a clustered instance of Confluence, you need to configure the remote server to accept requests from each cluster node. If you do not set up each node appropriately, your Confluence users may not be able to view any information from the remote server. You can set this up by either specifying each individual IP address for each node of the cluster (e.g. `172.16.0.10, 172.16.0.11, 172.16.0.12`), or specifying the IP address for the clustered Confluence instance using wildcards (e.g. `172.16.0.*`).
   - **'URL Patterns'** — Enter the URLs in the remote application that your local application will be allowed to access. Each URL corresponds to a particular application function. Enter one URL per line, as follows:

        - If your remote application is JIRA, enter the following URL Patterns: `/plugins/servlet/streams`, `/sr/jira.issueviews:searchrequest`, `/secure/RunPortlet`, `/rest`, `/rpc/soap`
        - If your remote application is Confluence, enter the following URL Patterns: `/plugins/servlet/streams`, `/plugins/servlet/applinks/whoami`
    - '**Certificate Timeout (ms)**' — Enter the certificate timeout. The default is 10 seconds. The certificate timeout is used to prevent replay attacks. For example, if a Trusted Applications request is intercepted and (maliciously) re-sent, the application will be able to check when the request was first sent. If the second request is sent more than 10 seconds (or whatever the certificate timeout is set to) after the initial request, it will be rejected. Please note, you should not have to change the default value of this field for most application links. Note that the certificate timeout relies on the clocks on both servers being synchronised.
6. Click the '**Apply**' button to save your changes.

Configuring Trusted Applications for Incoming Authentication

Configuring **incoming Trusted Applications authentication** will allow Confluence to trust the remote application that you are linking it to (i.e. allow your 'trusted' remote application to access specified functions and data on Confluence).

To configure Trusted Applications authentication for an incoming application link:

1. Log in as a system administrator and go to the administration page. Click 'Application Links' in the administration menu. The 'Configure Application Links' page will appear, showing the application links that have been set up.
2. Click the '**Configure**' link next to the application link that you want to configure Trusted Applications authentication for.
3. Click the '**Incoming Authentication**' tab. The imconing authentication page will show, with the '**Trusted Applications**' tab displayed.
4. The tab will show whether Trusted Applications is currently enabled or not. Use the '**Modify**' or '**Configure**' button to configure Trusted Applications. The Trusted Applications configuration settings will be displayed:
    - '**IP Patterns**' — Enter the IP addresses (IPv4 only) from which our application will accept requests. You can specify wildcard matches by using an asterisk (*), e.g. '`192.111.*.*`' (note, you cannot use netmasks to specify network ranges). If you are entering multiple IP addresses, separate them with commas or spaces.
      ⚠ *Please note, if you are setting up Trusted Applications between two applications that both have the Application Links plugin installed, you can leave this field blank (or explicitly use `*.*.*.*`). However, if your remote application does not have the Application Links plugin installed and you are configuring the IP Patterns in the remote application (not the Application Links plugin),* ***you must not leave this field blank nor use `*.*.*.*`****. Failure to configure IP address restrictions in this scenario is a security vulnerability, allowing an unknown site to log into your site under a user's login ID.*
      Consider the following scenarios, if you want to limit access by using this field:
        - If the remote application is using a proxy server, you need to add the proxy server's IP address to this field.
        - If the remote application is a clustered instance of Confluence, you need to accept requests from each cluster node. If you do not specify each node's address, Confluence users may not be able to view any data from your application. You can set this up by either specifying each individual IP address for each node of the cluster (e.g. 172.16.0.10, 172.16.0.11, 172.16.0.12), or specifying the IP address for your clustered Confluence instance using wildcards (e.g. 172.16.0.*).
    - **'URL Patterns'** — Enter the local URLs that the remote application will be allowed to access. Each URL corresponds to a particular application function. Enter one URL per line, as follows:
        - If your local application is JIRA, enter the following URL Patterns — `/plugins/servlet/streams`, `/sr/jira.issueviews:searchrequest`, `/secure/RunPortlet`, `/rest`, `/`

        `rpc/soap`
        - If your local application is Confluence, enter the following URL Patterns — `/plugins/servlet/streams`, `/plugins/servlet/applinks/whoami`
    - '**Certificate Timeout (ms)**' — Enter the certificate timeout. The default is 10 seconds. The certificate timeout is used to prevent replay attacks. For example, if a Trusted Applications request is intercepted and (maliciously) re-sent, the application will be able to check when the request was first sent. If the second request is sent more than 10 seconds (or whatever the certificate timeout is set to) after the initial request, it will be rejected. Please note, you should not have to change the default value of this field for most application links. Note that the certificate timeout relies on the clocks on both servers being synchronised.
5. Click the '**Apply**' button to save your changes.

Notes

Related Topics

Configuring Basic HTTP Authentication for an Application Link
Configuring OAuth Authentication for an Application Link

Incoming and Outgoing Authentication

When you configure authentication for an application link, you are defining the level of trust between the two linked servers. When configuring a link from one application to another, you can set up:

- **Incoming authentication** (authentication of requests coming from a linked application into this application).
- **Outgoing authentication** (authentication of requests sent from this application to a linked application).

See Configuring Authentication for an Application Link.

⚠ *The information on this page does not apply to Confluence OnDemand.*

Editing an Application Link

You can change the details, such as the application name and display URL, for an existing application link.

On this page:

- Editing an Application Link
- Notes

⚠ *The information on this page does not apply to Confluence OnDemand.*

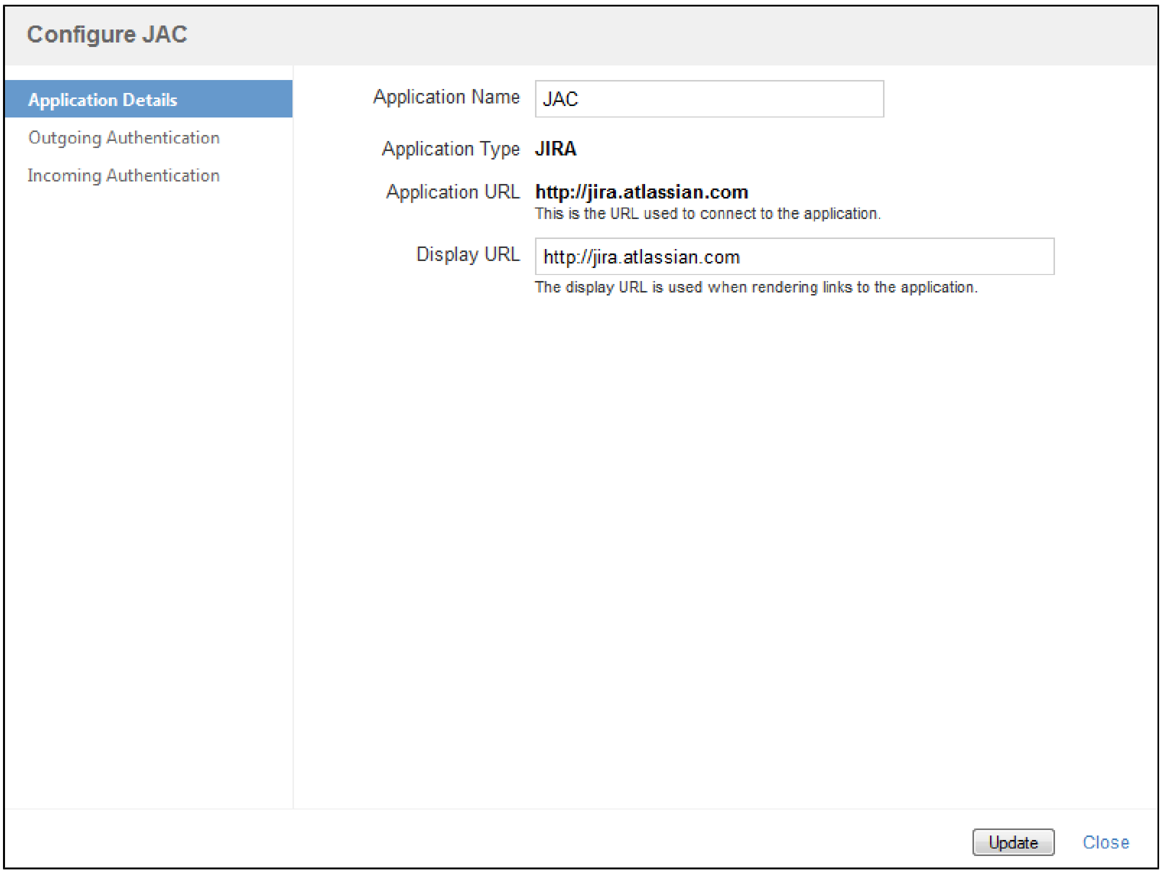
Editing an Application Link

To edit an application link:

1. Log in as a system administrator and go to the administration page. Click 'Application Links' in the administration menu. The 'Configure Application Links' page will appear, showing the application links that have been set up.
2. Click the '**Configure**' link next to the application link that you want to edit the details for. The application details for the application link will be displayed.
3. Update the application details as desired. Please note, you cannot update the Application Type nor the Application URL.
    - '**Application Name**' — Update this field to change the display name for the application that you are linking to.

