



1. Confluence SharePoint Connector Home	3
1.1 SharePoint Connector User's Guide	3
1.1.1 Embedding Confluence Content into SharePoint Pages	5
1.1.1.1 Using the SharePoint 2007 Web Parts	6
1.1.1.2 Using the SharePoint 2010 Web Parts	11
1.1.1.3 Connecting Data in your Web Parts	17
1.1.2 Embedding SharePoint Content into Confluence Pages	19
1.1.2.1 Using the SharePoint List Macro	19
1.1.2.2 Using the SharePoint Link Macro	25
1.1.3 Searching Confluence and Sharepoint Content	29
1.1.4 Setting your Browser Options for Automatic Login	30
1.2 SharePoint Connector Administrator's Guide	36
1.2.1 Updating your SharePoint Connector License Details	36
1.2.2 Configuring the SharePoint Connector NTLM Proxy	37
1.2.3 SharePoint Connector Security Advisories	39
1.2.3.1 SharePoint Connector Security Advisory 2010-01-18	39
1.2.3.2 SharePoint Connector Security Advisory 2010-11-29	40
1.2.4 Support Policies	40
1.2.4.1 Bug Fixing Policy	41
1.2.4.2 How to Report a Security Issue	41
1.2.4.3 New Features Policy	42
1.2.4.4 Patch Policy	42
1.2.4.5 Security Advisory Publishing Policy	43
1.2.4.6 Security Patch Policy	43
1.2.4.7 Severity Levels for Security Issues	44
1.2.5 Troubleshooting the SharePoint Connector	45
1.2.5.1 Analysing the SharePoint Logs	45
1.2.5.2 Tracing the SharePoint Feature	46
1.2.5.3 Troubleshooting the SharePoint Configuration in Confluence	47
1.2.5.4 Using the CSI Diagnostics Tool to Test Confluence and SharePoint Connectivity	48
1.2.5.5 Determining which NTLM version is used	50
1.2.5.6 Enable Detailed Logging for the SharePoint Connector NTLM Proxy	51
1.3 SharePoint Connector Installation and Upgrade Guide	51
1.3.1 Release Notes	52
1.3.1.1 SharePoint Connector 1.3 Release Notes	52
1.3.1.1.1 SharePoint Connector 1.3 Upgrade Notes	57
1.3.1.2 SharePoint Connector 1.2.1 Release Notes	58
1.3.1.3 SharePoint Connector 1.2 Release Notes	59
1.3.1.3.1 SharePoint Connector 1.2 Upgrade Notes	65
1.3.1.4 SharePoint Connector 1.1.1 Release Notes	66
1.3.1.5 SharePoint Connector 1.1 Release Notes	66
1.3.1.5.1 SharePoint Connector 1.1 Upgrade Notes	69

1.3.1.6 SharePoint Connector 1.0 Release Notes	71
1.3.1.6.1 SharePoint Connector 1.0 Changelog	72
1.3.2 Installing the SharePoint Connector	73
1.3.2.1 Installing the SharePoint Connector on SP 2007	74
1.3.2.1.1 Planning your Environment with SP 2007	74
1.3.2.1.2 Configuring Access to SharePoint with SP 2007	78
1.3.2.1.3 Installing and Configuring the Confluence Plugins for SP 2007	90
1.3.2.1.4 Configuring Access to Confluence for SP 2007	94
1.3.2.1.5 Installing and Configuring the SharePoint Feature on SP 2007	101
1.3.2.2 Installing the SharePoint Connector on SP 2010	115
1.3.2.2.1 Planning your Environment with SP 2010	116
1.3.2.2.2 Configuring Access to SharePoint with SP 2010	120
1.3.2.2.3 Installing and Configuring the Confluence Plugins for SP 2010	132
1.3.2.2.4 Configuring Access to Confluence for SP 2010	136
1.3.2.2.5 Installing and Configuring the SharePoint Feature on SP 2010	143
1.3.3 Upgrading the SharePoint Connector	156
1.3.3.1 Upgrading the SharePoint Connector on SharePoint 2007	156
1.3.3.2 Upgrading the SharePoint Connector on SharePoint 2010	158
1.3.4 Applying Specific Confluence Configurations	160
1.3.4.1 Configuring Tomcat-Connector for IIS 6.0 (Windows Server 2003)	160
1.3.4.2 Configuring Tomcat-Connector for IIS 7.0 (Windows Server 2008)	164
1.3.4.3 Configuring Confluence to use Jespa for NTLM Authentication	171
1.3.4.4 Configuring Confluence to use JCIFS for NTLM Authentication	173
1.3.5 Deploying the SharePoint Connector to More SharePoint Sites	175
1.4 SharePoint Connector FAQ	177
1.4.1 Comparing SharePoint Versions and Editions	177
1.4.2 Planning your Authentication Configuration	178
1.4.3 NTLM and Anonymous Access	178
1.4.4 Introduction to SharePoint and Confluence Terminology	179
1.4.5 How the SharePoint Connector Manages Permissions	180
1.4.6 Connecting to Multiple SharePoint Sites	180
1.4.7 Manual SharePoint Feature Installation	180
1.4.8 Using the SharePoint Connector with Confluence Clustered	182
1.4.9 Using the SharePoint Connector with a Confluence Starter License	182
1.5 Documentation under Review	182
1.5.1 SharePoint Connector FAQ under review	182
1.6 Contributing to the SharePoint Connector Documentation	185

Confluence SharePoint Connector Home

SharePoint Connector 1.3

About the Confluence SharePoint Connector

With the [Confluence SharePoint Connector](#) you can combine Confluence's free-form, easy to edit wiki with the document management and workflow strengths of SharePoint.

- Display SharePoint document libraries, calendars, links, discussions and more on your Confluence wiki pages. Edit SharePoint's Office documents directly from Confluence and save them back to SharePoint.
- Embed Confluence pages and Confluence page trees into a SharePoint page. Click through from SharePoint to Confluence.
- Enjoy automatic login (single sign-on) between Confluence and SharePoint.
- Search Confluence and SharePoint content together, retrieving a unified set of results

User's Guide

The [SharePoint Connector User's Guide](#) is for project managers, developers, testers – anyone who uses the Confluence SharePoint Connector. New to the SharePoint Connector? Start with an overview of the connector's features on our [website](#). Then have a more detailed look at the SharePoint web parts and Confluence macros, described in the [user's guide](#). Never used Confluence before? Then you need the [Confluence documentation](#) first.

Administrator's Guide

The [SharePoint Connector Administrator's Guide](#) is for people with Confluence and SharePoint administration rights. It will help you update your [license details](#) and understand our [support policies](#). There are also some handy guides to [troubleshooting](#). You may also find the [Knowledge Base](#), [FAQ](#) and [forum](#) useful. Of course, the [Confluence Administrator's Guide](#) is also for you.

Installation Guide

The [SharePoint Connector Installation Guide](#) is for people who are installing the connector for the first time. Check our guides to planning your environment [with SharePoint 2007](#) or [with SharePoint 2010](#). Then follow the detailed [guide](#) to install the plugins into Confluence and the features into SharePoint.

Upgrade Guide

The [SharePoint Connector Upgrade Guide](#) is for people who are upgrading from one version of the connector to a later version. Start by reading the [latest release notes](#) and the attached upgrade notes for the version to which you are upgrading. Then and follow the upgrade guide [for SharePoint 2007](#) or [for SharePoint 2010](#).

SharePoint Connector User's Guide

The SharePoint Connector User's Guide tells you how to search Confluence and SharePoint content, display SharePoint content in Confluence and display Confluence content in SharePoint.

On this page:

- [Embedding Confluence Content on a SharePoint Page](#)
- [Embedding SharePoint Content on a Confluence Page](#)
- [Searching Confluence and Sharepoint Content](#)

Embedding Confluence Content on a SharePoint Page

Using the Confluence SharePoint Connector, you can display Confluence pages and page trees on your SharePoint pages.

**Quick guide to adding Confluence content on SharePoint pages**

- Go to a web part page in SharePoint and edit the page.
- Click '**Add a Web Part**' in the zone where you want to put your Confluence web part.
- Scroll down to find the Confluence web parts:
 - Select the '**Confluence Page**' web part if you want to embed a single Confluence page.
 - Select the '**Confluence Pages Tree View**' web part if you want to embed a hierarchical tree of pages from a Confluence space.
- The web part is now part of your SharePoint page. Click the web part's dropdown menu and select '**Modify Shared Web Part**' or '**Edit Web Part**'.
- The web part editor appears. Select the required space, and the page if relevant.
- Click '**OK**'.

Want more?

Please refer to the guide for [SharePoint 2007 web parts](#) and for [SharePoint 2010 web parts](#).

Embedding SharePoint Content on a Confluence Page

Displaying SharePoint Lists on a Confluence Page

Add the SharePoint List macro to a Confluence page, to embed SharePoint content into the page.

**Quick guide to the SharePoint List macro**

Using the simplest form of the macro, all you need to enter is the name of your SharePoint list and the list type. The macro will display default columns, based on the list type.

- Enter the following text onto the Confluence page:

```
{sp-list:LIST NAME|LIST TYPE}
```

- Replace the text 'LIST NAME' and 'LIST TYPE' with your own values.

Linking to a SharePoint List or Document from a Confluence Page

Add the SharePoint Link macro to a Confluence page, to link to a SharePoint list or document from the Confluence page.

**Quick guide to the SharePoint Link macro**

Using the simplest form of the macro, all you need to enter is the name of your SharePoint list or document library, and optionally the path to a document. The SharePoint Link macro will create a hyperlink on your page, pointing to the SharePoint location or file specified.

- Enter the following text onto the Confluence page to link to a list:

```
{sp-link:LIST-NAME}my hyperlinked text{sp-link}
```

Or enter the following text to link to a specific document:

```
{sp-link:LIBRARY-NAME/DOCUMENT-NAME}my hyperlinked text{sp-link}
```

- Replace the text 'LIST-NAME' with your own values for your SharePoint list name, or replace the text 'LIBRARY-NAME/DOCUMENT-NAME' with your SharePoint document library and file name.
- Replace the text 'my hyperlinked text' with the words that you want displayed as a hyperlink on the Confluence page.

Want more?

Please refer to the details of the parameters and options for the [{sp-list} macro](#) and the [{sp-link} macro](#).


Searching Confluence and Sharepoint Content

Searching in SharePoint

When you perform a search in SharePoint:

- By default, all searches will return content from both Confluence and Sharepoint.
- The results will be ordered by relevance, regardless of which system they are from.

To search for Confluence and SharePoint content from a SharePoint page,

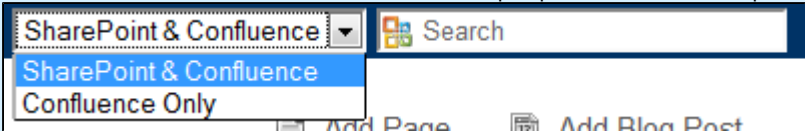
1. Select '**All Sites**' in the search scope option. Note that your search scope cannot be '**This Site**' or '**This List**'.
2. Enter your search words and click the '**Go Search**' icon. Here is an example of the SharePoint search box:
 
3. The search results page will open, showing the Confluence federated search results web part.

Searching in Confluence

There are two options when searching from a Confluence screen:

- Searching Confluence only
- Searching SharePoint and Confluence.

To search for Confluence and SharePoint content from a Confluence page,

1. Select '**SharePoint & Confluence**' in the search scope option. Here is an example of the Confluence search box:
 
2. Enter your search words and click the '**Search**' button.
3. The search will open in **SharePoint** and the results will be the same as when you perform the search from SharePoint.

Want more?

Please refer to the [detailed guide to searching](#).

RELATED TOPICS

- [Troubleshooting the SharePoint Connector](#)
- [Embedding Confluence Content into SharePoint Pages](#)
- [Embedding SharePoint Content into Confluence Pages](#)
- [Searching Confluence and Sharepoint Content](#)
- [Setting your Browser Options for Automatic Login](#)

Embedding Confluence Content into SharePoint Pages

Using the Confluence SharePoint Connector, you can display Confluence pages and page trees on your SharePoint pages.



Quick guide to adding Confluence content on SharePoint pages

- Go to a web part page in SharePoint and edit the page.
- Click '**Add a Web Part**' in the zone where you want to put your Confluence web part.
- Scroll down to find the Confluence web parts:
 - Select the '**Confluence Page**' web part if you want to embed a single Confluence page.
 - Select the '**Confluence Pages Tree View**' web part if you want to embed a hierarchical tree of pages from a Confluence space.
- The web part is now part of your SharePoint page. Click the web part's dropdown menu and select '**Modify Shared Web Part**' or '**Edit Web Part**'.
- The web part editor appears. Select the required space, and the page if relevant.
- Click '**OK**'.

The following pages give more details of the above procedure:

- [Using the SharePoint 2007 Web Parts](#)
- [Using the SharePoint 2010 Web Parts](#)
- [Connecting Data in your Web Parts](#)

Using the SharePoint 2007 Web Parts

This page tells you how to embed Confluence content into SharePoint pages, when your SharePoint and Confluence sites are connected via the Confluence SharePoint Connector. The instructions on this page apply to **SharePoint 2007**.

The SharePoint Connector provides SharePoint web parts that you can use to display Confluence pages and page trees in SharePoint. Users can view the Confluence content from within SharePoint and click through from SharePoint to Confluence.



Quick guide to adding Confluence content on SharePoint pages

- Go to a web part page in SharePoint and edit the page.
- Click '**Add a Web Part**' in the zone where you want to put your Confluence web part.
- Scroll down to find the Confluence web parts:
 - Select the '**Confluence Page**' web part if you want to embed a single Confluence page.
 - Select the '**Confluence Pages Tree View**' web part if you want to embed a hierarchical tree of pages from a Confluence space.
- The web part is now part of your SharePoint page. Click the web part's dropdown menu and select '**Modify Shared Web Part**' or '**Edit Web Part**'.
- The web part editor appears. Select the required space, and the page if relevant.
- Click '**OK**'.

The rest of this page gives more details of the above procedure.

On this page:

- [Adding a SharePoint Web Part](#)
- [Using the Confluence Page Web Part](#)
 - [Hiding and Showing Page Comments](#)
- [Using the Confluence Pages Tree View Web Part](#)

Adding a SharePoint Web Part

Below is a summary of how to add the Confluence web parts in SharePoint. For detailed instructions on the SharePoint side of things, please refer to the SharePoint online help.

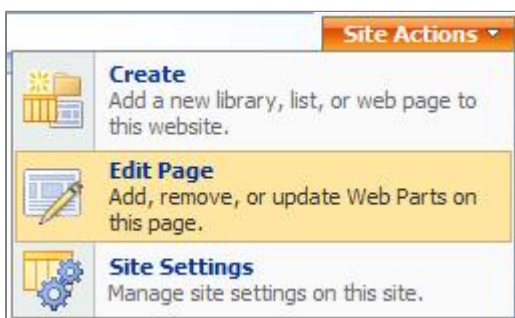
To add a SharePoint web part, you need SharePoint 'Design' permission level or better. This permission is available to anyone in a group that has the SharePoint 'Add and Customize Pages' site permission.

You can add web parts to a SharePoint 'web part page'. Many of the pages in SharePoint are web part pages, including the home page in any SharePoint site. You can also create web part pages in a document library that has the 'Web Part Page' document template. Such a document library typically has the name 'Pages'.

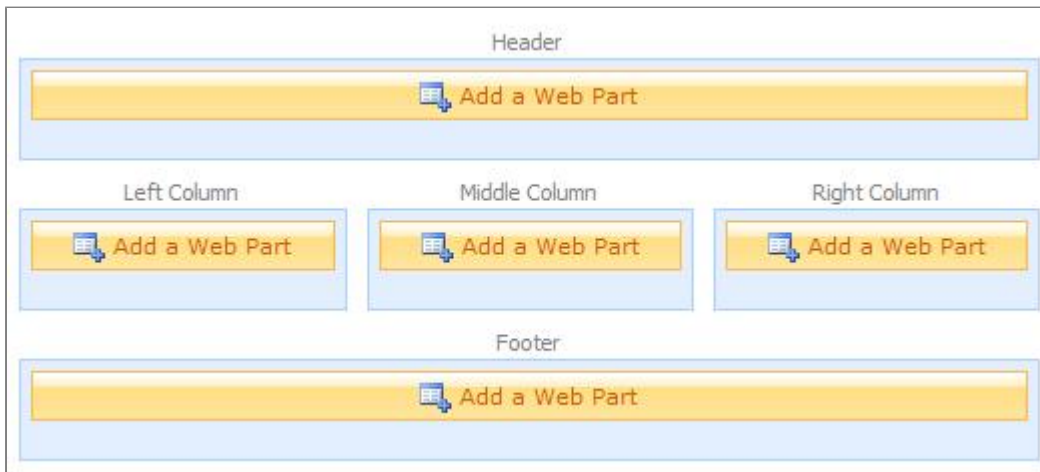
To add the Confluence web parts in SharePoint,

1. Go to a web part page in SharePoint.
2. Edit the page. (Click '**Site Actions**' then '**Edit Page**'.)
3. The page opens in edit mode, showing the web part zones defined for the page. Click the '**Add a Web Part**' button in the zone where you want your web part(s) to reside.
4. The '**Add Web Parts**' dialogue appears. Scroll down to find the Confluence web parts and select one or both of them.