- '**Display URL**' — This URL is used when displaying links to the application in the browser. When creating the application link, you may have used a URL that is not accessible to other users, such as an internal IP address. If so, you can change the display URL to an address in a domain that is accessible to other users.

4. Click the '**Update**' button to save your changes.



Configure JAC

Application Name: JAC

Application Type: JIRA

Application URL: http://jira.atlassian.com
This is the URL used to connect to the application.

Display URL: http://jira.atlassian.com
The display URL is used when rendering links to the application.

Screenshot above: Editing an application link

Notes

Related Topics

Configuring Authentication for an Application Link
Making an Application Link the Primary Link
Relocating an Application Link

Making an Application Link the Primary Link

If you have set up application links to more than one of the same application type, e.g. you have linked your application to two JIRA servers, then one of the servers will be marked as the 'Primary' link. This means that any outgoing requests will be directed to the primary link's application.

For example, if you have set up a Confluence server that is linked to two JIRA servers with two-way authentication for both links, you can nominate an application link to one of the JIRA servers as the primary link. Every time Confluence requests JIRA information (e.g. for a JIRA issues macro), it will request it from the primary link's JIRA server. Note, both JIRA servers can still make requests of the Confluence server (e.g. a Confluence page gadget on the dashboards of each JIRA instance).

On this page:

The information on this page does not apply to Confluence OnDemand.

Making an Application Link the Primary Link

To make an application link the primary link:

1. Log in as a system administrator and go to the administration page. Click 'Application Links' in the administration menu. The 'Configure Application Links' page will appear, showing the application links that have been set up.
2. Click the '**Make Primary**' link next to the application link that you want to make the primary link. A '✅' symbol will display in the 'Primary' column next to the application link.
   The 'Primary' column and 'Make Primary' link will only display if you have set up application links to more than one of the same application type, e.g. you have linked your application to two JIRA servers.

Notes

Please read Making a Project Link the Primary Link for information on how primary project links also influence the information shared between servers.

Related Topics

Making a Project Link the Primary Link

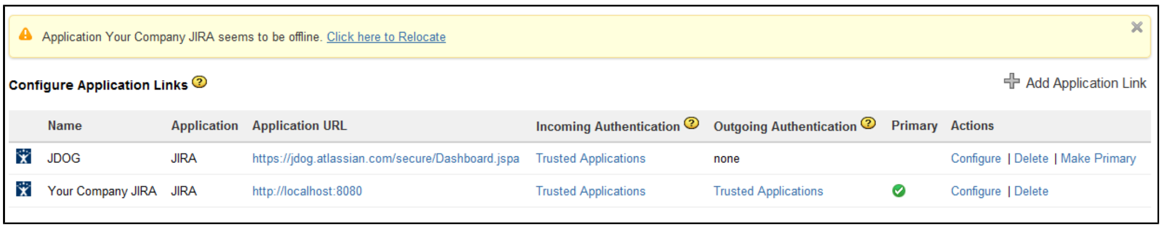
Relocating an Application Link

This page describes how to change the location of an application link. You will need to relocate an application link if the target application has been moved to a new address.

The information on this page does not apply to Confluence OnDemand.

To relocate an application link:

1. Log in as a system administrator and go to the administration page. Click 'Application Links' in the administration menu. The 'Configure Application Links' page will appear, showing the application links that have been set up.
2. If the remote application for an application link cannot be reached by your application, the '**List Application Links**' page will display a warning message (see 'Relocate Link - Warning Message' screenshot below).
3. If your remote application has been moved to a different address (rather than just being offline temporarily), click the '**Relocate**' link in the warning message (see 'Relocate Link - Updating URL' screenshot below).
4. Enter the new URL for the remote application of your application link and click '**Relocate**'.
5. You will need to confirm the relocation, if the new URL cannot be contacted. Otherwise, the application link will be updated.



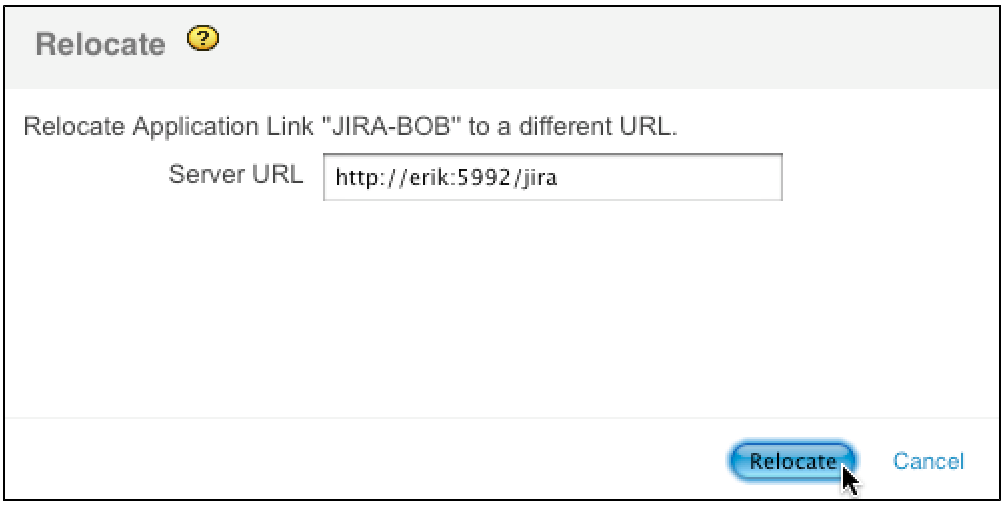
Application Your Company JIRA seems to be offline. Click here to Relocate

Configure Application Links

Add Application Link

Name	Application	Application URL	Incoming Authentication	Outgoing Authentication	Primary	Actions
JDOG	JIRA	https://jdog.atlassian.com/secure/Dashboard.jspa	Trusted Applications	none		Configure | Delete | Make Primary
Your Company JIRA	JIRA	http://localhost:8080	Trusted Applications	Trusted Applications	✓	Configure | Delete

Screenshot above: Relocate link – The warning message



Relocate Application Link "JIRA-BOB" to a different URL.

Server URL: http://erik:5992/jira

Screenshot above: Relocate link – Updating the URL

Related Topics

Making an Application Link the Primary Link

Upgrading an Application Link

The instructions on this page describe how to upgrade an existing application link. You may want to upgrade an application link in either of the two situations below:

- Your Confluence instance has been upgraded from a version that does not include Application Links to a version that does. For example, you may have configured Trusted Applications or OAuth in a Confluence 3.4 instance (does not include Application Links) and then upgraded to Confluence 3.5 (includes Application Links).
- Your remote application has been upgraded to a version that includes Application Links. For example, you had set up an application link in a Confluence 3.5 instance (includes Application Links) to JIRA 4.2 instance (does not include Application Links), and then upgrade to JIRA 4.3 (includes Application Links).

On this page:

⚠ *The information on this page does not apply to Confluence OnDemand.*

Upgrading an Application Link (Local App Upgraded to Include Application Links)

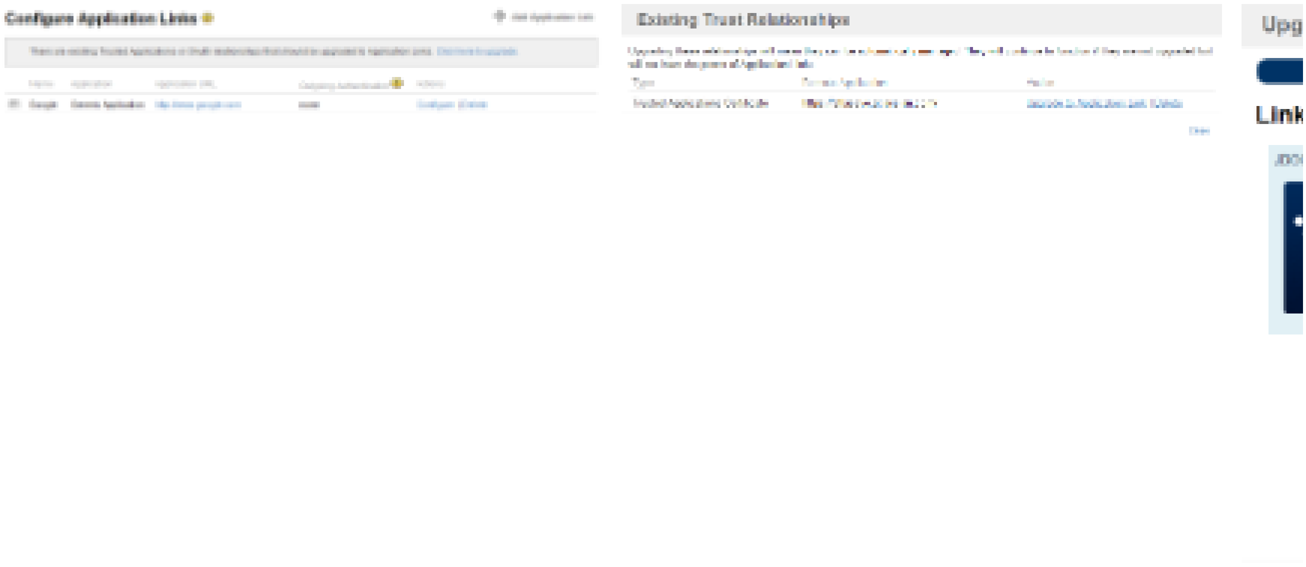
When you upgrade from a Confluence version that does not include Application Links to version that does, you will have the option of converting any Trusted Applications or OAuth links to Application Links. The advantage of converting your links to Application Links is that link configuration will be simplified in future.

To upgrade an application link when your local application has been upgraded to include Application Links:

1. After your application upgrade, navigate to the administration console.
2. Click '**Application Links**'. The 'Configure Application Links' screen will be displayed with the following message:
   *"There are existing Trusted Applications or OAuth relationships that should be upgraded to Application Links. **Click here to upgrade.**"*
3. Click the '**Click here to upgrade**' link. The 'Existing Trust Relationships' screen will be displayed showing

all Trusted Applications and OAuth relationships that can be upgraded to Application Links.

4. Click the '**Upgrade to Application Link**' link next to the desired trust relationship. The 'Upgrade to Application Link' wizard will be displayed.
5. Complete the wizard. The process will be similar to adding a new link (described on Adding an Application Link), except that most fields should be pre-filled.



Step 1 Step 2

Screenshots above: Upgrading an application link for local application

Upgrading an Application Link (Remote App Upgraded to Include Application Links)

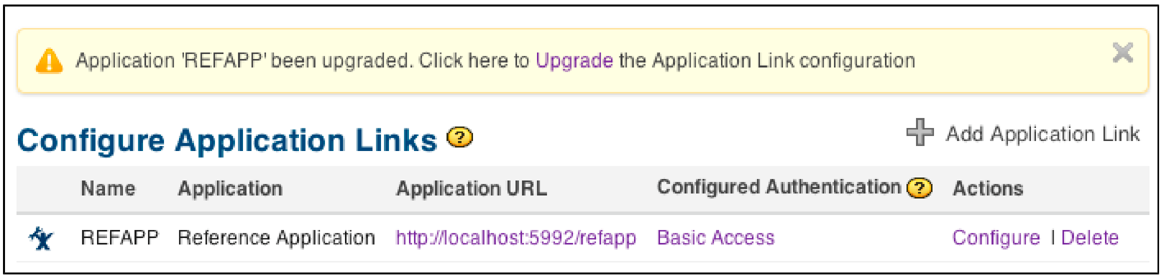
When an application link is created between a version of Confluence that supports Application Links, and a remote legacy application (either a non-Atlassian product, or an older version of an Atlassian product that did not ship with Application Links), this link is configured to run in "legacy mode". While there is no distinguishable difference to a user, connection and configuration without Application Links is a little different. For example:

- Setting up OAuth requires manual configuration by the administrator. In OAuth authentication for between applications that support Application Links, exchange of the consumer keys and public keys is done automatically.
- The Trusted Applications protocol (Atlassian-specific) will not be available for authentication.

If you upgrade your remote application to a version that does include Application Links, the application link will continue to work. However, upgrading your link may simplify link configuration and make additional authentication protocols available (as mentioned above).

To upgrade an application link when your remote application has been upgraded to include Application Links:

1. After you have upgraded your remote application to a version that includes Application Links, go to the administration console of your local application. A warning will be displayed, requesting that you upgrade the link to full Application Links mode.
2. Click '**Upgrade**' in the warning message to start the upgrade wizard. Note the following:
   - You will be prompted to make your application link a reciprocal link. You will need to provide administrator credentials for your remote application, if you choose to do so.
   - If you make your application link a reciprocal link, you will also be able to make reciprocal links for your project links. For example, you may be able to link your JIRA project to a FishEye repository and also make a link from your FishEye repository back to the JIRA project.