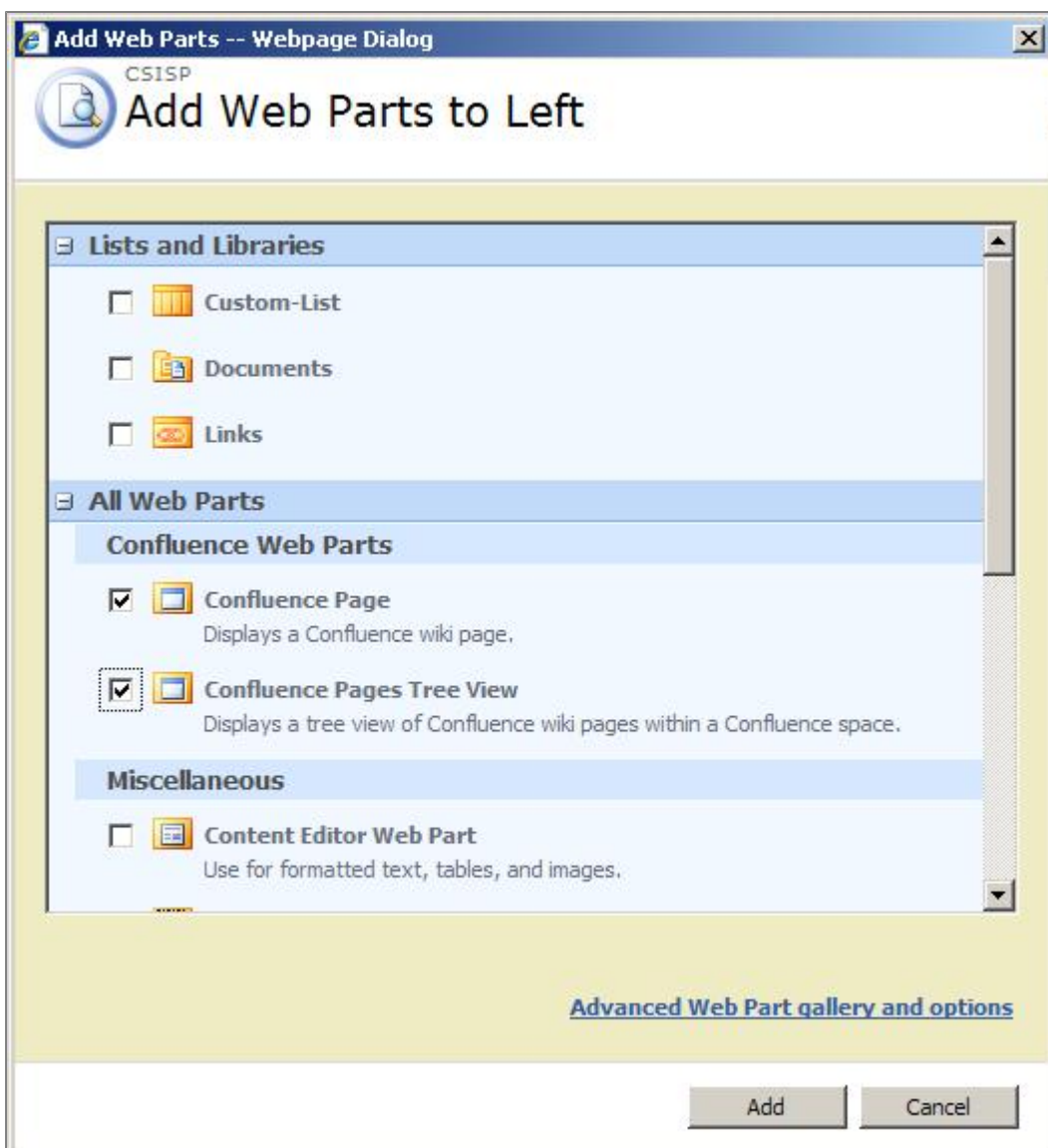
Screenshot 1: Editing a page via the 'Site Actions' menu



Screenshot 2: Page zones with 'Add a Web Part' buttons



Screenshot 3: Selecting the Confluence web parts



Using the Confluence Page Web Part

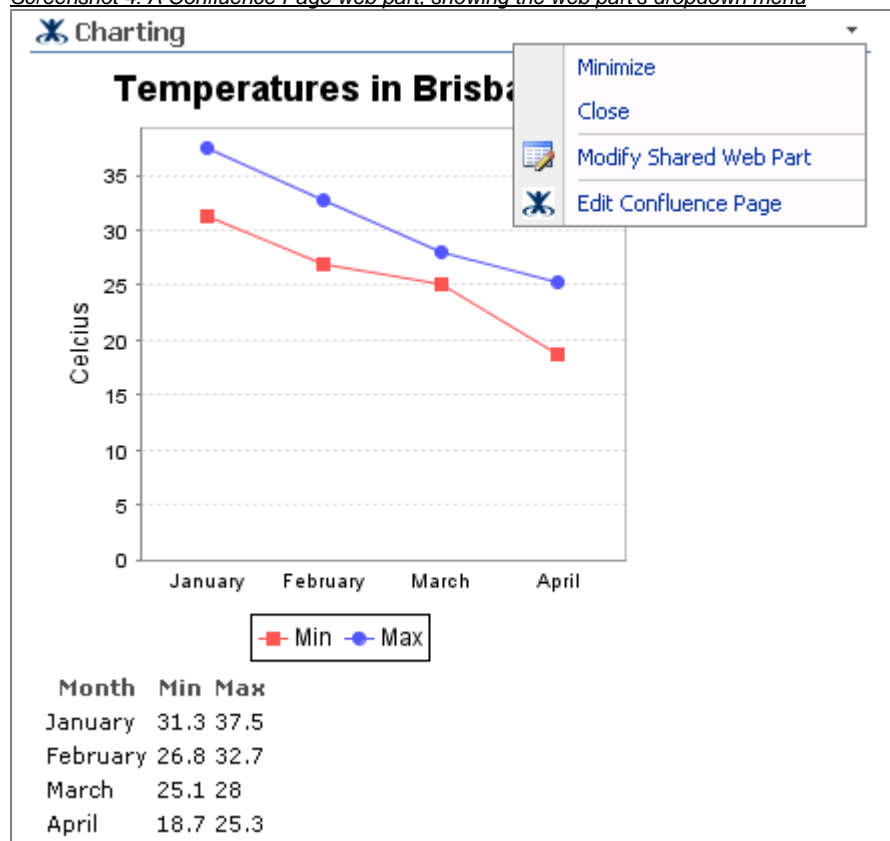
You can use the Confluence Page web part to display a specific page from Confluence in SharePoint.

To add and customise the Confluence Page web part,

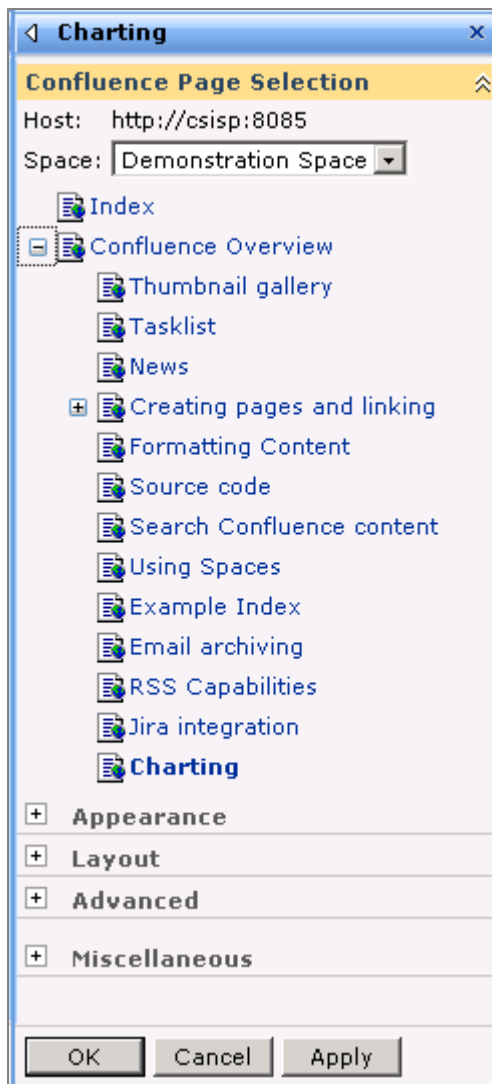
1. Add the '**Confluence Page**' web part, following the instructions [above](#).
2. The web part is now part of your SharePoint page. Click the web part's dropdown menu and select '**Modify Shared Web Part**'.
3. The '**Confluence Page Selection**' web part editor appears. Select the required space from the '**Space**' dropdown list.
4. A hierarchical (tree view) list of pages appears. Select the required page.
5. Click '**OK**' or '**Apply**' to make the page show in the web part.

See our guide to [web part connections](#) for information on connecting this web part to other web parts.

Screenshot 4: A Confluence Page web part, showing the web part's dropdown menu



Screenshot 5: The 'Confluence Page Selection' web part editor



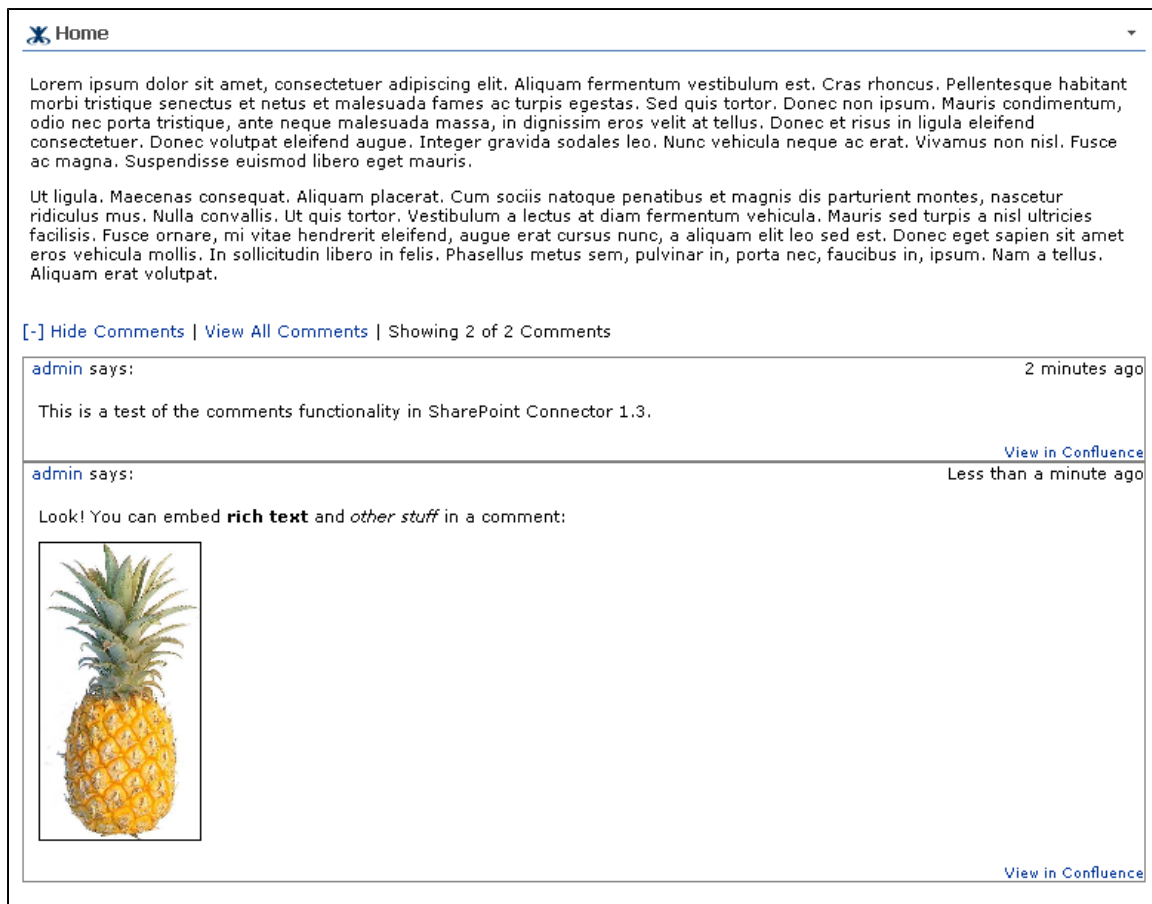
As shown in the above screenshot, the 'Confluence Page Selection' web part editor displays the following information:

- The editor title is the Confluence page name.
- The Confluence '**Host**' comes from the settings in SharePoint's 'Confluence Settings' page (found under 'Site Settings').
- The list of Confluence spaces shows only those spaces that the user has permission to see, based on the Confluence space permissions.

Hiding and Showing Page Comments

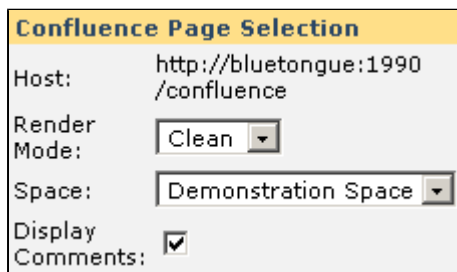
By default, displaying a Confluence page using the Confluence Page web part will also display any comments on the page.

Screenshot 4: Displaying page comments in the Confluence Page web part



To prevent the comments from displaying, edit the web part and ensure that the **'Display Comments'** option is not selected.

Screenshot 5: Disable the 'Display Comments' option to hide any comments on the page



Using the Confluence Pages Tree View Web Part

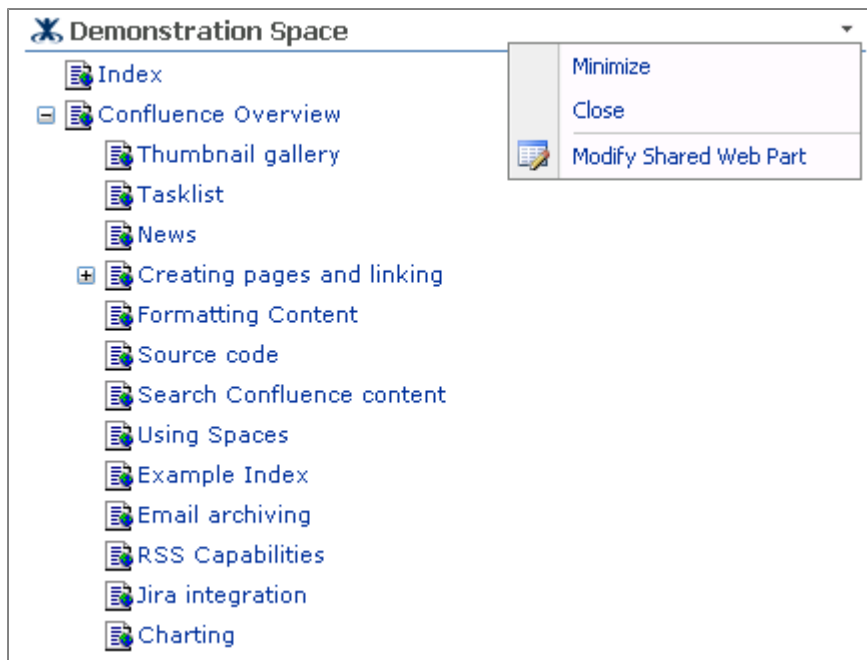
You can use the Confluence Pages Tree View web part to display a hierarchical view of pages from a specific Confluence space.

To add and customise the Confluence Pages Tree View web part,

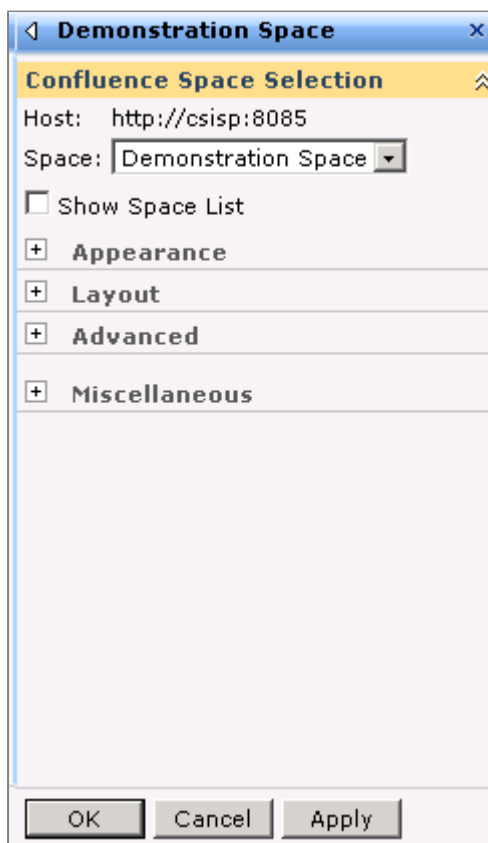
1. Add the **'Confluence Pages Tree View'** web part, following the instructions [above](#).
2. The web part is now part of your SharePoint page. Click the web part's dropdown menu and select **'Modify Shared Web Part'**.
3. The **'Confluence Space Selection'** web part editor appears. Select the required space from the **'Space'** dropdown list.
4. Select the **'Show Space List'** option:
 - If you select this option, the web part on the SharePoint page will display a dropdown menu allowing users to select a different space.
 - If you do not select this option, users will see only the page tree for the space that you selected. They will not be able to choose a different space.
5. Click **'OK'** or **'Apply'** to make the page tree show in the web part.