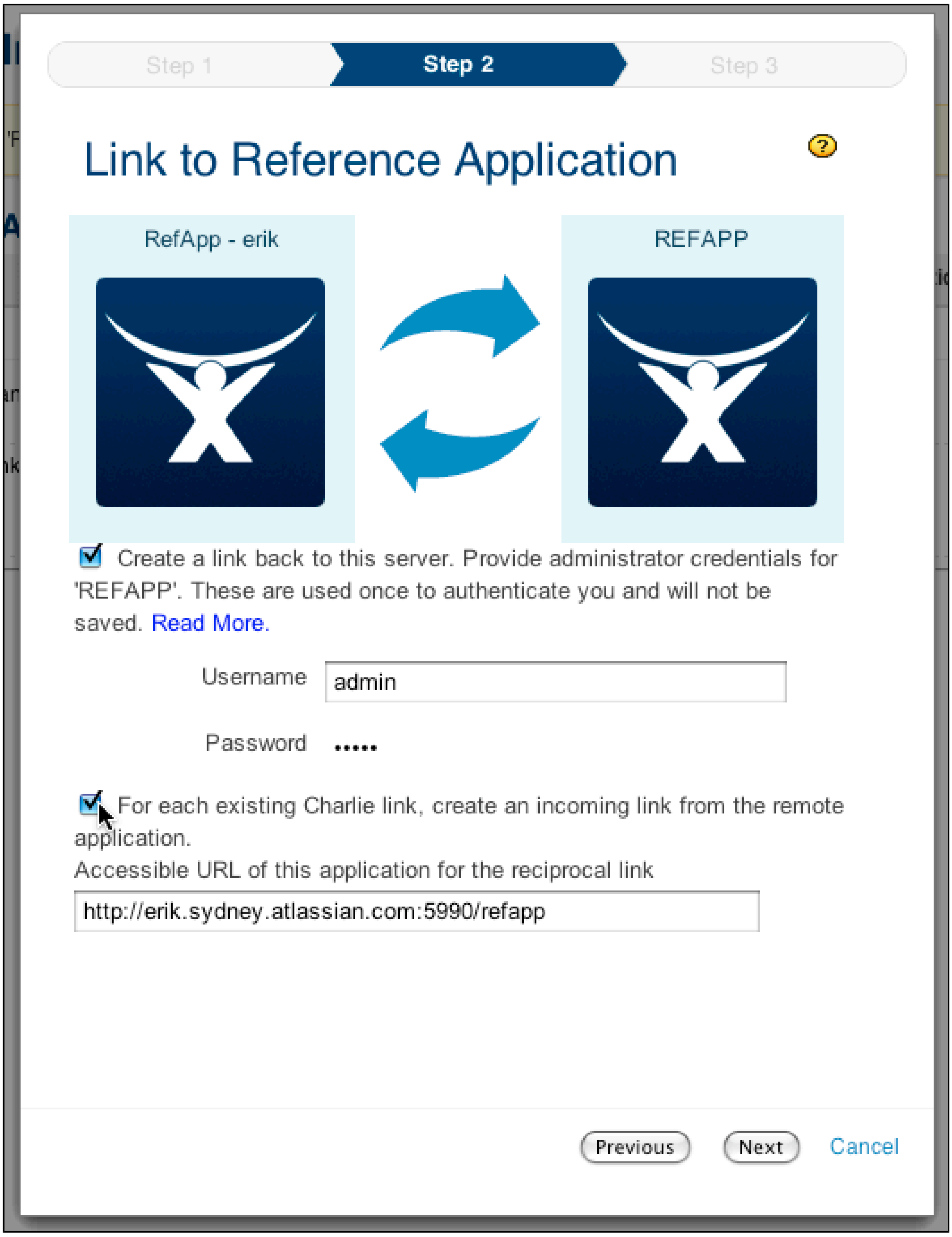


Application 'REFAPP' been upgraded. Click here to Upgrade the Application Link configuration

Configure Application Links

Name	Application	Application URL	Configured Authentication	Actions
REFAPP	Reference Application	http://localhost:5992/refapp	Basic Access	Configure | Delete

Screenshot above: Upgrading an application link for remote application



Link to Reference Application

☑ Create a link back to this server. Provide administrator credentials for 'REFAPP'. These are used once to authenticate you and will not be saved. Read More.

Username: admin

Password: •••••

☑ For each existing Charlie link, create an incoming link from the remote application.

Accessible URL of this application for the reciprocal link

http://erik.sydney.atlassian.com:5990/refapp

Screenshot above: Upgrading an application link wizard

Notes

Related Topics

[Adding an Application Link]

Configuring Authentication for an Application Link

Deleting an Application Link

Deleting an application link stops the two applications from sharing information. You will no longer be able to make requests from one application to the other. This means that certain features may not work, e.g. JIRA issues macro in Confluence, Confluence Page Gadget in JIRA, etc.

If you have set up application links to multiple servers of the same application type, e.g. you have linked your application to multiple JIRA servers, deleting the primary link will mean that another of the links will be made the primary link.

Deleting an application link will also delete all project links set up for that application link.

> ⚠ *The information on this page does not apply to Confluence OnDemand.*

To delete an application link:

1. Log in as a system administrator and go to the administration page. Click 'Application Links' in the administration menu. The 'Configure Application Links' page will appear, showing the application links that have been set up.
2. Click the '**Delete**' link next to the application link that you want to delete. A confirmation screen will be displayed.
3. Click the '**Confirm**' button to delete the application link.

RELATED TOPICS

Editing an Application Link
Relocating an Application Link

Configuring Project Links across Applications

Let's assume that you are managing a project or team. You would like to connect your project's Confluence space with your JIRA project, and link up your team's source repository too.
When you have connected your applications via Application Links, you can also connect the areas of those applications that contain information relating to your project or team. Using **project links** (also called **entity links**) you can associate one or more projects, spaces and repositories across the linked applications.

To connect all the information relating to the project or team that you are managing, you can link one or more of the following:

- JIRA projects.
- Confluence spaces.
- FishEye repositories.
- FishEye projects. A FishEye 'project' is the Crucible project if you have installed FishEye and Crucible, otherwise it is the paths associated via the 'FishEye Project Content' function in FishEye.
- Crucible projects.
- Bamboo projects.

On this page:

> ⚠ *The information on this page does not apply to Confluence OnDemand.*

Uses for Project Links

The following integration features use project links:

- Activity streams. For example, the project links determine the activity retrieved from JIRA to display in the activity stream of a FishEye repository or a Crucible project.
- The JIRA FishEye plugin. For example:
  - The link between a JIRA project and a FishEye repository determines the repository searched for a particular issue key when displaying the FishEye source tab in JIRA.
  - The link between a JIRA project and a Crucible project determines the Crucible project scanned for review activity when displaying the Crucible reviews tab in JIRA.
  - When you create a defect in Crucible, Crucible will know which JIRA project to put it in.
- Third-party plugins may make use of project links to enrich their functionality too.

Managing Project Links

- Adding Project Links between Applications
- Making a Project Link the Primary Link
- Deleting a Project Link

RELATED TOPICS

Adding an Application Link

Adding Project Links between Applications

Let's assume that you are managing a project or team. You would like to connect your project's Confluence space with your JIRA project, and link up your team's source repository too.
When you have connected your applications via Application Links, you can also connect the areas of those applications that contain information relating to your project or team. Using **project links** (also called **entity links**) you can associate one or more projects, spaces and repositories across the linked applications.

To connect all the information relating to the project or team that you are managing, you can link one or more of the following:

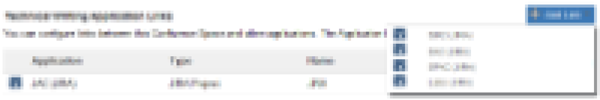
- JIRA projects.
- Confluence spaces.
- FishEye repositories.
- FishEye projects. A FishEye 'project' is the Crucible project if you have installed FishEye and Crucible, otherwise it is the paths associated via the 'FishEye Project Content' function in FishEye.
- Crucible projects.
- Bamboo projects.

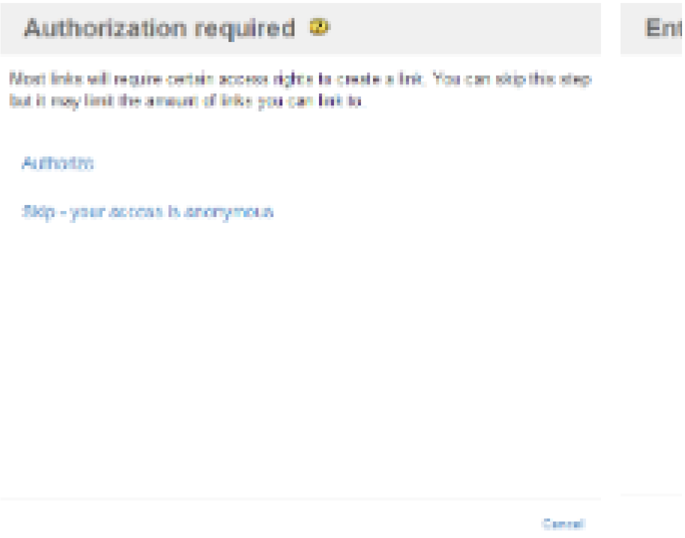
> ⚠ *The information on this page does not apply to Confluence OnDemand.*

To link a Confluence space to a project in another application:

1. Choose **Browse** > **Space Admin**.
   ℹ **Space Admin** is displayed only if you are a space administrator for that space or you are a Confluence system administrator.
2. Click '**Application Links**' in the left-hand panel.
3. Choose the Confluence space that you want to link from.
4. The instructions for adding a project link will vary depending on whether the target application has the Application Links functionality installed:
   - If the target application has Application Links:
     a. Click '**Add Link**'. A dropdown menu will appear listing the applications you have already linked to.

   b. In the dropdown menu, click the application that contains the project you want to link to. For example, if you want to link to a specific JIRA project, click the JIRA site that contains that project. If you want to link to a Confluence space, click the Confluence site that contains that space.
   c. Click one of the options on the 'Authorization required' screen:
      - '**Authorize**' — Click this option if you want to grant your project authorised access to the target project. The target application will open in a new window, so that you can log in and authorise access.
      - '**Skip – your access is anonymous**' — Click this option if you only want to allow anonymous access to the target project.
   d. In the '**Name or Key**' field, enter the name/key of the project in the remote application that you want to link to. For example, if you want to link to a JIRA project, enter the project key. If you want to link to a Confluence space, enter the space key.
   e. Click the '**Create**' button to create the project link.
- If the target application does not have Application Links:
   a. Click '**Add Link**'. A dropdown menu will display listing the applications you have already linked to.
   b. In the dropdown menu, click the application that contains the project you want to link to. For example, if you want to link to a specific JIRA project, click the JIRA site that contains that project. If you want to link to a Confluence space, click the Confluence site that contains that space.
   c. In the '**Key**' field, enter the name/key of the project in the remote application that you want to link to. For example, if you want to link to a JIRA project, enter the project key. If you want to link to a Confluence space, enter the space key.
   d. *(optional)* Enter the alias for the project in the '**Alias**' field. This is the display name for the project in your administration console.
   e. Click the '**Create**' button to create the project link.





Authorization required

Most links will require certain access rights to create a link. You can skip this step but it may limit the amount of links you can link to

Step 1 Step 2

Screenshots above: Linking to a JIRA project (where the target JIRA server supports Application Links)

RELATED TOPICS

[Making a Project Link the Primary Link](#)
[Deleting a Project Link](#)

Making a Project Link the Primary Link

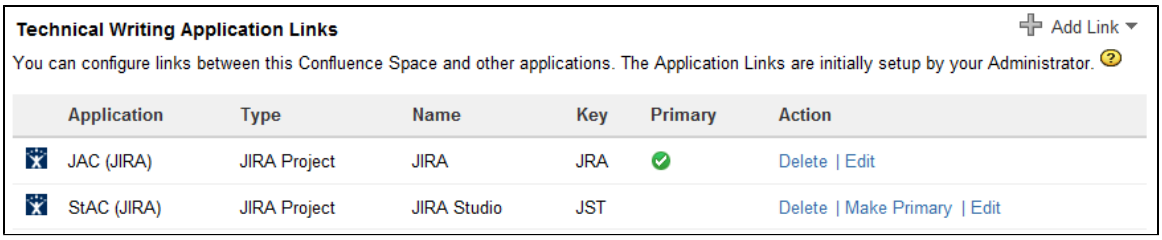
If you have set up project links to more than one project in the same application, for example you have linked your Confluence space to two JIRA projects, then one of the project links will be marked as the primary link. All outgoing requests will be directed to the primary link.

For example, if you have a Confluence space that is linked to two JIRA projects, you can nominate the link to one of the JIRA projects as the primary link. Every time Confluence requests JIRA information (for example, in a JIRA issues macro) it will request it from the primary link's JIRA project. Note, both JIRA projects can still request information from the Confluence space (for example, a Confluence page gadget on the dashboards of each JIRA instance).

> *The information on this page does not apply to Confluence OnDemand.*

To make a project link the primary link:

1. Choose **Browse** > **Space Admin**.
   Space Admin is displayed only if you are a space administrator for that space or you are a Confluence system administrator.
2. Click '**Application Links**' in the left-hand panel.
3. Click the '**Make Primary**' link in the '**Action**' column for the project link that you want to make the primary link. A ✓ symbol will display in the 'Primary' column next to the link.
   Note: The 'Primary' column and 'Make Primary' link will appear only if you have set up multiple project links to the same application, for example you have linked a Confluence space to a number of JIRA projects.



Technical Writing Application Links

You can configure links between this Confluence Space and other applications. The Application Links are initially setup by your Administrator.

Application	Type	Name	Key	Primary	Action
JAC (JIRA)	JIRA Project	JIRA	JRA	✓	Delete | Edit
StAC (JIRA)	JIRA Project	JIRA Studio	JST		Delete | Make Primary | Edit

Screenshot above: Viewing the project links for a Confluence space

RELATED TOPICS

Adding Project Links between Applications
Deleting a Project Link

Deleting a Project Link

Deleting a project link stops the two projects from sharing information.

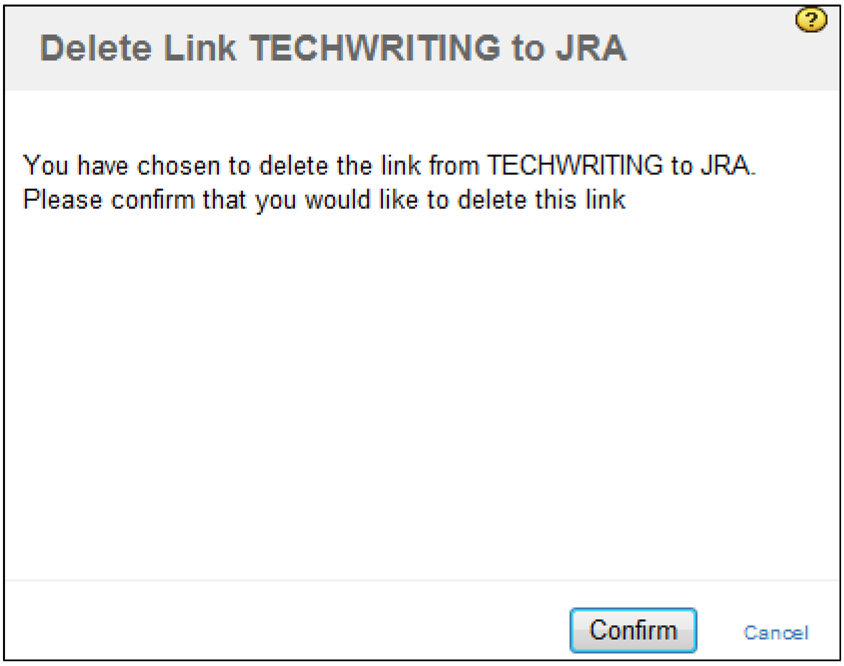
If you have set up multiple project links to the same application, for example you have linked a Confluence space to multiple JIRA projects, deleting the primary link will mean that another of the links will be made the primary link.

> *The information on this page does not apply to Confluence OnDemand.*

To delete a project link:

1. Choose **Browse** > **Space Admin**.
   Space Admin is displayed only if you are a space administrator for that space or you are a Confluence system administrator.
2. Click '**Application Links**' in the left-hand panel.
3. Click the '**Delete**' link next to the link that you want to delete.

4. A confirmation screen will appear. Click the '**Confirm**' button to delete the link.



Delete Link TECHWRITING to JRA

You have chosen to delete the link from TECHWRITING to JRA.
Please confirm that you would like to delete this link

Screenshot above: Confirming the deletion of a project link

Related Topics

Adding Project Links between Applications
Making a Project Link the Primary Link

Confluence and JIRA

- Installing Confluence and JIRA Together
- Integrating JIRA and Confluence
- Setting Up Trusted Communication between JIRA and Confluence

RELATED TOPICS

Connecting to Crowd or JIRA for User Management
JIRA Issues Macro
JIRA Portlet Macro

> ⚠ *The information on this page does not apply to Confluence OnDemand.*

Installing Confluence and JIRA Together

This page describes Atlassian's recommendation for installing JIRA and Confluence on the same server. Refer to Here Be Dragons for instructions on integrating all Atlassian applications.

⚠ **Do not deploy multiple Atlassian applications in a single Tomcat container** —
Deploying multiple Atlassian applications in a single Tomcat container is **not supported.** We do not test this configuration and upgrading any of the applications (even for point releases) is likely to break it. There are also a number of known issues with this configuration (see this FAQ for more information).

We also do not support deploying multiple Atlassian applications to a single Tomcat container for a number of practical reasons. Firstly, you must shut down Tomcat to upgrade any application and secondly, if one application crashes, the other applications running in that Tomcat container will be inaccessible.

Finally, we recommend not deploying *any other applications* to the same Tomcat container that runs Confluence, especially if these other applications have large memory requirements or require additional libraries in Tomcat's `lib` subdirectory.

⚠ *The information on this page does not apply to Confluence OnDemand.*

Recommended Setup - Separate Stand-Alone Installations

Atlassian recommends running JIRA and Confluence in separate stand-alone instances running behind an Apache Web Server. See the guides for:

- Installing Confluence
- Running Confluence behind Apache
- Installing JIRA
- Integrating JIRA with Apache

Advantages

- Each application can be restarted without affecting the other.
- If one webapp hangs for any reason (eg. running out of memory), it doesn't affect the other.
- Any problems can be debugged more easily. Logs are separate and product-specific, rather than everything going to catalina.out. Thread and heap dumps are smaller and more relevant.
- It reduces the likelihood of jar conflicts (eg. jars that must be installed in `common/lib` or `lib` for Confluence running off Apache Tomcat version 6 or above), particularly if you later want to install a third webapp not from Atlassian.
- Apache HTTP Web Server is well suited for running publicly available sites, with extensive modules for security and efficiency. It also allows for flexibility with URLs (ie http://confluence.atlassian.com, http://confluence, and so on).