See our guide to [web part connections](#) for information on connecting this web part to other web parts.

Screenshot 6: A Confluence Pages Tree View web part, showing the web part's dropdown menu



Screenshot 7: The 'Confluence Space Selection' web part editor



As shown in the above screenshot, the 'Confluence Space Selection' web part editor displays the following information:

- The editor title is the Confluence space name.
- The Confluence **Host** comes from the settings in SharePoint's 'Confluence Settings' page (found under 'Site Settings').
- The list of Confluence spaces shows only those spaces that the user has permission to see, based on the Confluence space permissions.

RELATED TOPICS

[SharePoint Connector User's Guide](#)
[Configuring the SharePoint Web Part on SP 2007](#)

Using the SharePoint 2010 Web Parts

This page tells you how to embed Confluence content into SharePoint pages, when your SharePoint and Confluence sites are connected via the Confluence SharePoint Connector. The instructions on this page apply to **SharePoint 2010**.

The SharePoint Connector provides SharePoint web parts that you can use to display Confluence pages and page trees in SharePoint. Users can view the Confluence content from within SharePoint and click through from SharePoint to Confluence.



Quick guide to adding Confluence content on SharePoint pages

- Go to a web part page in SharePoint and edit the page.
- Click '**Add a Web Part**' in the zone where you want to put your Confluence web part.
- Scroll down to find the Confluence web parts:
 - Select the '**Confluence Page**' web part if you want to embed a single Confluence page.
 - Select the '**Confluence Pages Tree View**' web part if you want to embed a hierarchical tree of pages from a Confluence space.
- The web part is now part of your SharePoint page. Click the web part's dropdown menu and select '**Modify Shared Web Part**' or '**Edit Web Part**'.
- The web part editor appears. Select the required space, and the page if relevant.
- Click '**OK**'.

The rest of this page gives more details of the above procedure.

On this page:

- [Adding a SharePoint Web Part](#)
- [Using the Confluence Page Web Part](#)
 - [Hiding and Showing Page Comments](#)
- [Using the Confluence Pages Tree View Web Part](#)
- [Screenshot of SharePoint Page with Two Web Parts](#)

Adding a SharePoint Web Part

Below is a summary of how to add the Confluence web parts in SharePoint. For detailed instructions on the SharePoint side of things, please refer to the SharePoint online help.

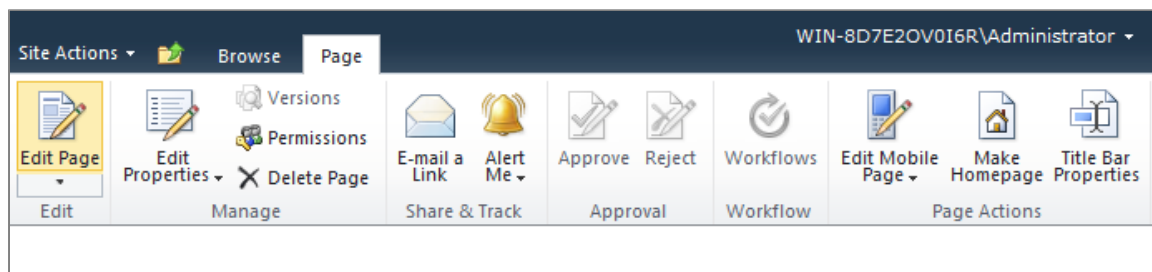
To add a SharePoint web part, you need SharePoint 'Design' permission level or better.

You can add web parts to a SharePoint 'web part page'. Many of the pages in SharePoint are web part pages, including the home page in any SharePoint site. You can also create web part pages in a document library that has the 'Web Part Page' document template. Such a document library typically has the name 'Pages'.

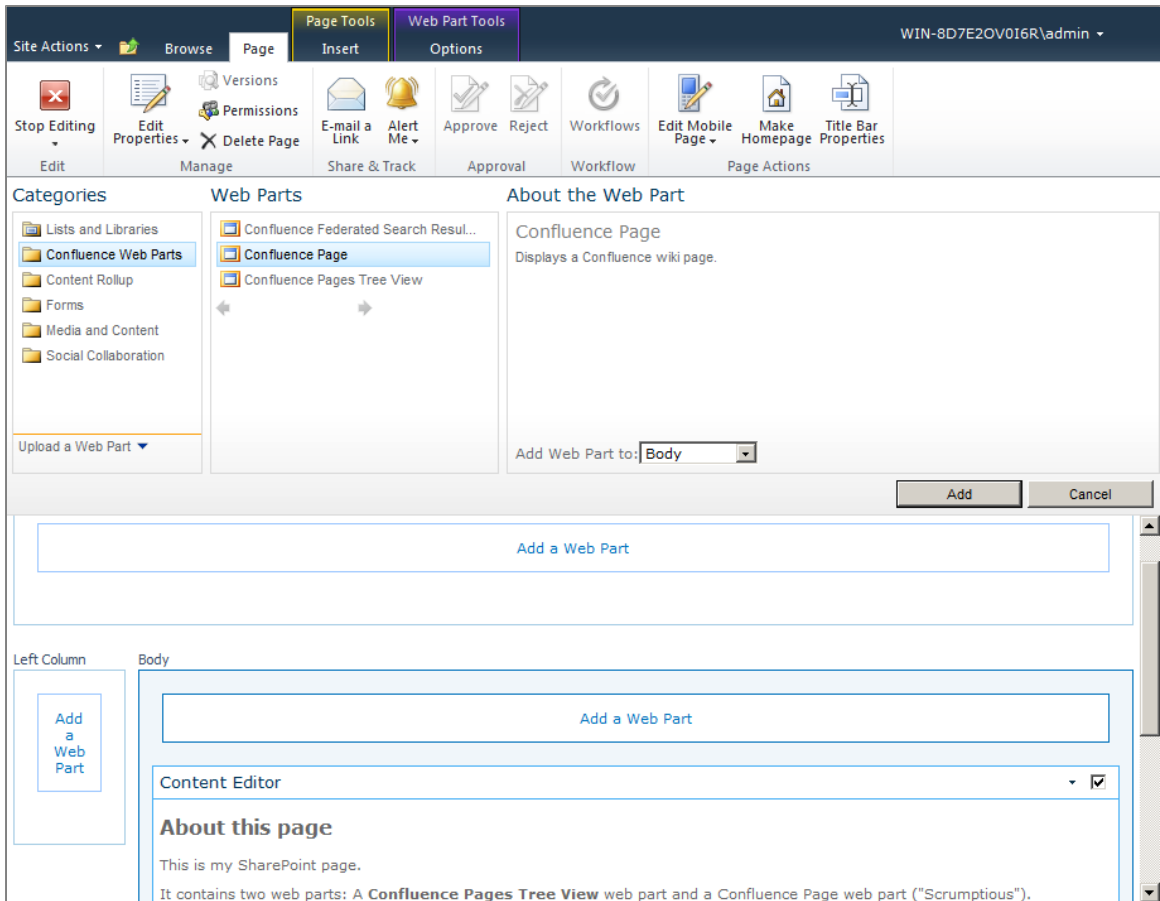
To add the Confluence web parts in SharePoint,

1. Go to a web part page in SharePoint.
2. Edit the page. (Click '**Page**' then '**Edit Page**' in the ribbon, or click '**Site Actions**' then '**Edit Page**'.)
3. The page opens in edit mode, showing the web part zones defined for the page. Click '**Add a Web Part**' in the zone where you want your web part to reside.
4. The web part selection dialogue appears. Select '**Confluence Web Parts**' in '**Categories**' column.
5. The list of Confluence web parts appears in the '**Web Parts**' column. Select the one you want. Details of each web part are below.
6. Click '**Add**'.

Screenshot 1: The 'Edit Page' option in the SharePoint ribbon



Screenshot 2: Selecting the Confluence web parts



Using the Confluence Page Web Part

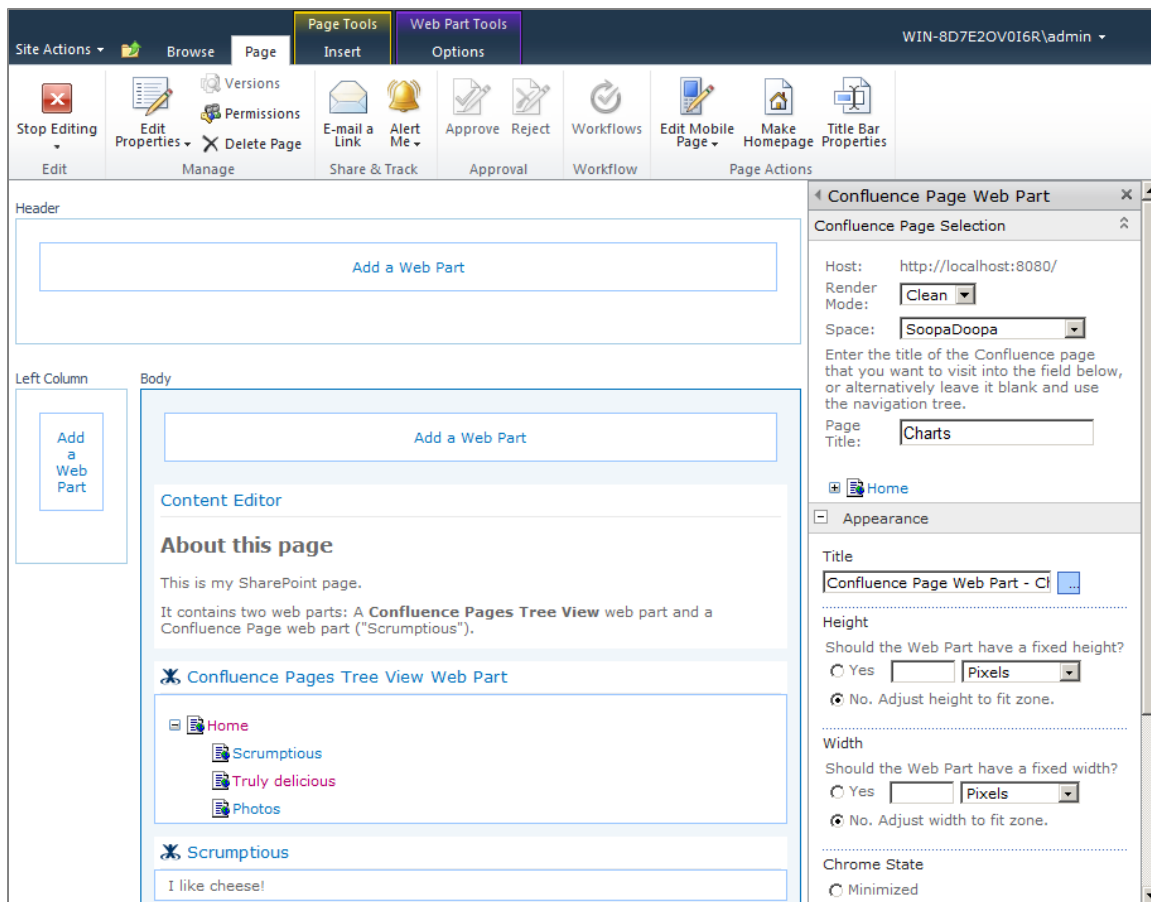
You can use the Confluence Page web part to display a specific page from Confluence in SharePoint.

To add and customise the Confluence Page web part,

1. Add the '**Confluence Page**' web part, following the instructions [above](#).
2. The web part is now part of your SharePoint page. Click the web part's dropdown menu and select '**Edit Web Part**'.
3. The '**Confluence Page**' web part editor appears on the right of the screen. Select the required space from the '**Space**' dropdown list.
4. A hierarchical (tree view) list of pages appears. Select the required page, or enter the page name into the '**Page Title**' text box.
5. Click '**OK**' or '**Apply**' to make the page show in the web part.

See our guide to [web part connections](#) for information on connecting this web part to other web parts.

Screenshot 3: The 'Confluence Page' web part editor on the right of the screen




As shown in the above screenshot, the 'Confluence Page Selection' web part editor displays the following information:

- The Confluence **Host** comes from the settings in SharePoint's 'Confluence Settings' page (found under 'Site Settings').
- The list of Confluence spaces shows only those spaces that the user has permission to see, based on the Confluence space permissions.

Hiding and Showing Page Comments

By default, displaying a Confluence page using the Confluence Page web part will also display any comments on the page.

Screenshot 4: Displaying page comments in the Confluence Page web part

 **Marketing Draft Launch Document**

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Aliquam fermentum vestibulum est. Cras rhoncus. Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Sed quis tortor. Donec non ipsum. Mauris condimentum, odio nec porta tristique, ante neque malesuada massa, in dignissim eros velit at tellus. Donec et risus in ligula eleifend consectetur. Donec volutpat eleifend augue. Integer gravida sodales leo. Nunc vehicula neque ac erat. Vivamus non nisl. Fusce ac magna. Suspendisse euismod libero eget mauris.

Ut ligula. Maecenas consequat. Aliquam placerat. Cum sociis natoque penatibus et magnis dis parturient montes, nascetur ridiculus mus. Nulla convallis. Ut quis tortor. Vestibulum a lectus at diam fermentum vehicula. Mauris sed turpis a nisl ultricies facilisis. Fusce ornare, mi vitae hendrerit eleifend, augue erat cursus nunc, a aliquam elit leo sed est. Donec eget sapien sit amet eros vehicula mollis. In sollicitudin libero in felis. Phasellus metus sem, pulvinar in, porta nec, faucibus in, ipsum. Nam a tellus. Aliquam erat volutpat.

Sed id velit ut orci feugiat tempus. Pellentesque accumsan augue at libero elementum vestibulum. Maecenas sit amet metus. Etiam molestie massa sed erat. Aenean tincidunt. Mauris id eros. Quisque eu ante, Fusce eu dolor. Aenean ultricies ante ut diam. Donec iaculis, pede eu aliquet lobortis, wisi est dignissim diam, ut fringilla eros magna a mi. Nulla vel lorem. Donec placerat, lectus quis molestie hendrerit, ante tortor pharetra risus, ac rutrum arcu odio eu tortor. In dapibus lacus nec ligula. Aenean vel metus. Nunc mattis lorem posuere felis. In vehicula tempus lacus. Phasellus arcu. Nam ut arcu. Duis eget elit id eros adipiscing dignissim.

[\[-\] Hide Comments](#) | [View All Comments](#) | Showing 6 of 6 Comments

Liz Lemon says: 14 minutes ago

What do you think about the opening paragraph, here? I think we need some catchier that really highlights the great features in this release!

[View in Confluence](#)

Jack Donaghy says: Less than a minute ago

The focus should be on the Web Part Connections enhancement (**CSI-136**), which I hope many customers will be excited we are now delivering. Actually, I tried it out myself the other day and it was pretty neat.

[View in Confluence](#)

Liz Lemon says: 11 minutes ago

OK, I've edited the opening paragraph. Web Part Connections is now the headline feature.

[View in Confluence](#)

Jack Donaghy says: 11 minutes ago

Looks good. I think we're ready to ship.

[View in Confluence](#)

Tracy Jordan says: 8 minutes ago

There's an error in the second paragraph. The SharePoint Connector doesn't actually have any integration with the International Space Station; I'm not actually sure where you got this information from?

I've removed the offending sentence... hope that's okay!

[View in Confluence](#)

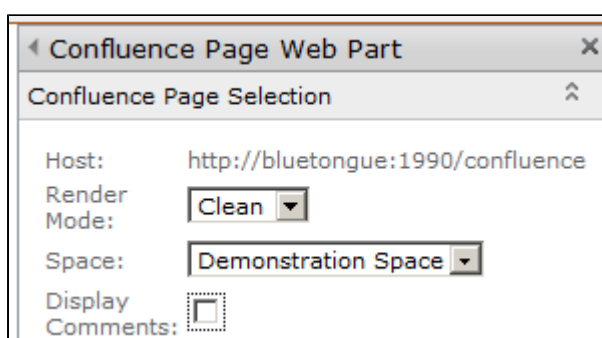
Liz Lemon says: 6 minutes ago

Haha, whoops! I think I must have been a bit tipsy when I wrote that. Thanks for fixing it up. 😊

[View in Confluence](#)

To prevent the comments from displaying, edit the web part and ensure that the '**Display Comments**' option is not selected.

Screenshot 5: Disable the 'Display Comments' option to hide any comments on the page.