ℹ Apache Web Server is recommended and reliable. It is also a third-party product, and therefore not developed nor supported by Atlassian. See Atlassian Support Offerings for details.

Integrating JIRA and Confluence

Please refer to the guide to Installing Confluence and JIRA Together.

JIRA and Confluence are designed to complement each other. Collect your team's thoughts, plans and knowledge in Confluence, track your issues in JIRA, and let the two applications work together to help you get your job done.

Below are some ways you can get JIRA and Confluence working together.

On this page:

⚠ *The information on this page does not apply to Confluence OnDemand.*

Setting Up Trusted Communication between JIRA and Confluence

An administrator can configure JIRA (3.12.0 or later) and Confluence to communicate in a trusted way, so that Confluence can request information from JIRA on behalf of the currently logged-in user. JIRA will not ask the user to log in again or to supply a password.

Trusted communication is used when embedding information from one application (for example, a list of JIRA issues) into another application (for example, a Confluence page).

Read more about trusted communication.

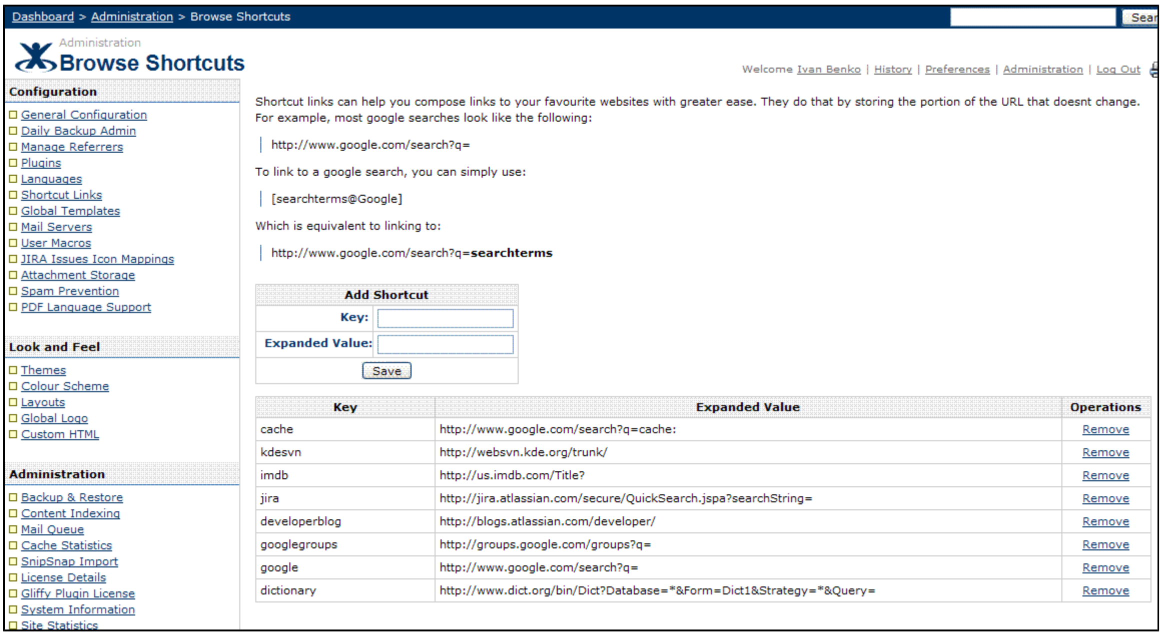
Inserting JIRA issues

You can insert issues from a JIRA site onto your Confluence page using the 'Insert JIRA Issue' dialogue box. You can also use this dialogue box to create a new issue on the JIRA site. See Inserting JIRA Issues.

Combining Confluence Shortcuts and JIRA Quick Search

In our Confluence site's global configuration (`Administration > Shortcut Links`) we have the following shortcut defined:

```
JIRA:
http://jira.atlassian.com/secure/QuickSear
ch.jspa?searchString=
```



Dashboard > Administration > Browse Shortcuts

Administration
Browse Shortcuts

Welcome Ivan Benko | History | Preferences | Administration | Log Out

Configuration

- □ General Configuration
- □ Daily Backup Admin
- □ Manage Referrers
- □ Plugins
- □ Languages
- □ Shortcut Links
- □ Global Templates
- □ Mail Servers
- □ User Macros
- □ JIRA Issues Icon Mappings
- □ Attachment Storage
- □ Spam Prevention
- □ PDF Language Support

Look and Feel

- □ Themes
- □ Colour Scheme
- □ Layouts
- □ Global Logo
- □ Custom HTML

Administration

- □ Backup & Restore
- □ Content Indexing
- □ Mail Queue
- □ Cache Statistics
- □ SnipSnap Import
- □ License Details
- □ Gliffy Plugin License
- □ System Information
- □ Site Statistics

Shortcut links can help you compose links to your favourite websites with greater ease. They do that by storing the portion of the URL that doesnt change. For example, most google searches look like the following:

```
http://www.google.com/search?q=
```

To link to a google search, you can simply use:

```
[searchterms@Google]
```

Which is equivalent to linking to:

http://www.google.com/search?q=**searchterms**

Add Shortcut

Key:	
Expanded Value:	

Save

Key	Expanded Value	Operations
cache	http://www.google.com/search?q=cache:	Remove
kdesvn	http://websvn.kde.org/trunk/	Remove
imdb	http://us.imdb.com/Title?	Remove
jira	http://jira.atlassian.com/secure/QuickSearch.jspa?searchString=	Remove
developerblog	http://blogs.atlassian.com/developer/	Remove
googlegroups	http://groups.google.com/groups?q=	Remove
google	http://www.google.com/search?q=	Remove
dictionary	http://www.dict.org/bin/Dict?Database=*&Form=Dict1&Strategy=*&Query=	Remove

Use the above option to create links using Confluence's shortcut notation.

- Link directly to JIRA issues like this: CONF-1000
- Use JIRA's quick-search functionality to create links to particular groups of issues. The following link will display a list of all open issues in the Confluence project of type 'Improvement': CONF open improvements

Viewing Confluence Content in JIRA or JIRA Content in Confluence

Using Gadgets

You can embed a Confluence activity stream or a Confluence page in JIRA's dashboard. Likewise, JIRA gadgets can be rendered on a Confluence page. See Adding a Confluence Gadget to a JIRA Dashboard and Gadget Macro for information on how to set up gadgets.

Using the JIRA Issues macro

For versions earlier than Confluence 3.1 and JIRA 4.0, use the {jiraissues} and {jiraportlet} macros to embed JIRA reports and portlets into your Confluence site

Any JIRA search result can be embedded in a Confluence page using the JIRA Issues macro with your choice of included fields and field ordering, and any JIRA dashboard portlet can be embedded in a Confluence page using the JIRA Portlet macro.

Integrating JIRA and Confluence User Management

To save you having to enter users into both JIRA and Confluence, you may benefit from using Atlassian Crowd a s the user repository for both applications. Alternatively you can configure Confluence to use JIRA's user database. See Connecting to Crowd or JIRA for User Management.

Useful Plugins

Before installing a plugin into your Confluence site, please check the plugin's information page to see whether it is supported by Atlassian, by another vendor, or not at all. See our guidelines on plugin support.

- The JIRA Linker plugin provides a custom field that helps you find an URL, particularly a Confluence page, so you can add a page link into a JIRA issue.

Setting Up Trusted Communication between JIRA and Confluence

An administrator can configure JIRA and Confluence to communicate in a trusted way, so that Confluence can request information from JIRA on behalf of the currently logged-in user. JIRA will not ask the user to log in again or to supply a password.

When JIRA is configured to trust Confluence in this way, we call Confluence the '**trusted application**' and JIRA the '**trusting application**'.

Trusted communication is used when embedding information from one application (e.g. a list of JIRA issues) into another application (e.g. a Confluence page). Currently only JIRA can be configured to trust Confluence, and only the following two macros have been enhanced to use trusted communication:

- JIRA Issues macro
- JIRA Portlet macro

Further implementations will follow, especially as we roll out the tight integration required between Atlassian products for JIRA Studio.

Potential security risk

Do not configure a trusted application unless you trust all code in that application to behave itself at all times. Trusted communication uses public/private key cryptography to establish the identity of the trusted server, so you must also be sure that the trusted application will maintain the security of its private key. Read the details of the security risks below.

On this page:

⚠ *The information on this page does not apply to Confluence OnDemand.*

Prerequisites

- JIRA 3.12.0 or later.
- Confluence 2.7.0 or later.
- In order to authenticate successfully against JIRA, the Confluence user must also be registered as a JIRA user with the same username.

⚠ **Common user base recommended**

It is **highly recommended** that your JIRA and Confluence instances share a common user base, rather than two separate user bases with duplicated usernames. You will receive an error if Confluence passes JIRA a username which JIRA cannot recognise. Also, with separate user bases you run the risk that the same username may be used by two different people. The trusted application does not supply the user's password, so the trusting application will assume the username belongs to the user registered in the trusting application's own user base.

✓ **Tip:** Try Atlassian Crowd for a tidy user management solution.

Why do we need Trusted Communication?

The JIRA Issues and the JIRA Portlet macros allow you to embed a list of JIRA issues into a Confluence page. Prior to Confluence 2.7, if you wanted to display JIRA issues that had restricted viewing, then you needed to store the JIRA user's credentials (username and password) in the macro code directly on the Confluence page. This was not very secure.

The reasons we require the user credentials are:

- Your JIRA instance might not be public, and you might not want to allow anonymous access to your issues.
- You might have security restrictions on some of your issues. So you don't want to allow someone to leak data from your JIRA project by using the JIRA Issues Macro on a Confluence page.

Overview

Here is a summary of the integration points in a trusted communications relationship. Each of the following points is described in more detail in the sections below.

- A JIRA System Administrator configures JIRA to trust Confluence.
- A Confluence System Administrator configures the macro plugin to use (or not use) trusted communication.
- A Confluence user adds one of the macros to a Confluence page.
- A Confluence user or anonymous user views the Confluence page.

Configuring JIRA to Trust Confluence Using Trusted Applications

Trust only has to be established once between the two applications. Once trust has been established, it is entirely transparent to the Confluence users.

Application links are used to enable trust relationships between two applications. Linking two applications allows you to share information and access one application's functions from within the other.

You can configure an application link to use Trusted Applications as the authentication mechanism. For instructions, see Configuring Trusted Applications Authentication for an Application Link.

Configuring the Macro Plugin in Confluence

By default, Confluence ships with trusted communication enabled for the following macros:

- JIRA Issues macro
- JIRA Portlet macro

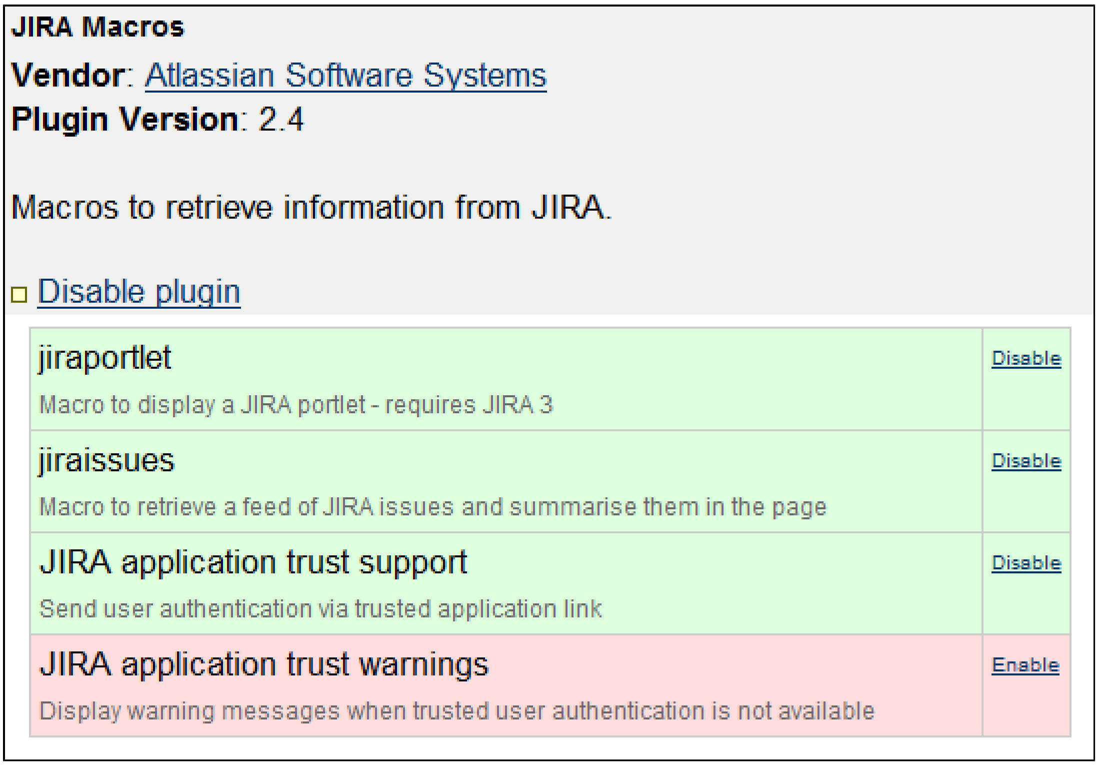
A Confluence System Administrator can decide on the level of trusted communication used by the macros. The different levels are:

- Ignore trusted communications altogether. Trusted communication is turned off at the global level.
- Perform trusted communications whenever the macro is used on a Confluence page, but do not show certain warning messages.
- Perform trusted communications whenever the macro is used on a Confluence page, and show all warning messages. **This is the default configuration.**

To change the default trusted communication level for the JIRA Macros plugin,

1. Choose **Browse** > **Confluence Admin**.
2. Select '**Plugins**' in the left-hand panel.
3. The '**Plugin Manager**' screen appears, showing a list of installed plugins. Scroll down and click the '**JIRA Macros**' link.
4. The '**JIRA Macros**' panel appears in the top middle of the screen, as shown below. Click '**Enable**' or '**Disable**' next to the following options:
    - '**JIRA application trust support**' – With this option enabled, Confluence will attempt trusted communication with JIRA whenever a user views a page containing the JIRA Issues or Portlet macro, provided criteria are met as described below. With this option disabled, Confluence will never attempt trusted communication with JIRA for these macros.
      ✓ Disable the above option if you do not intend to configure trusted communication between JIRA and Confluence.
    - '**JIRA application trust warnings**' – With this option enabled, Confluence will display all error and warning messages that may arise from a problem during trusted communication (assuming that trusted communication is enabled). With this option disabled, Confluence will suppress certain warnings. See troubleshooting below.
      ✓ Disable the above option if you have a large number of existing JIRA macros already on your Confluence instance, pointing at a diverse range of JIRA servers. Some of those JIRA servers may have a trusted communication link established (requiring the functionality to be enabled) while other JIRA servers may have no trusted communication link. In this case, you may want to turn off the warning messages so they do not appear on your Confluence pages where the JIRA macros point to non-trusting JIRA servers.

Screenshot: JIRA Macros panel in Plugin Manager



JIRA Macros
Vendor: Atlassian Software Systems
Plugin Version: 2.4

Macros to retrieve information from JIRA.

□ Disable plugin

jiraportlet Macro to display a JIRA portlet - requires JIRA 3	Disable
jiraissues Macro to retrieve a feed of JIRA issues and summarise them in the page	Disable
JIRA application trust support Send user authentication via trusted application link	Disable
JIRA application trust warnings Display warning messages when trusted user authentication is not available	Enable

Adding the Macro to a Confluence Page

The Confluence user can add and edit the macros as described on the following pages:

- Using the JIRA Issues macro

- Using the JIRA Portlet macro

✓ **Remove the username and password from your macro markup code**

Prior to Confluence 2.7, you needed to include a username and password in the macro markup code if you wanted to display JIRA issues which had restricted viewing. Once your administrator has set up trusted communication between Confluence and JIRA, you no longer need to include a username and password in the markup code for your JIRA macros.