Confluence Page Web Part

Confluence Page Selection

Host: http://bluetongue:1990/confluence

Render Mode: **Clean**

Space: **Demonstration Space**

Display Comments: ☐

Using the Confluence Pages Tree View Web Part

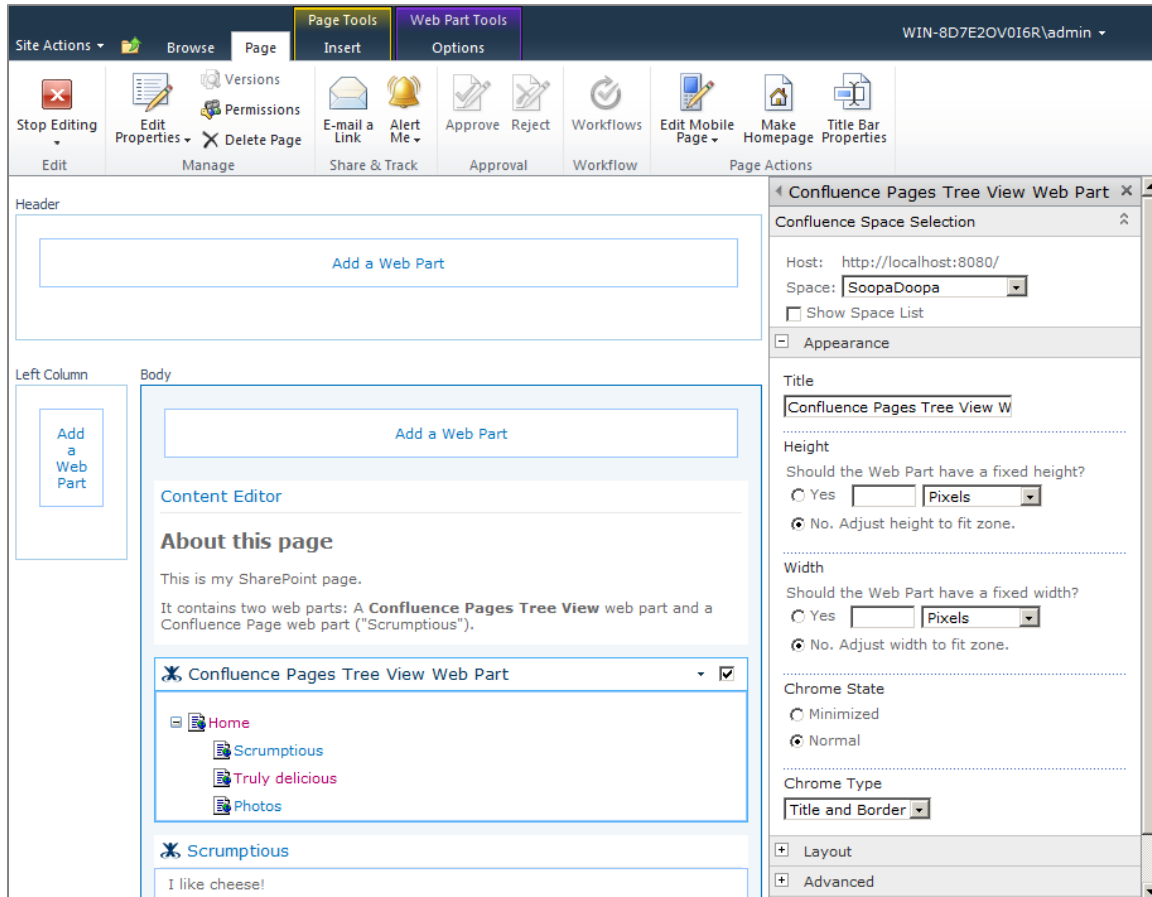
You can use the Confluence Pages Tree View web part to display a hierarchical view of pages from a specific Confluence space.

[To add and customise the Confluence Pages Tree View web part,](#)

1. Add the '**Confluence Pages Tree View**' web part, following the instructions [above](#).
2. The web part is now part of your SharePoint page. Click the web part's dropdown menu and select '**Edit Web Part**'.
3. The '**Confluence Pages Tree View**' web part editor appears on the right of the screen. Select the required space from the '**Space**' dropdown list.
4. Select the '**Show Space List**' option:
 - If you select this option, the web part on the SharePoint page will display a dropdown menu allowing users to select a different space.
 - If you do not select this option, users will see only the page tree for the space that you selected. They will not be able to choose a different space.
5. Click '**OK**' or '**Apply**' to make the page tree show in the web part.

See our guide to [web part connections](#) for information on connecting this web part to other web parts.

Screenshot 6: The 'Confluence Pages Tree View' web part editor on the right of the screen



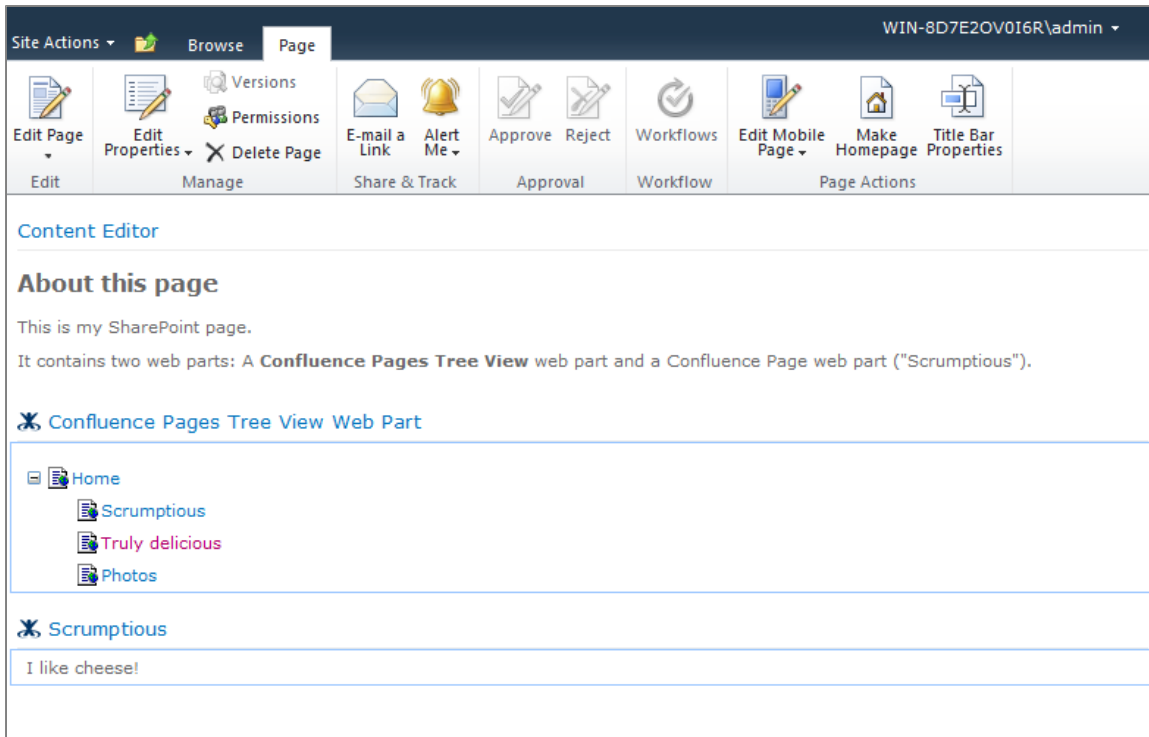
As shown in the above screenshot, the 'Confluence Space Selection' web part editor displays the following information:

- The Confluence '**Host**' comes from the settings in SharePoint's 'Confluence Settings' page (found under 'Site Settings').
- The list of Confluence spaces shows only those spaces that the user has permission to see, based on the Confluence space permissions.

Screenshot of SharePoint Page with Two Web Parts

This screenshot shows a SharePoint page containing a Confluence Web Page web part and a Confluence Pages Tree View web part.

Screenshot 7: A SharePoint page with the two Confluence web parts



RELATED TOPICS

[SharePoint Connector User's Guide](#)
[Configuring the SharePoint Web Part on SP 2010](#)

Connecting Data in your Web Parts

The Confluence SharePoint Connector supports SharePoint's [web part connections](#) for the two web parts provided by the connector:

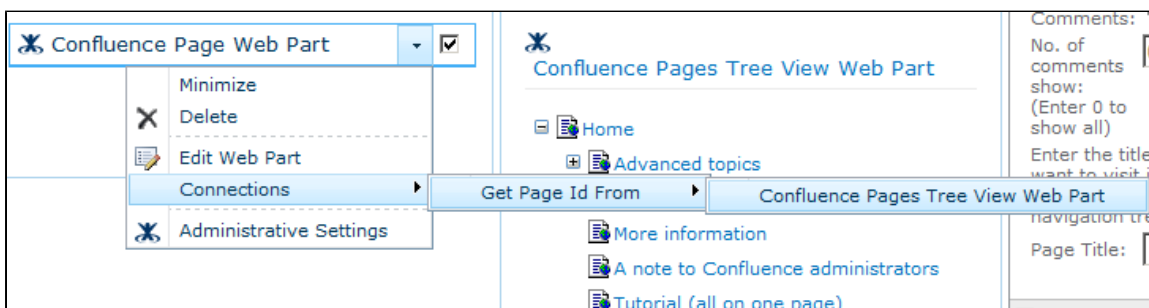
- **Confluence Pages Tree View web part:** This web part allows another web part to provide it with the space key so that it can display the hierarchy of pages for the given space.
- **Confluence Page web part:** This web part allows another web part to provide it with the Confluence page ID so that it can display the Confluence page.

 Web part connections work in the same way for both SharePoint 2007 and SharePoint 2010. The screenshots below are from SharePoint 2007, and it's easy to apply the same guidelines to SharePoint 2010.

Connecting the Pages Tree View and Page Web Parts

The most common scenario for connecting the Confluence web parts is setting up a Page web part to display the content of a page selected in a corresponding Pages Tree View web part.

Screenshot: Confluence Web Parts Connected Together



1. Create a web part page, go into edit mode on the page.
2. Add a Confluence Pages Tree View web part.
3. Confluence the tree view web part to display the pages in a specific Confluence space.
4. Add a Confluence Page web part.
5. Edit the connection of the Page web part and set its provider to the Tree View web part.
6. Save/Check-in/Publish the page.

A Simple Example using the Confluence Web Parts

A simple scenario is to use a list web part that contains the space key and/or the page ID that can be passed to the Confluence web parts. Below we show an example of this scenario. When viewing the SharePoint page, the user clicks a radio button to choose an item in the list. The list web part passes the corresponding space key and/or page ID to the web parts below the list.

Screenshot: Web Part Connections

Web Part Connection - List Connection Demonstration

Atlassian - Confluence/SharePoint Integration

Web Part Connections

	Title	Space Key	Page Id
<input checked="" type="radio"/>	Test 1 <small>NEW</small>	ds	32771
<input type="radio"/>	Test 2 <small>NEW</small>	ds	32777
<input type="radio"/>	Test 3 <small>NEW</small>	tc	425989

Demonstration Space **Tasklist**

Index

Confluence Overview

Thumbnail gallery

Tasklist

News

Creating pages and linking

Formatting Content

Source code

Search Confluence content

Using Spaces

Example Index

Email archiving

RSS Capabilities

Jira integration

More information about the tasklist macro is available at [Tasklist macro](#)

The tasklist macro comes packaged with Confluence (since version 1.3). It allows you to create lists of tasks which need to be performed and keeps track of who has completed them.

Tasks: thingsToDo **uncheck all**

Mary to preview her presentation with the team ☒ (sample.administrator)

Tony to call meeting with investors ☒ (sample.administrator)

Tony to book catering ☒ (sample.administrator)

Mary to finalize presentation with Steve ☐

Everyone relax before presentation ☐

The above was created with the following wiki markup:

```
{tasklist:thingsToDo}
Mary to preview her presentation with the team
Tony to call meeting with investors
Tony to book catering
Mary to finalize presentation with Steve
Everyone relax before presentation
{tasklist}
```

Take the following steps to reproduce the above scenario:

1. Create a SharePoint custom list with 2 fields: a space key and a page ID.
2. Create a web part page, go into edit mode on the page, and add the following to the web part page:
 - The list web part you have just created.
 - A Confluence Page web part.
 - A Confluence Pages Tree View web part.
3. Edit the connection of the Confluence Pages Tree View web part and set its provider to the appropriate field (space or page ID) from the list, as shown below.

Screenshot: Making a connection

Add a Web Part

Demonstration Space edit x

Minimize

Close

Delete

Modify Shared Web Part

☒ **Connections**

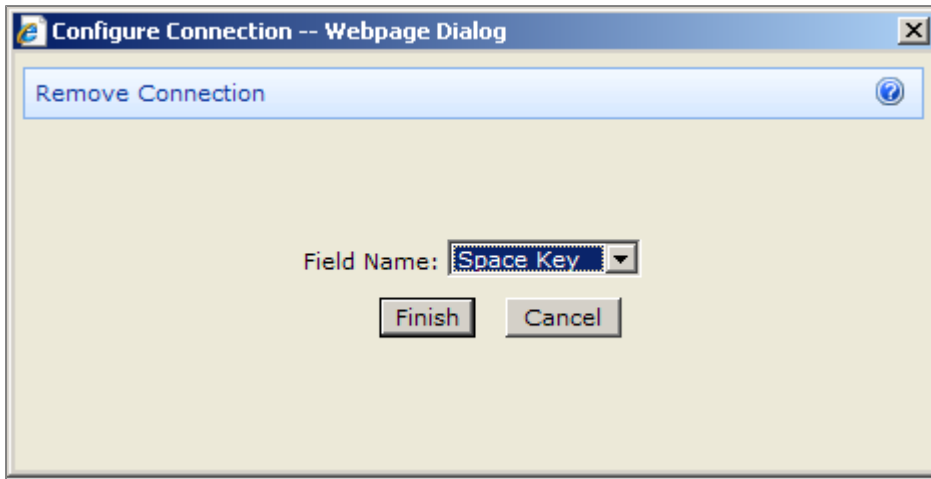
☒ **Get Space Key From**

☒ **Web Part Connections**

Administrative Settings

Formatting Content

Screenshot: Configuring the connection



Other SharePoint Web Part Connections

SharePoint provides some out-of-the-box web parts that specialise in connections, such as the [Filter Web Parts](#) that come with the Enterprise version of MOSS 2007. You can configure such a filter web part to obtain the space key or page ID from different sources and provide one of them to the Confluence SharePoint Connector web parts. Here are some of the filter web parts in MOSS Enterprise 2007:

- Business Data Catalog Filter – can provide a space key or page ID taken from a database or web service.
- Choice Filter – can provide a hard-coded choice of space keys from which the user can choose.
- Page Field Filter – looks at fields stored with the current web part page (in a Pages document library, for example) to provide their values.
- Query String Filter – can provide values from the query string.
- SQL Server 2005 Analysis Services Filter – can provide values from SSAS.
- Text Filter – allows the user to type in a value that can be passed.

Technical note: The Confluence SharePoint Connector web parts consume the `IWebPartField` interface. This is one of the interfaces provided by list web parts and filter web parts. You can create your own web part and have it provide data through this interface as well.

RELATED TOPICS

[Using the SharePoint 2007 Web Parts](#)
[Using the SharePoint 2010 Web Parts](#)

Embedding SharePoint Content into Confluence Pages

Using the Confluence SharePoint Connector, you can display SharePoint document libraries, calendars, links, discussions and more on your Confluence wiki pages. People can:

- View the SharePoint content on the Confluence wiki page.
- Click through to SharePoint to edit the SharePoint page.
- Click through straight from Confluence to edit an Office document and save it back to SharePoint.


How to embed SharePoint content into Confluence pages:

- [Using the SharePoint List Macro](#)
- [Using the SharePoint Link Macro](#)




Using the SharePoint List Macro

You can use the SharePoint List macro `{sp-list}` to display a SharePoint list on a Confluence wiki page. The macro can display most SharePoint list types.

[Screenshot: The SharePoint List macro in Confluence](#)






Page Containing a SharePoint List

 Edit
  Add
  Tools

Added by [Administrator](#), last edited by [Administrator](#) on Feb 02, 2010

This Confluence page contains the SharePoint List macro, showing the list of documents from my document library in SharePoint.

My SharePoint document library

Document Name	File Size	Modified	Author	view
 atlassian-cover-image.png	9 kb	02/02/2010 10:36 AM	MARKSPIMAGE\Administrator	View / Edit
 readme-UpdatedBySarah.txt	2 kb	02/02/2010 10:36 AM	MARKSPIMAGE\Administrator	View / Edit
 SharePoint Connector documentation.pdf	1.97 Mb	02/02/2010 12:55 PM	MARKSPIMAGE\Administrator	View / Edit

[Add Labels](#)

[Add Comment](#)


On this page:

- Usage with the Macro Browser
- Usage with the Wiki Markup Editor
 - Basic Form
 - Full Form
- Parameters
- Examples of List Types
 - Document Libraries
 - Links
 - Calendars
 - Tasks
 - Issues
 - Discussions
 - Custom Lists
- The Debug Option

Usage with the Macro Browser

The Macro Browser is a graphical menu that allows you to view the list of available Confluence macros and add them to the current page or blog post.

To insert the SharePoint List macro into a page using the Macro Browser,

1. Go to the Confluence page or blog post where you want to display the SharePoint list.
2. Click the **'Edit'** button. The page or blog post opens in edit mode.
3. Click the Macro Browser icon  on the toolbar.
4. The macro browser window opens. Find the **'SharePoint List'** macro:
 - Scroll through the list of macros, or
 - Start typing the macro name into the search box at the top right of the macro browser window. Macros with a matching name will appear in the main pane.
5. Click the macro to access its parameters and preview the macro output.
6. Enter the macro parameters. See the parameter descriptions [below](#).
7. If you would like to preview your changes, click **'Refresh'**.
8. Click **'Insert'** to add the macro to the page.

Usage with the Wiki Markup Editor**Basic Form**

**Quick guide to the SharePoint List macro**




Using the simplest form of the macro, all you need to enter is the name of your SharePoint list and the list type. The macro will display default columns, based on the list type.

- Enter the following text onto the Confluence page:

```
{sp-list:LIST NAME|LIST TYPE}
```

- Replace the text 'LIST NAME' and 'LIST TYPE' with your own values.

In the example below, we show the list of documents in a SharePoint document library. The list name is 'documents' and the list type is 'document'.

What you need to type	What you will get			
{sp-list:documents document}	Document Name	File Size	Modified	Author
	 atlassian-cover-image.png	9 kb	02/02/2010 10:36 AM	MARKSPIMAGE\Administrator
	 readme-UpdatedBySarah.txt	2 kb	02/02/2010 10:36 AM	MARKSPIMAGE\Administrator
	 SharePoint Connector documentation.pdf	1.97 Mb	02/02/2010 12:55 PM	MARKSPIMAGE\Administrator

Full Form

Make sure that you enter the entire text on a single line without any line breaks.

Parameters

Parameters are options that you can include in Confluence macros to control the content or format of the macro output. The table below lists relevant parameters for this macro.


Parameter names are different in the macro browser and in wiki markup. Below we show the macro browser parameter names in **bold** text, and the equivalent wiki markup parameters in *(bracketed)* text. If we do not show any parameter name for the wiki markup, then you should leave out the parameter name and simply include the parameter value as the first parameter, immediately after the colon (:).

Separating Multiple Parameters

In wiki markup, the parameters are separated by a pipe character (|). The SharePoint List macro has a slightly more complex format than other Confluence macros. For each parameter, you can enter multiple values separated by a comma (,) or a semi-colon (;). We give a detailed description in the table below.

Parameter	Default	Description
-----------	---------	-------------

listname (SharePoint site alias: listName)	No default	<p>The first parameter can contain either just the name of the SharePoint list ('listName') or the SharePoint site alias and the list name, separated by a colon (:). The text 'listName' is optional.</p> <p>The following example has two parameters. The first parameter contains just the list name 'documents'. (The second parameter is the list type, as described below, and is not relevant here.) For now, please look at just the first parameter before the pipe character ():</p> <div data-bbox="671 353 1417 389" style="border: 1px dashed blue; height: 16px; width: 467px; margin: 10px 0;"></div> <p>In the next example, the first parameter contains an alias 'mySharePoint' and the list name 'documents':</p> <div data-bbox="671 488 1417 524" style="border: 1px dashed blue; height: 16px; width: 467px; margin: 10px 0;"></div> <p>Here is another example with alias and list name, where the parameter name 'listName' is explicitly specified:</p> <div data-bbox="671 622 1417 658" style="border: 1px dashed blue; height: 16px; width: 467px; margin: 10px 0;"></div> <p>The SharePoint site alias is the nickname of the SharePoint server as specified in the SharePoint Admin settings. See the Confluence SharePoint plugin configuration guide. Note that this value is case sensitive – use the same capital and lower-case letters as in the plugin configuration screen.</p> <p>The listName is the name of the list in SharePoint. This value is not case sensitive.</p> <p>Specifying the full path to your list</p> <p>You must give the full path to the list. In the above example, we have assumed that the list is located at the root (top-level) SharePoint site. However, if the list is in a SharePoint site called 'mySubSite' that is a child of the root site collection, you might specify the following:</p> <div data-bbox="671 1043 1417 1079" style="border: 1px dashed blue; height: 16px; width: 467px; margin: 10px 0;"></div> <p>Displaying the contents of a document folder</p> <p>To display the contents of a folder 'my folder' within a document library, add a double forward slash(//):</p> <div data-bbox="671 1218 1417 1254" style="border: 1px dashed blue; height: 16px; width: 467px; margin: 10px 0;"></div>
(Unnamed parameter: List type)	No default	<p>Use this parameter to specify the type of the list in SharePoint. If you do not specify the columns (see below), then you must specify the list type. If you do not specify the columns, Confluence will display default columns for the given list type. The macro supports the following list types:</p> <ul style="list-style-type: none"> • doc, docs, document • link • cal, calendar • task, tasks • issue, issues • discussion, discussions <p>See the examples below.</p>

columns (columns)	If the 'list type' parameter is present and there is no 'columns' parameter, then SharePoint will display default columns for the given list type.	<p>Use this parameter to specify the columns of the SharePoint list that will be displayed on the Confluence page. If you do not specify the columns, Confluence will display default columns for the given list type. If you specify both the list type and the columns, Confluence will display the specified columns instead of the default columns.</p> <p> Use 'view' as a column name to create a link to the original SharePoint list.</p> <p>You can enter one or more columns, separated by a semi-colon (;). For each column, you can specify the column name, alias and type, separated by a comma (,). The format is:</p> <div style="border: 1px dashed blue; height: 20px; width: 460px; margin: 10px 0;"></div> <p>For example:</p> <div style="border: 1px dashed blue; height: 20px; width: 460px; margin: 10px 0;"></div> <p>The column name is a unique SharePoint 'field ID' for the column. Please refer to Frode's awesome list of Sharepoint Column Field IDs. For example, to find the field ID for the column containing the file size, go to Frode's page for F to P. As shown on the page, the field ID is <code>FileSizeDisplay</code>.</p> <p>Alternatively, you can use the 'debug' parameter to obtain a list of SharePoint field IDs. See more about the debug option below.</p> <p>The column alias will be displayed as the column header on the Confluence wiki page. You can enter any value you like here.</p> <p>The column type determines how the macro will format the value when displaying it on the Confluence page. The following values are supported:</p> <ul style="list-style-type: none"> • fileSize – Formats the column value as a file size. • author – Formats the column value as a link to the user's profile on SharePoint. • date – Formats the column value as a date in the form "MM/dd/yyyy" (ie. the "American" format). • dateTime – Formats the column value as a date and time in the form "MM/dd/yyyy hh:mm aa". • url – Formats the column value as a hyperlink. • boolean – Displays a value of 'yes' or 'no'. • percent – Formats the column value as a percentage. • doc – Formats the column value as a link to a document in the SharePoint list.
debug	False	Set this parameter to 'true' if you want to send the SharePoint SOAP response to the HTML source of the page. You can see the result by viewing the source of the page. See more below .

Examples of List Types

Below are some examples of the list types supported by the SharePoint List macro.





Document Libraries

List types: `doc`, `docs`, `document`

Using the default columns:

Specifying the columns:

Output:

Document Name	File Size	Modified	Author	view
 contract.doc	28 kb	Oct 14,2007	System Account	View / Edit
 Distributable VHD Image EULA.doc	104 kb	Oct 03,2007	System Account	View / Edit
 ReadMe.htm	37 kb	Oct 03,2007	System Account	View / Edit
 RELEASE.TXT	26 kb	Oct 03,2007	System Account	View / Edit

Links

List type: link

Using the default columns:

Specifying the columns:

Output:

URL	Comments
http://www.cnn.com , a news website	CNN reports news.
http://www.slashdot.org , News For Nerds	Lots of techie stories.
http://www.digg.com , another techie news site	stories are posted by readers and then voted up to the point where they appear on the front page.
http://www.atlassian.com , Atlassian home site	Makers of several products including Confluence, JIRA, Crowd, Crucible, Bamboo, Crowd, FishEye and a few others.

Calendars

List types: cal, calendar

Using the default columns:

Specifying the columns:

Output:

Title	Location	Start Time	End Time	All Day Event
Confluence SharePoint integration dailey standup meeting	virtual	Oct 17,2007	Aug 15,2011	no
Web 2.0	San Francisco	Oct 17,2007	Oct 19,2007	yes
Kitesurf equipment demo in Santa Monica		Oct 20,2007	Oct 20,2007	no

Tasks

List types: task, tasks

Using the default columns:

Specifying the columns:

Output:

Title	AssignedTo	Status	Priority	DueDate	Percent Complete
upgrade Confluence SharePoint connector	ATLASSIAN-SERV\administrator	Not Started	(2) Normal		-
send timesheet	Brendan Test Visitors	Not Started	(3) Low	2007-10-27 00:00:00	40%

Issues

List types: issue, issues

Using the default columns:

Specifying the columns:

Output:

Issue ID	Title	AssignedTo	Status	Priority	Due Date
1	create a Confluence SharePoint Connector demo site	Brendan Test Visitors	Active	(2) Normal	Oct 29,2007
2	build out SharePoint web service API	-	Active	(2) Normal	-
3	column chooser for sp-list macro	-	Active	(2) Normal	-

Discussions

List types: discussion, discussions

Using the default columns:

Specifying the columns:

Output:

Title	Author	Replies	Last Updated
what are the requirements to run the Confluence SharePoint Connector?	System Account	1;#2	Oct 25,2007

Custom Lists

List types: Not applicable

You can use the SharePoint List macro to display custom lists, provided that you specify the columns to be displayed.

Specifying the columns:

Output:

Title	ID	Modified	Author	view
A custom list item	1	02/02/2010	MARKSPIIMAGE\Administrator	View / Edit
Another custom list item	2	02/02/2010	MARKSPIIMAGE\Administrator	View / Edit

The Debug Option

You can add a debug parameter to your macro as follows:

This will cause the macro to write out the XML for the list that the SharePoint service returns. The XML is included in the HTML page, but is commented out. To see it, right click on the web page and select '**View Source**'. The XML will appear as part of the source, immediately after the following line:

The XML contains all the available SharePoint field IDs. This is one way of finding the values for the macro column names (see [above](#)). Note that you should strip off the prefix 'ows_' from the field name before using it as a the macro parameter. Some field names include two underscores after 'ows' instead of just one. In that case, you should strip off only one underscore.

For example:

Field ID shown in XML	Column Name to use in Macro
ows_ServerUrl	ServerUrl
ows__EditMenuTableStart	_EditMenuTableStart

RELATED TOPICS

[Working with Macros](#)
[SharePoint Connector User's Guide](#)

Using the SharePoint Link Macro

You can use the SharePoint Link macro {sp-link} to put a link on a Confluence wiki page, pointing to a SharePoint list, document or list item. When someone clicks the link, the SharePoint list or document will open. The macro supports most SharePoint list types.

On this page:


- [Usage with the Macro Browser](#)
- [Usage with the Wiki Markup Editor](#)
- [Parameters](#)

- Office Integration
- Examples of List Types
 - Document Libraries
 - Links
 - Calendars
 - Tasks
 - Issues
 - Discussions
 - Custom Lists

Usage with the Macro Browser

The 'Macro Browser' is a graphical menu that allows you to view the list of available Confluence macros and add them to the current page or blog post.

To insert the SharePoint Link macro into a page using the Macro Browser,

1. Go to the Confluence page or blog post where you want to display the SharePoint link.
2. Click the 'Edit' button. The page or blog post opens in edit mode.
3. Click the Macro Browser icon  on the toolbar.
4. The macro browser window opens. Find the 'SharePoint Link' macro:
 - Scroll through the list of macros, or
 - Start typing the macro name into the search box at the top right of the macro browser window. Macros with a matching name will appear in the main pane.
5. Click the macro to access its parameters and preview the macro output.
6. Enter the macro parameters. See the parameter descriptions below.
7. If you would like to preview your changes, click 'Refresh'.
8. Click 'Insert' to add the macro to the page.

Usage with the Wiki Markup Editor



Quick guide to the SharePoint Link macro

Using the simplest form of the macro, all you need to enter is the name of your SharePoint list or document library, and optionally the path to a document. The SharePoint Link macro will create a hyperlink on your page, pointing to the SharePoint location or file specified.

- Enter the following text onto the Confluence page to link to a list:

```
{sp-link:LIST-NAME}my hyperlinked text{sp-link}
```

Or enter the following text to link to a specific document:

```
{sp-link:LIBRARY-NAME/DOCUMENT-NAME}my hyperlinked text{sp-link}
```

- Replace the text 'LIST-NAME' with your own values for your SharePoint list name, or replace the text 'LIBRARY-NAME/DOCUMENT-NAME' with your SharePoint document library and file name.
- Replace the text 'my hyperlinked text' with the words that you want displayed as a hyperlink on the Confluence page.

In the example below, we link to a specific document in a SharePoint document library. The library name is 'documents' and the document name is 'checklist.docx'.

What you need to type	Hyperlink created
<code>{sp-link:documents/checklist.docx}a good checklist{sp-link}</code>	a good checklist

Parameters

Parameters are options that you can include in Confluence macros to control the content or format of the macro output. The table below lists relevant parameters for this macro.

Parameter names are different in the macro browser and in wiki markup. Below we show the macro browser parameter names in **bold text**, and the equivalent wiki markup parameters in *bracketed* text. If we do not show any parameter name for the wiki markup, then you should leave out the parameter name and simply include the parameter value as the first parameter, immediately after the colon (:).

Parameter	Default	Description
-----------	---------	-------------

listname (listName)	No default	<p>The first parameter may contain either the name of a SharePoint list, document library or the path to a document within a document library ('listName'). The listName may also be prefixed with a SharePoint site alias, separated by a colon (:). If a site alias is not specified, the default SharePoint site is used. The text 'listName' is optional.</p> <p>The following example creates a link to the SharePoint document library called 'documents'. The linked text is 'my link text'. When someone clicks this link, their browser will open the SharePoint document library in the SharePoint web interface:</p> <div data-bbox="400 331 1417 365" style="border: 1px dashed blue; height: 15px; margin: 10px 0;"></div> <p>Here is another example, where the parameter name 'listName' is explicitly specified. The results are the same as the previous example:</p> <div data-bbox="400 461 1417 495" style="border: 1px dashed blue; height: 15px; margin: 10px 0;"></div> <p>In the following example, we link to a specific document 'checklist.docx' within the library:</p> <div data-bbox="400 566 1417 600" style="border: 1px dashed blue; height: 15px; margin: 10px 0;"></div> <p>This final example shows how we can specify a specific SharePoint site in order to identify the location of a document:</p> <div data-bbox="400 696 1417 730" style="border: 1px dashed blue; height: 15px; margin: 10px 0;"></div>
---------------------------------	------------	--

Specifying the full path to your list

You must give the full path to the list (or library). In the above example, we have assumed that the list is located at the root (top-level) SharePoint site. However, if the list is in a SharePoint site called 'mySubSite' that is a child of the root site collection, you might specify the following:

Linking to a document folder

To link to a folder 'my folder' within a document library, add a double forward slash(//):

Office Integration

If you are using Microsoft Office integrated with SharePoint, the {sp-link} macro will make use of this integration. When someone clicks on the link created by the macro, it integrates with MS Office in the same way as SharePoint. You can check documents in and out of SharePoint and edit the document from within the Office application.

In order for the Office integration to work, you must be using Internet Explorer as the browser when accessing the Confluence page.

[Diagram: Office integration with the SharePoint Link macro](#)

Using the SharePoint Link macro to link to a SharePoint Office document directly from a Confluence page

SP Link Macro with Office integration

Added by [A. D. Ministrator](#), last edited by [A. D. Ministrator](#) on Apr 09, 2010 ([view change](#))

Macro code:

```
{sp-link:listname=test doc library/Test document.doc}Open and edit me in Word{sp-link}
```

Link created by macro:

[Open and edit me in Word](#)

Use the {sp-link} macro to put a hyperlink on a Confluence page.

Click the link to open the document in Word.

Edit the document in Word.

Save it back into SharePoint.

Test document.doc - Microsoft Word

This is a test document.

Now updating in MS Word.

Now updating it again, after turning on version control.

Now updating it in Word after clicking the sp-link macro from a Confluence page.

Save As

Save in: test doc library on markspimage

Home

test doc library

Type	Name	Modified By	Modified
Folder	Folder of awesome docs	MARKSPIMAGE\Administrator	3/31/2010 2:08 PM
File	conf-14248	MARKSPIMAGE\Administrator	3/25/2010 3:42 PM
File	cubeon	MARKSPIMAGE\Administrator	3/25/2010 3:42 PM
File	Test document	MARKSPIMAGE\Administrator	4/9/2010 3:28 PM
File	Test document2	MARKSPIMAGE\Administrator	4/9/2010 4:08 PM

File name: Test document.doc

Save as type: Word Document (*.doc)

Save Cancel

Examples of List Types

Below are some examples of the list types supported by the SharePoint Link macro.

Document Libraries

See the examples given above.