The following options are available for determining the issues which will be retrieved from JIRA and displayed on the Confluence page:

What you want to do	Macro parameter	URL parameter	Comments
Display the JIRA issues which the logged-in user is authorised to see. And if the user is not logged in, display only issues which allow unrestricted viewing.			Do not specify any authentication parameters. In this case, the behaviour depends on the way your administrator has set up trusted communication between JIRA and Confluence. Here is a summary of the behaviour. If trusted communication is **enabled**, the authorisation will work seamlessly. When a logged-in user views your page, they will see only the JIRA issues they are allowed to see. And if they are not logged in, they will see only the issues which allow unrestricted viewing. If trusted communication is **disabled**, the Confluence page will show only the JIRA issues which allow unrestricted viewing.

Ensure that Confluence will display only the JIRA issues which allow unrestricted viewing.	`anonymous`		Regardless of who the user is (logged in or not), the Confluence page will show only anonymously-visible issues. Confluence will not attempt to set up a trusted communication link with JIRA in this case.
Use a pre-determined username and password to access the JIRA issues.		`&os_username=MYNAME&os_password=MYPASSWORD`	**Not recommended**. Prior to Confluence 2.7, this was the only way of displaying issues with restricted viewing. For Confluence 2.7 and later, this method will still work. Confluence will not attempt to set up a trusted communication link with JIRA in this case.

Refer to the section below for details of what happens when a user views a Confluence page containing a JIRA macro.

Viewing the Confluence Page

When a user views a Confluence page which contains a JIRA Issues or JIRA Portlet macro, this is what happens:

- If the macro markup contains an explicit username and password in the URL parameter, Confluence will not request trusted communication with JIRA. Confluence will retrieve the JIRA issues which the specified username is authorised to see. This behaviour is the same as Confluence versions prior to 2.7.
- If the macro markup contains the `anonymous` parameter, Confluence will retrieve only the JIRA issues which allow unrestricted viewing. Confluence will not attempt to set up a trusted communication link with JIRA in this case.
- If the user is anonymous (not logged in), Confluence will retrieve only the JIRA issues which allow unrestricted viewing. Confluence will not attempt to set up a trusted communication link with JIRA in this case.
- If trusted communication is disabled via the Plugin Manager in Confluence, then Confluence will not request trusted communication with JIRA. So if there is no explicit username and password in the markup code, Confluence will retrieve only the JIRA issues which allow unrestricted viewing. This behaviour is the same as Confluence versions prior to 2.7.
- If trusted communication is enabledvia the Plugin Manager in Confluence:
  - If the user is logged in, then Confluence attempts trusted communication with JIRA. Confluence sends the username to JIRA. JIRA returns a set of issues which that username is authorised to access, based on the JIRA user base and the JIRA groups and permissions. Confluence displays those issues on the page.
  - If JIRA or Confluence encounters a problem during the trusted communication process, an error message may appear on the Confluence page above the macro output – see troubleshooting below.

Security Risks

Please take the following considerations into account when setting up trusted communication:

- When you configure JIRA to trust an application, you are allowing the application to access JIRA in the name of a particular user. The trusted application passes JIRA the user's login name, but no other authentication information. JIRA does not request the user's password. By doing this, you are **bypassing JIRA's authentication mechanism**.
- Do not configure a trusted application unless you **trust all code in that application** to behave itself at all times.
- Trusted communication uses public/private key cryptography to establish the identity of the trusted server. The trusted application needs to maintain the security of its private key. Confluence stores its private key in the database. **So you must be sure that the Confluence database is secure, and also any full backups of the database.**
- Ensure that you **specify an IP address** for your Confluence site when configuring trusted applications in JIRA. Do not use the wild card `*.*.*.*` as the IP address. Failure to configure IP address restrictions is a security vulnerability, allowing an unknown site to log into your JIRA site under a user's login ID.
- Be aware of the risks associated with using separate user bases, as explained above. **We strongly recommend a common user base between the trusted and trusting applications.**
- When configuring an application to trust another application, you should use a trusted network or SSL to **protect the sensitive information passed between the applications during the configuration procedure**. This will help to prevent man-in-the-middle attacks.

Troubleshooting

Below are the warning messages which may appear on your Confluence page, above the output of the JIRA Issues or JIRA Portlet macro.

Warning Message	Cause	Solution	Warning Message Can be Turned Off?
`javax.net.ssl.SSLHandshakeException: sun.security.validator.ValidatorException: PKIX path building failed: sun.security.provider.certpath.SunCertPathBuilderException: unable to find valid certification path to requested target`	JIRA is running over SSL	Add JIRA's SSL Certificate to the Java Keystore	**No**
`The JIRA server does not recognise your user name. Issues have been retrieved anonymously.`	The logged-in Confluence user is not registered in the JIRA user base.	Add the username to your JIRA user base. It is **highly recommended** th at your JIRA and Confluence instances share a common user base.	**No**

The JIRA server does not trust this Confluence instance for user authentication. Issues have been retrieved anonymously. You can set the macro to always use an anonymous request by setting the 'anonymous' parameter to 'true'.	Your JIRA instance has not been configured to trust your Confluence instance.	One of the following solutions: - Configure JIRA to trust Confluence. - Disable trusted communications for the JIRA macros in Confluence. - Use the anonymous parameter in all your JIRA Issues and JIRA Portlet macros.	Yes
The JIRA server does not support trust requests. Issues have been retrieved anonymously. You can set the macro to always use an anonymous request by setting the 'anonymous' parameter to 'true'.	Your JIRA instance is not able to handle trusted communications (i.e. the JIRA version is earlier than 3.12.0).	One of the following solutions: - Download the latest version of JIRA and then configure JIRA to trust Confluence. - Disable trusted communications for the JIRA macros in Confluence. - Use the anonymous parameter in all your JIRA Issues and JIRA Portlet macros.	Yes
Failed to login trusted application: confluence:14159892 due to: com.atlassian.security.auth.trustedapps.CertificateTooOldException: OLD_CERT; Certificate too old.	There is a date/time difference between the JIRA server and Confluence server.	- Certificate Too Old KnowledgeBase Entry	-

Consult Troubleshooting the JIRA Issues Macro and Trusted Applications for further troubleshooting.

Technical Overview of the Trusted Applications Authentication (TAA) Protocol

✅ Read this section if you want a bit more information on the technical side of things.

Atlassian has developed its own protocol to set up trust between JIRA and Confluence. Below is a technical overview of the process.

Configuring JIRA to trust Confluence:

1. When the JIRA System Administrator provides the base URL of the Confluence instance, JIRA requests a trusted application authentication certificate from Confluence. The certificate contains Confluence's trusted application ID and public key (generated specifically for use with the TAA protocol).
2. JIRA validates the certificate and asks the System Administrator for a few extra details about the trust relationship, such as a name for the Confluence instance, timeout, allowed IP addresses and allowed request URLs.
3. JIRA stores all this information in the database.

Making a trusted request from Confluence to JIRA:

1. Confluence sends a web request to JIRA, appending additional headers to the request, including:
   - Timestamp (nonce) of the request + user name of the currently logged-in Confluence user, encrypted with a symmetric key (generated on the fly).
   - The symmetric key, encrypted with Confluence's private key.
   - Confluence's application ID (as displayed when trusted communication was established).
2. JIRA attempts to decode the encrypted headers, using the stored information about the relationship. It conducts the following checks to validate the request:
   - The trusted application ID refers to a valid trusted application.
   - The given username exists in the JIRA user base.
   - The agreed timeout has not expired.
   - The request originated from a trusted IP address.
   - The resource being requested matches those specified in the URL match list.
3. If any of these checks fails, a response is sent to Confluence indicating the reason for failure. Otherwise, JIRA will authenticate the specified user for the duration of the single request, and respond with the resources (i.e. the JIRA issues).

RELATED TOPICS

JIRA Issues Macro
JIRA Portlet Macro
Connecting to LDAP or JIRA or Other Services via SSL
Single Sign-on Integration with JIRA and Confluence
Troubleshooting the JIRA Issues Macro and Trusted Applications