Links

Linking to a list of links:

Calendars

Linking to a calendar:

Tasks

Linking to a list of tasks:

Issues

Linking to a list of SharePoint issues:

Discussions

Linking to a list of SharePoint discussions:

Custom Lists

Linking to a custom SharePoint list:

RELATED TOPICS

[Using the SharePoint List Macro](#)
[Working with Macros](#)
[SharePoint Connector User's Guide](#)

Searching Confluence and Sharepoint Content

With the SharePoint Connector for Confluence you can find your content no matter whether the content is in SharePoint or Confluence. The search will return the same set of relevant results from across your SharePoint and Confluence sites, no matter which system you are using.

You do not need to do anything differently. With the SharePoint Connector for Confluence installed, you can use the search function as usual.

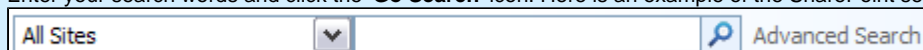
Searching in SharePoint

When you perform a search in SharePoint:

- By default, all searches will return content from both Confluence and Sharepoint.
- The results will be ordered by relevance, regardless of which system they are from.

To search for Confluence and SharePoint content from a SharePoint page,

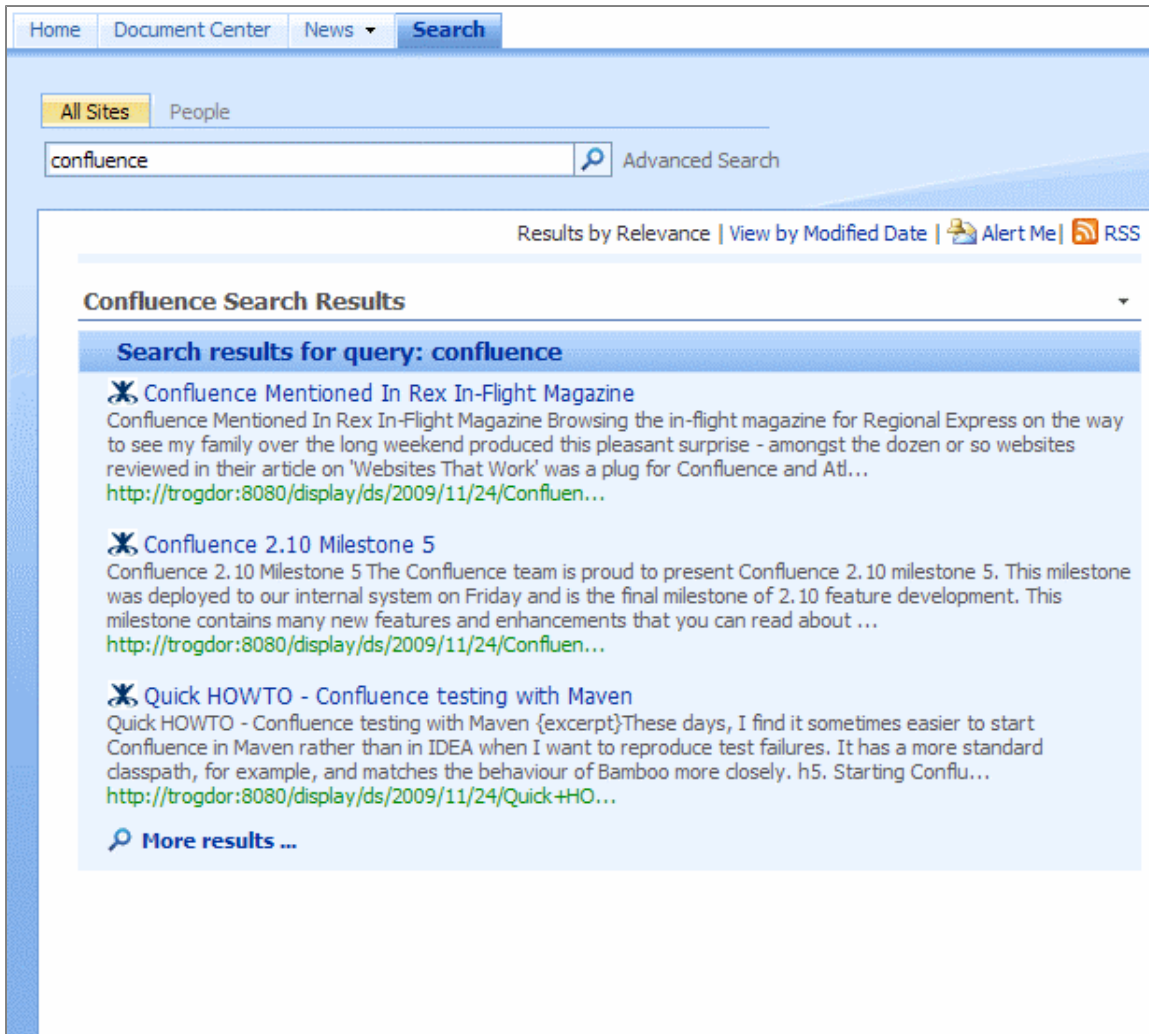
1. Select '**All Sites**' in the search scope option. Note that your search scope cannot be '**This Site**' or '**This List**'.
2. Enter your search words and click the '**Go Search**' icon. Here is an example of the SharePoint search box:



3. The search results page will open, showing the Confluence federated search results web part.

Your SharePoint administrator will configure the Confluence federated search results web part, as described in the [configuration guide](#).

[Screenshot: Search results in SharePoint](#)



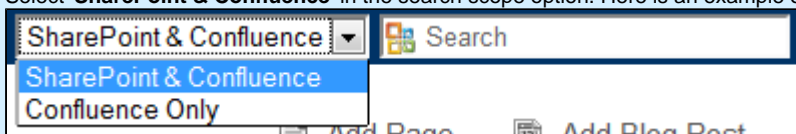
Searching in Confluence

There are two options when searching from a Confluence screen:

- Searching Confluence only
- Searching SharePoint and Confluence.

To search for Confluence and SharePoint content from a Confluence page,

1. Select '**SharePoint & Confluence**' in the search scope option. Here is an example of the Confluence search box:



2. Enter your search words and click the '**Search**' button.
3. The search will open in **SharePoint** and the results will be the same as when you perform the search from SharePoint.

The SharePoint Connector supplies a drop-down menu next to the Confluence search box that offers two options:

- '**SharePoint & Confluence**' --- If you select this option, the search results page will open in SharePoint and will show results from both SharePoint and Confluence.
- '**Confluence Only**' --- If you select this option, the search results page will open in Confluence and will show results from Confluence only.

RELATED TOPICS

Configuring the SharePoint Federated Search on SP 2007
 Configuring the SharePoint Federated Search on SP 2010

Setting your Browser Options for Automatic Login

If your browser and web applications support automatic login, you will be able to log in to your desktop computer, your intranet and the relevant web applications without being asked to log in again. Automatic login is also called pass-through sign-on, pass-through authentication, and sometimes single sign-on (SSO).



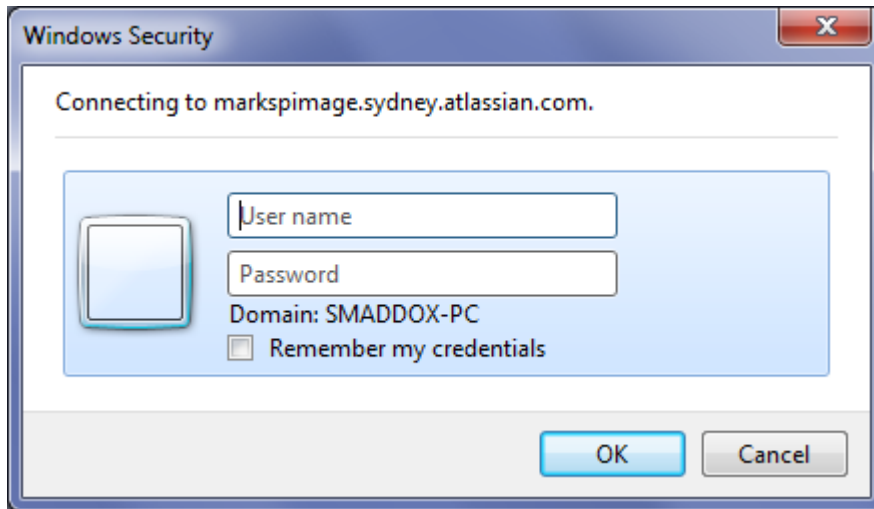
Applies to Confluence with Integrated Windows Authentication only

If unsure, ask your administrator if this information is relevant to you. It applies only if your administrator has set up Confluence to use Integrated Windows Authentication (IWA) via IIS (see documentation for [SharePoint 2007](#) and for [SharePoint 2010](#)) or Jespa (see documentation for [SharePoint 2007](#) and for [SharePoint 2010](#)).

This page tells you how to set the options in your web browser (Internet Explorer or Firefox) to enable automatic login to Confluence. This will make it much more pleasant to use the Confluence SharePoint Connector.

What happens if you do not configure your browser as described below? You will keep getting the standard browser login popup each time you access Confluence. The popup looks like this:

Screenshot: Login dialogue from Internet Explorer

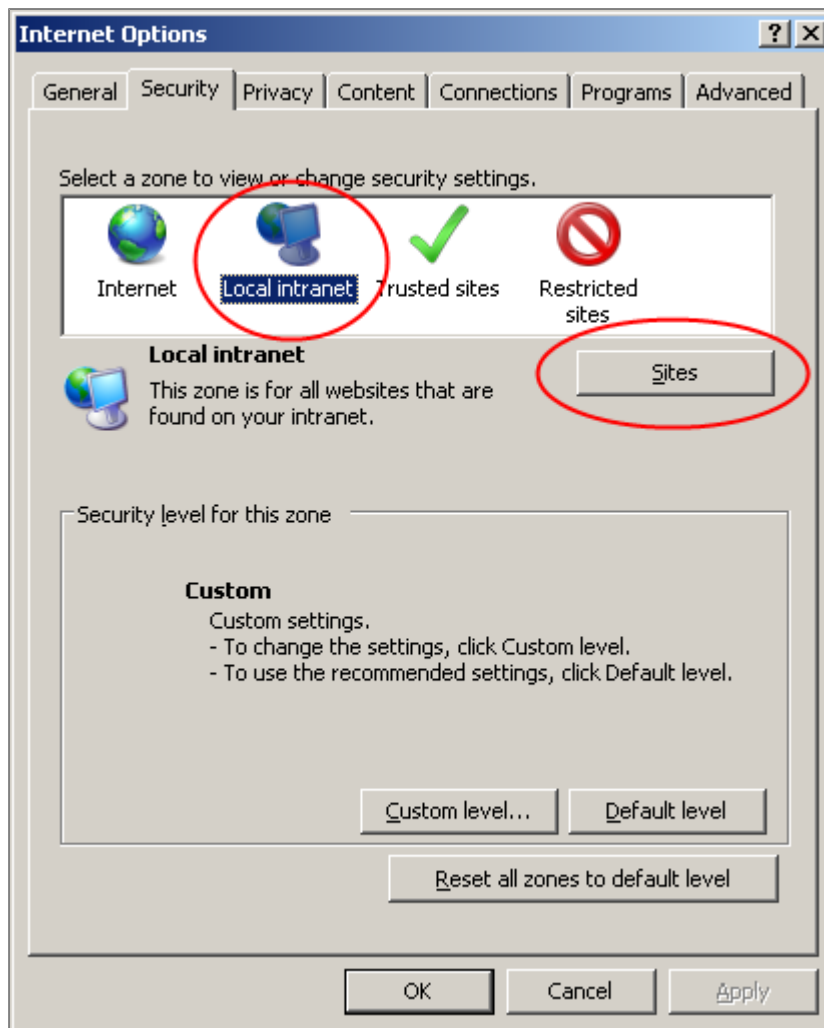


Setting up Internet Explorer

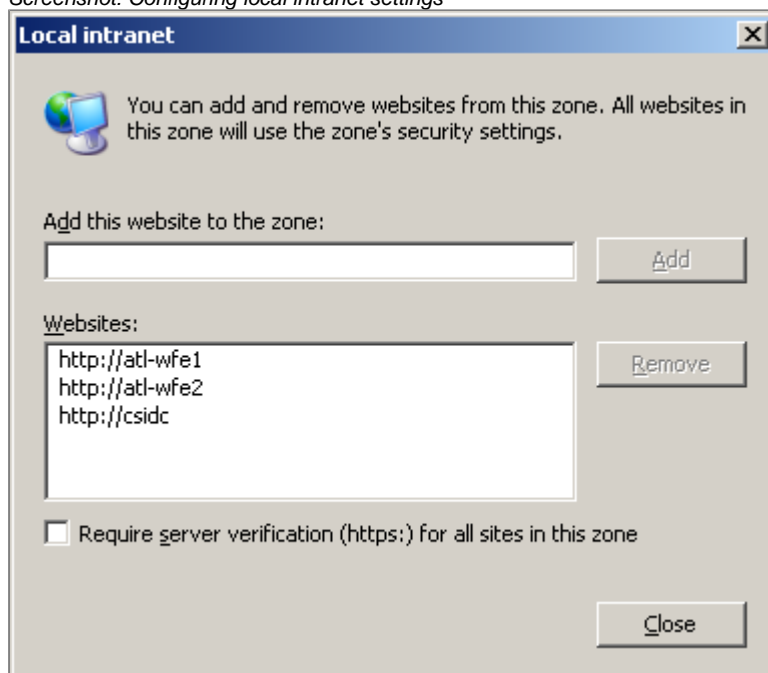
Set your options as follows for IE 6, 7 and 8.

1. Ensure that your SharePoint site(s) and Confluence site are included in the list of 'Local Intranet' sites.
 - Open Internet Explorer's **'Tools'** menu and select **'Internet Options'**.
 - Click the **'Security'** tab.
 - Select the **'Local intranet'** zone.
 - Click **'Sites'**.

Screenshot: Selecting Internet Explorer options



- Click '**Advanced**'.
 - Check the list of '**Websites**' displayed.
- Screenshot: Configuring local intranet settings*



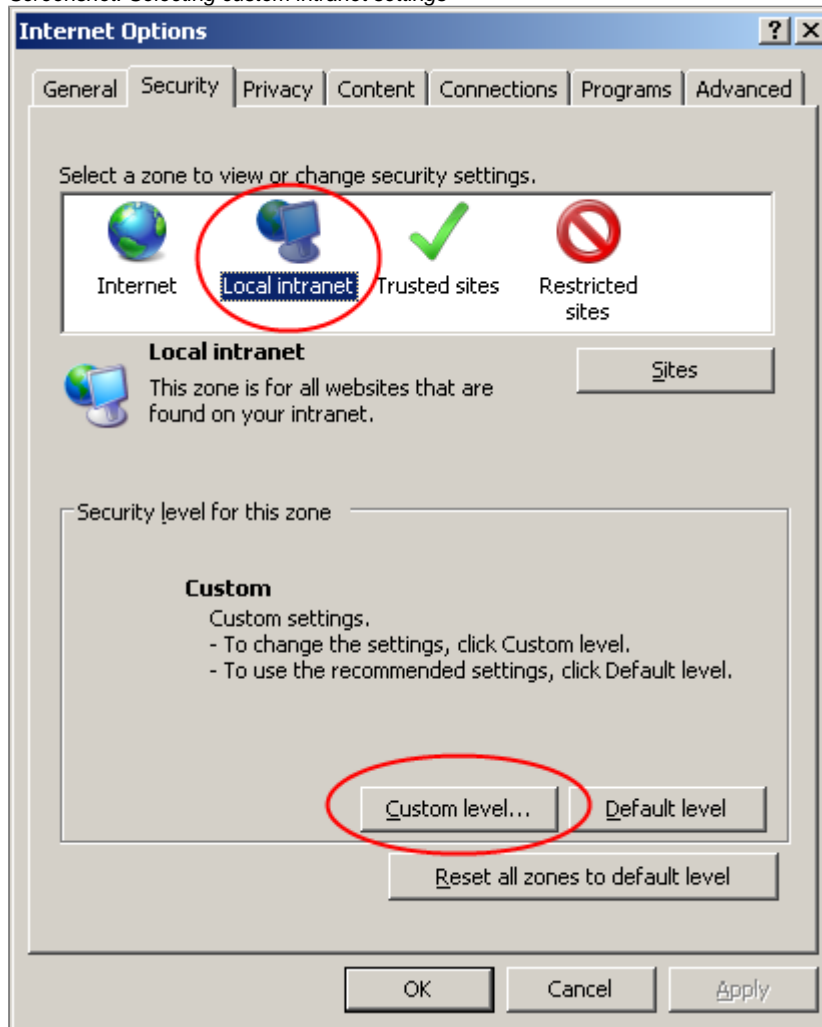
- If not already present, enter the web address (URL) of your SharePoint site(s) and your Confluence site into the textbox titled '**Add this website to the zone**' and click '**Add**' to add each address.
- Click '**Close**' to close the window showing the list of websites.
- Click '**OK**'.

2. Set automatic login in the intranet zone. If you are currently logged in with an Active Directory account, you will be automatically

logged into SharePoint and Confluence.

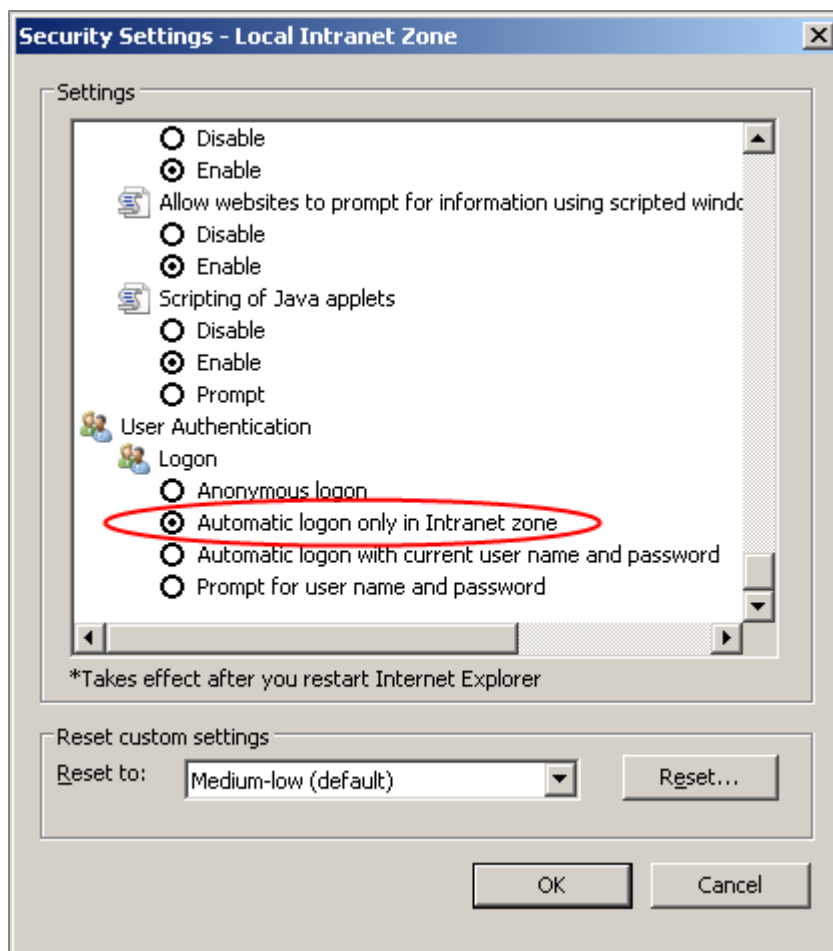
- On the **'Security'** tab, make sure the **'Local intranet'** zone is still selected and click **'Custom level'**.

Screenshot: Selecting custom intranet settings



- Scroll down to the **'User Authentication'** section (near the bottom of the list) and select the **'Automatic logon only in Intranet Zone'** option.

Screenshot: Choosing automatic 'log on' settings



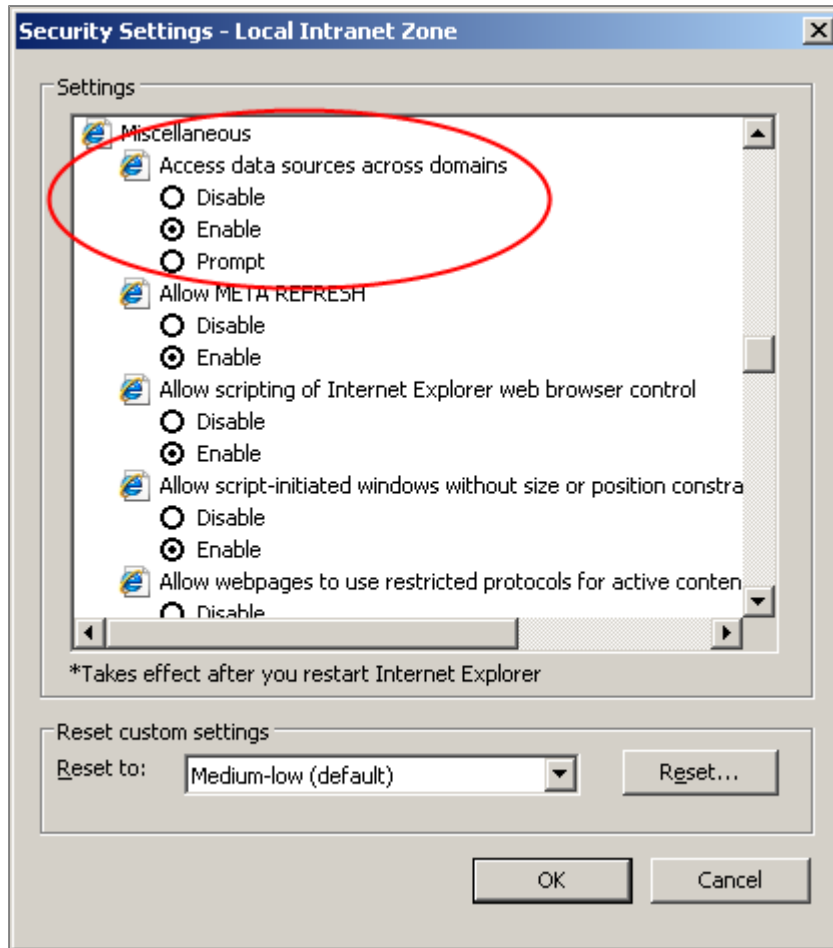
3. Set the option to access data sources across domains. This will prevent a warning message from appearing when the browser attempts to log in to Confluence.



Please check with your system administrator that this setting is acceptable for your environment

Setting this option may increase the susceptibility of your browser to XSS (cross-site scripting) attacks within the local intranet zone. This should be fine if your intranet is accessible to trusted users only.

- Scroll up to the '**Miscellaneous**' section (about half way down) and select '**Enable**' under to '**Access data sources across domains**'.
Screenshot: Enabling data source access across domains



- Click 'OK'.

4. Close all your Internet Explorer tabs and windows, and start Internet Explorer again, to ensure that the new settings take effect.

Setting up Firefox 3.x


Follow the steps below to configure automatic login in Firefox 3.x.

1. Open Firefox.
2. Type 'about:config' into your Firefox address bar.
3. When prompted, click 'I'll be careful, I promise'.
4. Find the following 'Preference Name': `network.automatic-ntlm-auth.trusted-uris`.
5. Right-click it and select 'Modify'.
6. The 'Enter string value' dialogue box will appear. Type the URL of your Confluence site and the URL(s) of your SharePoint sites, separated by commas. For example:


Another example:

Replace the one or more `sharepoint-url-x` values with the addresses of the SharePoint site(s) hosting the Confluence web parts.

7. Click 'OK'.

 Administrators may find this Mozilla Firefox documentation useful: [Deploying Firefox – Centralized Settings Management and Control](#).

Setting up Firefox 2.0

 This procedure will relax your Firefox security quite a bit. Firefox will no longer pop up a security dialogue when a cross-domain AJAX call is made. If you wish, you can set up a separate profile in Firefox to use to verify your configuration before using it with your usual profile. Please refer to the [Firefox documentation](#) for more information on managing profiles.

Follow the steps below to configure automatic login in Firefox 2.0.

1. Close all your Firefox tabs and windows. The setup procedure will not work if Firefox is open, because Firefox will overwrite the

changes you make to the `prefs.js` file.

2. Find your `prefs.js` file.
 - In Windows, it is typically located in the following location:
`C:\Documents and Settings\<YOUR_USERNAME>\ApplicationData\Mozilla\Firefox\Profiles\<YOUR_TEST_USER_PROFILE_ID>`
 - In Mac OS, it is typically located at:
`/Users/<YOUR_USERNAME>/Library/Application Support/Firefox/Profiles/<YOUR_TEST_USER_PROFILE_ID>/prefs.js`
3. Open the file for editing and add the following lines:

```
user_pref("capability.policy.confluence.XMLHttpRequest.open", "allAccess");
user_pref("capability.policy.confluence.sites", "http://<sharepoint url 1>
http://<sharepoint url 2> http://<sharepoint url n...> ");
user_pref("capability.policy.policynames", "confluence");
```

Replace the one or more `<sharepoint url>` values with the addresses of the SharePoint site(s) hosting the Confluence web parts. Please leave a space after the setting.

4. Save the `prefs.js` file.
5. Restart Firefox.

Setting the `<sharepoint url>` value(s) will limit Firefox to opening XMLHttpRequest FROM pages hosted by the respective SharePoint sites.

SharePoint Connector Administrator's Guide

This manual contains information on administering the Confluence SharePoint Connector.

- [Updating your SharePoint Connector License Details](#)
- [Configuring the SharePoint Connector NTLM Proxy](#)
- [SharePoint Connector Security Advisories](#)
- [Support Policies](#)
- [Troubleshooting the SharePoint Connector](#)

Updating your SharePoint Connector License Details

This page tells you how to update the license details for your Confluence SharePoint Connector, once you have purchased a license.

Overview of Licensing

SharePoint

You will need to comply with Microsoft's licensing requirements for SharePoint itself:

- SharePoint 2007: If you have Microsoft Office SharePoint Server (MOSS), you must buy a license from Microsoft. Windows SharePoint Services (WSS) 3.0 is free.
- SharePoint 2010: If you have SharePoint Server 2010, you must buy a license from Microsoft. SharePoint Foundation 2010 is free.

See our guide to the [SharePoint versions and editions](#).

Confluence

Each Confluence installation must be licensed with Atlassian. Cluster nodes are licensed separately. A 4-node cluster needs four Confluence licenses.

See the [Confluence documentation on licensing](#) and see our website for [Confluence pricing](#).

The Confluence SharePoint Connector

The SharePoint Connector must also be licensed with Atlassian.

- You must have a single license for the SharePoint Connector for every Confluence installation (or cluster node in an installation) that integrates with SharePoint.
- If you have one Confluence installation, you only need one license for the Confluence SharePoint Connector even if several SharePoint farms, web applications or sites are connecting to your Confluence installation.

See our website for [pricing and license details](#).

Applying your SharePoint Connector License Key

To update your SharePoint Connector license details:

1. Go to the Confluence '**Administration Console**'. To do this:
 - Open the '**Browse**' menu and select '**Confluence Admin**'. The 'Administration Console' view will open.
2. Click '**SharePoint Admin**' in the 'Administration' section of the left-hand navigation panel.
3. The '**SharePoint Admin**' screen appears. Scroll down to the licensing section and copy your license key into the '**License**' text box.
4. Click '**Save License**'.

Screenshot: The licensing section of the Confluence 'SharePoint Admin' page

You can use the form below to update the SharePoint plugin license.

Organisation	qa
Date Purchased	May 18, 2010
License Type	SharePoint: Evaluation
License	<div style="border: 1px solid #ccc; height: 100px; width: 100%;"></div>

RELATED TOPICS

[SharePoint Connector Administrator's Guide](#)
[Installing the SharePoint Connector](#)

Configuring the SharePoint Connector NTLM Proxy

This page gives information on configuring the SharePoint Connector's NTLM SOAP proxy.

Overview

The SharePoint Connector NTLM proxy is a .NET proxy that makes it possible for Confluence to communicate with SharePoint using the full range of Integrated Windows Authentication methods, including:

- NTLM
- NTLMv2
- Kerberos

For details of the full authentication configuration, see the guide to accessing SharePoint using Integrated Windows Authentication with [SharePoint 2007](#) and [SharePoint 2010](#)

The proxy only works when Confluence is run on a Windows server. If the proxy causes problems, you can disable it. You can also change the port on which the proxy listens for requests.

Defaults:

- The proxy is **enabled** by default when Confluence is running on a Windows server.
- The proxy listens on **port 56000** by default.

Effects of Disabling the Proxy

If you disable the proxy, then Confluence will only be able to communicate with SharePoint using **NTLM**. It will not be able to use NTLMv2 or Kerberos.

Configuring the Proxy

To enable, disable and configure the NTLM proxy:

1. Go to the Confluence '**Administration Console**'. To do this:
 - Open the '**Browse**' menu and select '**Confluence Admin**'. The 'Administration Console' view will open.
2. Click '**Plugins**' in the 'Configuration' section of the left-hand navigation panel.
3. The '**Plugin Manager**' screen appears. Click '**SharePoint Plugin**' in the list of installed plugins.

4. The details for the SharePoint Plugin appear, as shown below. Click '**Configure**' next to '**Windows NTLM SOAP Proxy Manager**'.
Screenshot: Confluence plugin manager showing details of the SharePoint Plugin

The screenshot shows the 'Plugin Manager' interface. On the left is a sidebar with navigation links: Configuration (General Configuration, Daily Backup Admin, Manage Referrers), Plugins (Plugin Repository, Languages, Shortcut Links, External Gadgets, Global Templates, Import Templates, Mail Servers, User Macros, JIRA Issues Icon Mappings, Attachment Storage, Spam Prevention, PDF Export Language Support, Default Space Content, Configure Whitelist, Office Connector Configuration, WebDAV Configuration), Look and Feel (Themes, Colour Scheme, Layouts, Stylesheet, Global Logo, Custom HTML), and Administration (Backup & Restore, Content Indexing, Mail Queue, Cache Statistics). The main area is titled 'Manage Plugins' and includes a 'Scan' button for new plugins and an 'Upload' button for existing ones. A yellow banner states: 'You can find and install more plugins from the [plugin repository](#).' Below this is the 'Installed Plugins' section. The 'SharePoint Plugin' is highlighted, showing its vendor as 'Atlassian Software Systems' and version as '1.2-RC3'. A description states: 'A plugin which offers integration with SharePoint'. There are three links: 'Configure plugin', 'Disable plugin', and 'Uninstall plugin'. A table lists various sub-plugins with their status and actions:

Plugin Name	Description	Action
Configuration Manager	Internal module for retrieving configuration information	Disable
Web Service Stub Factory	Factory to create web service stubs to connect to Sharepoint	Disable
Windows NTLM SOAP Proxy Manager	Manages a simple proxy executable that allows Confluence on Windows to communicate with SharePoint using LM, NTLM, NTLMv2 or Kerberos.	Configure Disable
Caching Web Service Stub Factory	Layer to cache web service stubs	Disable
SharePoint Web Service Factory	Factory to create accessors to connect to Sharepoint	Disable
State Listener	Performs initialisation and cleanup of the plugin when it is enabled/disabled.	Disable
sp-list	Macro to query and output a SharePoint list to Confluence	Disable
sp-config-util	Internal macro for querying SharePoint Connector configuration within the theme template.	Disable
sp-config	Internal macro for querying SharePoint Connector configuration within the theme	Disable

5. The '**SharePoint Connector NTLM Proxy**' screen appears, as shown below. Enable, disable or configure the proxy as required.
Screenshot: Confluence NTLM proxy configuration

The screenshot shows the 'Proxy Configuration' screen. It includes a description: 'Configure the behaviour of the SharePoint Connector's NTLM SOAP Proxy, which allows Confluence to communicate with SharePoint using the full range of Windows authentication methods (eg. NTLMv2, Kerberos). This feature is only functional when Confluence is run on a Windows server and Microsoft .NET Framework 2.0 is installed on the Confluence server.' Below this is a table with configuration options:

Proxy State	Enabled [Disable]
Confluence Server Compatibility	Proxy is compatible with your Confluence Server.
Current Status	Proxy is running; no problems detected.
Debug Logging	Debug Logging is disabled. [Enable]
Listen Port	<input type="text" value="56000"/> Update

At the bottom, there is a link: 'Go to [SharePoint Admin](#)'.

6. Click '**Update**' to save the changes.

RELATED TOPICS

Access SharePoint using Integrated Windows Authentication (NTLM Only) with SP 2007
 Access SharePoint using Integrated Windows Authentication (NTLM Only) with SP 2010

SharePoint Connector Security Advisories

As a public-facing web application, application-level security of the Confluence SharePoint Connector is important. This document answers a number of questions that commonly arise when customers ask us about the security of our product.



This document is for system administrators looking to evaluate the security of the Confluence SharePoint Connector. This section only addresses overall application security. It does not address any internal security models (such as user/group management and content permissions).

On this page:

- [Finding and Reporting a Security Vulnerability](#)
- [Publication of Confluence SharePoint Connector Security Advisories](#)
- [Severity Levels](#)
- [Our Patch Policy](#)
- [Published Security Advisories](#)

Finding and Reporting a Security Vulnerability

Atlassian's approach to releasing patches is detailed in [How to Report a Security Issue](#).

Publication of Confluence SharePoint Connector Security Advisories

Atlassian's approach to publishing security advisories is detailed in [Security Advisory Publishing Policy](#).

Severity Levels

Atlassian's scale for measuring security issues is detailed in [Severity Levels for Security Issues](#).

Our Patch Policy

Atlassian's approach to releasing patches is detailed in our [Security Patch Policy](#).

Published Security Advisories

- [SharePoint Connector Security Advisory 2010-01-18](#)
- [SharePoint Connector Security Advisory 2010-11-29](#)

SharePoint Connector Security Advisory 2010-01-18

In this advisory:

- [XSS Vulnerability in the SharePoint List Macro](#)
 - [Severity](#)
 - [Risk Assessment](#)
 - [Risk Mitigation](#)
 - [Vulnerability](#)
 - [Fix](#)

XSS Vulnerability in the SharePoint List Macro

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 when using the SharePoint List macro on a page or blog post.

- 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 that you upgrade your Confluence SharePoint Connector 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 to your SharePoint site until you have applied the necessary upgrade. For even tighter control, you could restrict access to trusted groups.

Vulnerability

An attacker can execute their own rogue JavaScript code via the SharePoint List macro. All previous versions of the SharePoint Connector are affected by this vulnerability. The fix is available in Confluence SharePoint Connector 1.1. For more information, please refer to [CSI-501](#).

Fix

This issue has been fixed in Confluence SharePoint Connector 1.1 (see the [release notes](#)). Please refer to the [SharePoint Connector 1.1 Upgrade Notes](#) for further information on upgrading the Confluence SharePoint Connector.

Note that the SharePoint Connector 1.1 requires **Confluence 2.8.0 or later**. If you are using **Confluence 2.7.4 or earlier** and are unable to upgrade, please contact [our support team](#) for assistance in addressing the vulnerability.

SharePoint Connector Security Advisory 2010-11-29

In this advisory:

- [Security Vulnerability in Confluence Permission Checker RPC Plugin](#)
 - [Severity](#)
 - [Risk Assessment](#)
 - [Vulnerability](#)
 - [Risk Mitigation](#)
 - [Fix](#)

Security Vulnerability in Confluence Permission Checker RPC Plugin

Severity

Atlassian rates the severity level of this vulnerability 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 vulnerability in the Permission Checker RPC plugin, which is installed by default on all Confluence instances running the SharePoint Connector for Confluence. This vulnerability allows an attacker to access the wiki markup and/or rendered HTML of all Confluence pages in all spaces, even if permissions are applied which would only allow access to a specific sub-set of users.

Vulnerability

The table below describes the versions of the Permission Checker RPC plugin and SharePoint Connector affected by the vulnerability.

Confluence Feature	Affected Permission Checker RPC Plugin Versions	Affected SharePoint Connector Versions	Fixed Permission Checker RPC Plugin Version	Issue Tracking
Global, space and page-level permissions	1.0 – 1.2.1	1.0 – 1.2.1	1.2.2	CSI-677

Risk Mitigation

We recommend that you upgrade your Permission Checker RPC plugin to the latest version in order to fix this vulnerability.

We strongly advise that you disable the [remote API](#) 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

Version 1.2.2 of the Permission Checker RPC plugin fixes this issue. You can download this version from the [Atlassian Plugin Exchange](#). Alternatively, you can install the latest version of the plugin through the Confluence Administration Console. See the guide to [installing plugins](#).

Support Policies

Welcome to the support policies index page. Here, you'll find information about how Atlassian Support can help you and how to get in touch

with our helpful support engineers. Please choose the relevant page below to find out more.

- [Bug Fixing Policy](#)
- [How to Report a Security Issue](#)
- [New Features Policy](#)
- [Patch Policy](#)
- [Security Advisory Publishing Policy](#)
- [Security Patch Policy](#)
- [Severity Levels for Security Issues](#)

To request support from Atlassian, please raise a support issue in our online support system. To do this, visit support.atlassian.com, log in (creating an account if need be) and create an issue under Confluence. Our friendly support engineers will get right back to you with an answer.

Bug Fixing Policy

Summary

- Atlassian Support will help with workarounds and bug reporting.
- Critical bugs will generally be fixed in the next maintenance release.
- Non critical bugs will be scheduled according to a variety of considerations.



Raising a Bug Report

Atlassian Support is eager and happy to help verify bugs — we take pride in it! Please open a support request in our [support system](#) providing as much information as possible about how to replicate the problem you are experiencing. We will replicate the bug to verify, then lodge the report for you. We'll also try to construct workarounds if they're possible.

Customers and plugin developers are also welcome to open bug reports on our issue tracking systems directly. Use <http://jira.atlassian.com> for the stand-alone products and <http://studio.atlassian.com> for JIRA Studio.

When raising a new bug, you should rate the priority of a bug according to our [JIRA usage guidelines](#). Customers [should watch](#) a filed bug in order to receive e-mail notification when a "Fix Version" is scheduled for release.

How Atlassian Approaches Bug Fixing

Maintenance (bug fix) releases come out more frequently than major releases and attempt to target the most critical bugs affecting our customers. The notation for a maintenance release is the final number in the version (ie the 1 in 3.0.1).

If a bug is critical (production application down or major malfunction causing business revenue loss or high numbers of staff unable to perform their normal functions) then it will be fixed in the next maintenance release provided that:

- The fix is technically feasible (i.e. it doesn't require a major architectural change).
- It does not impact the quality or integrity of a product.

For non-critical bugs, the developer assigned to fixing bugs prioritises the non-critical bug according to these factors:

- How many of our supported configurations are affected by the problem.
- Whether there is an effective workaround or patch.
- How difficult the issue is to fix.
- Whether many bugs in one area can be fixed at one time.

The developers responsible for bug fixing also monitor comments on existing bugs and new bugs submitted in JIRA, so you can provide feedback in this way. We give high priority consideration to [security issues](#).

When considering the priority of a non-critical bug we try to determine a 'value' score for a bug which takes into account the severity of the bug from the customer's perspective, how prevalent the bug is and whether roadmap features may render the bug obsolete. We combine this with a complexity score (i.e. how difficult the bug is). These two dimensions are used when developers self serve from the bug pile.

Further reading

See [How to Get Legendary Support from Atlassian](#) for more support-related information.

How to Report a Security Issue

Finding and Reporting a Security Vulnerability

If you find a security bug in the product, please open an issue on <http://jira.atlassian.com> in the relevant project.

- Set the priority of the bug to 'Blocker'.
- Provide as much information on reproducing the bug as possible.
- Set the security level of the bug to 'Developer and Reporters only'.

All communication about the vulnerability should be performed through JIRA, so that Atlassian can keep track of the issue and get a patch out as soon as possible.



If you discover a security vulnerability, please attempt to create a test case that proves this vulnerability locally before opening either a bug or a support issue. When creating an issue, please include information on how the vulnerability can be reproduced; see <http://confluence.atlassian.com/display/DOC/Bug+Fixing+Policy> for general bug reporting guidelines. We will prioritise fixing the reported vulnerability if your report has information on how the vulnerability can be exploited.

Further reading

See [How to Get Legendary Support from Atlassian](#) for more support-related information.

New Features Policy

Summary

- We encourage and display customer comments and votes openly in our issue tracking systems, <http://jira.atlassian.com> and <http://studio.atlassian.com>.
- We do not publish roadmaps.
- Product Managers review our most popular voted issues on a regular basis.
- We schedule features based on a variety of factors.
- Our [Atlassian Bug Fixing Policy](#) is distinct from our Feature Request process.
- Atlassian provides consistent updates on the top 20 feature/improvement requests (in our issue tracker systems).

How to Track what Features are Being Implemented

When a new feature or improvement is scheduled, the 'fix-for' version will be indicated in the JIRA issue. This happens for the upcoming release only. We maintain roadmaps for more distant releases internally, but because these roadmaps are often pre-empted by changing customer demands, we do not publish them.

How Atlassian Chooses What to Implement

In every [major release](#) we *aim* to implement highly requested features, but it is not the only determining factor. Other factors include:

- **Direct feedback** from face to face meetings with customers, and through our support and sales channels.
- **Availability of staff** to implement features.
- **Impact** of the proposed changes on the application and its underlying architecture.
- How **well defined** the requested feature is (some issues gain in popularity rapidly, allowing little time to plan their implementation).
- Our long-term **strategic vision** for the product.

How to Contribute to Feature Development

Influencing Atlassian's release cycle

We encourage our customers to vote on feature requests in JIRA. The current tally of votes is available online in our issue tracking systems, <http://jira.atlassian.com> and <http://studio.atlassian.com>. Find out if your improvement request [already exists](#). If it does, please vote for it. If you do not find it, [create a new feature or improvement request](#) online.

Extending Atlassian Products

Atlassian products have powerful and flexible extension APIs. If you would like to see a particular feature implemented, it may be possible to develop the feature as a plugin. Documentation regarding the [plugin APIs](#) is available. Advice on extending either product may be available on the user mailing-lists, or at our community [forums](#).

If you require significant customisations, you may wish to get in touch with our [partners](#). They specialise in extending Atlassian products and can do this work for you. If you are interested, please [contact us](#).

Further reading

See [How to Get Legendary Support from Atlassian](#) for more support-related information.

Patch Policy

Patch Policy

Atlassian will only provide software patches in extremely unusual circumstances. If a problem has been fixed in a newer release of the product, Atlassian will request that you upgrade your instance to fix the issue. If it is deemed necessary to provide a patch, a patch will be provided for the current release and the last maintenance release of the last major version (e.g. JIRA 3.13.5) only.

Patches are issued under the following conditions:

- The bug is critical (production application down or major malfunction causing business revenue loss or high numbers of staff unable to perform their normal functions).
- A patch is technically feasible (i.e., it doesn't require a major architectural change)
OR
- The issue is a security issue, and falls under our [Security Policy](#).

Atlassian does not provide patches for non-critical bugs.

Provided that a patch does not impact the quality or integrity of a product, Atlassian will ensure that patches supplied to customers are added to the next maintenance release. Customers **should watch** a filed bug in order to receive e-mail notification when a "Fix Version" is scheduled for release.

Patches are generally attached to the relevant <http://jira.atlassian.com> issue.

Further reading

See [How to Get Legendary Support from Atlassian](#) for more support-related information.

Security Advisory Publishing Policy

Publication of Security Advisories

When a security vulnerability in an Atlassian product is discovered and resolved, Atlassian will inform customers through the following mechanisms:

- We will post a security advisory in the latest documentation of the affected product at the same time as releasing a fix for the vulnerability. This applies to all security advisories, including severity levels of critical, high, medium and low.
- We will send a copy of all security advisories to the **'Technical Alerts' mailing list** for the product concerned.
Note: To manage your email subscriptions and ensure you are on this list, please go to my.atlassian.com and click 'Email Prefs' near the top right of the page.
- If the person who reported the vulnerability wants to publish an advisory through some other agency, such as [CERT](#), we will assist in the production of that advisory and link to it from our own.

Early warning of critical security vulnerabilities:

- If the vulnerability is rated critical (see our criteria for setting [severity levels](#)) we will send an early warning to the 'Technical Alerts' mailing list approximately one week before releasing the fix. This early warning is in addition to the security advisory itself, described above.
- However, if the vulnerability is publicly known or being exploited, we will release the security advisory and patches as soon as possible, potentially without early warning.

Further reading

See [How to Get Legendary Support from Atlassian](#) for more support-related information.

Security Patch Policy

Product Security Patch Policy

Atlassian makes it a priority to ensure the customers' systems cannot be compromised by exploiting vulnerabilities in Atlassian products.

Scope

This page describes when and how we release security patches and security upgrades for our products. It does not describe the whole of disclosure process that we follow. It also excludes Studio, since Studio will always be patched by Atlassian without additional notifications.

Critical vulnerabilities

When a **Critical** security vulnerability is discovered by Atlassian or reported by a third party, Atlassian will do all of the following:

- Issue a new, fixed release for the current version of the affected product as soon as possible, usually in a few days.
- Issue a binary patch for the current release.
- Issue a binary patch for the latest maintenance release of the previous version of the product.
- Patches for older versions or releases normally will not be issued.

Patches will be attached to the relevant JIRA issue. You can use these patches as a "stop-gap" measure until you upgrade your installation in order to fully fix the vulnerability.

Non-critical vulnerabilities

When a security issue of a **High, Medium or Low** severity is discovered, Atlassian will do all of the following:

- Include the fix into the next scheduled release, both for the current and maintenance versions.
- Where practical, provide new versions of plugins or other components of the product that can be upgraded independently.

You should upgrade your installation in order to fix the vulnerability.

Other information

Severity level of vulnerabilities is calculated based on [Severity Levels for Security Issues](#).

Visit our general [Atlassian Patch Policy](#) as well.

Examples

Example 1: A critical severity vulnerability is found in a (hypothetical current release) JIRA 5.3.2. The last bugfix release in 5.2.x branch was 5.2.3. In this case, a patch will be created for 5.3.2 and 5.2.3. In addition, new bugfix releases, 5.3.3 and 5.2.4, which are free from this vulnerability, will be created in a few days.

Example 2: A high or medium severity vulnerability is found in the same release as in the previous example. The fix will be included into the currently scheduled releases 5.3.3 and 5.2.4. Release schedule will not be brought forward and no patches will be issued. If the vulnerability is in a plugin module, then a plugin upgrade package may still be supplied.

Further reading

See [How to Get Legendary Support from Atlassian](#) for more support-related information.

Severity Levels for Security Issues

Severity Levels

Atlassian security advisories include a severity level. This severity level is based on our self-calculated CVSS score for each specific vulnerability. CVSS is an industry standard vulnerability metric. You can learn more about CVSS at [FIRST.org](#) web site.

CVSS scores are mapped into the following severity ratings:

- Critical
- High
- Moderate
- Low

An approximate mapping guideline is as follows:

CVSS score range	Severity in advisory
0 – 2.9	Low
3 – 5.9	Medium
6.0 – 7.9	High
8.0 – 10.0	Critical

Below is a summary of the factors which illustrate types of vulnerabilities usually resulting in a specific severity level. Please keep in mind that this rating does not take into account details of your installation.

Severity Level: Critical

Vulnerabilities that score in the Critical range usually include:

- Exploitation of the vulnerability results in root-level compromise of servers or infrastructure devices.
- The information required in order to exploit the vulnerability, such as example code, is widely available to attackers.
- Exploitation is usually straightforward, in the sense that the attacker does not need any special authentication credentials or knowledge about individual victims, and does not need to persuade a target user, for example via social engineering, into performing any special functions.

For critical vulnerabilities, is advised that you patch or upgrade as soon as possible, unless you have other mitigating measures in place. For example, if your installation is not accessible from the Internet, this may be a mitigating factor.

Severity Level: High

Vulnerabilities that score in the High range usually have the following characteristics:

- The vulnerability is difficult to exploit.
- Exploitation does not result in elevated privileges.
- Exploitation does not result in a significant data loss.

Severity Level: Moderate

Vulnerabilities that score in the Moderate range usually have the following characteristics:

- Denial of service vulnerabilities that are difficult to set up.
- Exploits that require an attacker to reside on the same local network as the victim.
- Vulnerabilities that affect only nonstandard configurations or obscure applications.
- Vulnerabilities that require the attacker to manipulate individual victims via social engineering tactics.
- Vulnerabilities where exploitation provides only very limited access.

Severity Level: Low

Vulnerabilities in the Low range typically have very little impact on an organisation's business. Exploitation of such vulnerabilities usually requires local or physical system access.

Further reading

See [How to Get Legendary Support from Atlassian](#) for more support-related information.

Troubleshooting the SharePoint Connector

Please refer to our knowledge base for help with the known issues and limitations in the Confluence SharePoint Connector:

- [SharePoint Connector Limitations and Known Issues](#)

Here are some tools to help you diagnose and solve problems that you may encounter:

- [Analysing the SharePoint Logs](#) — In the event of errors or other unexpected behaviour, examining the SharePoint logs can often provide clues as to the source of the problem.
- [Tracing the SharePoint Feature](#) — To troubleshoot or debug the SharePoint feature you can enable tracing and then view the trace with a tool such as DebugView.
- [Troubleshooting the SharePoint Configuration in Confluence](#) — When the SharePoint Connector configuration is set up properly it just works. However when it does not work it can be tricky to diagnose the problem, given the two different platforms trying to authenticate, authorise, and communicate across different servers. Here are some things to check on the Confluence side.
- [Using the CSI Diagnostics Tool to Test Confluence and SharePoint Connectivity](#) — If you are having trouble connecting to SharePoint from Confluence or to Confluence from SharePoint, you may want to perform some diagnostics to see what the problem is. Attached is a tool called '**CSI Diagnostics**' which you can use to test the web services used to connect from SharePoint to Confluence and vice-versa.
- [Determining which NTLM version is used](#) — This applies if you are using the IWA (NTLM only) configuration.
- [Enable Detailed Logging for the SharePoint Connector NTLM Proxy](#)

Analysing the SharePoint Logs

The SharePoint infrastructure has a comprehensive logging system, often referred to as the Unified Logging System ("ULS"), which is used by the SharePoint Connector for Confluence to report errors and exception conditions. In the event of errors or other unexpected behaviour, examining the SharePoint logs can often provide clues as to the source of the problem.

Locating the Log Files

The log files from the Unified Logging Service are located in the SharePoint "Hive" directory, which is different depending on which version of SharePoint you have installed. Consult the table below to identify the location of your log files.

SharePoint Version	Log File Location
SharePoint 2007	C:\Program Files\Common Files\Microsoft Shared\Web Server Extensions\12\LOGS
SharePoint 2010	C:\Program Files\Common Files\Microsoft Shared\Web Server Extensions\14\LOGS

The Unified Logging Service uses a 'rolling' log file system, so the LOGS folder is likely to contain multiple log files, each of which represents the log messages that were generated during a certain period of time. It may be helpful to sort the files by their Last Modified Date so that the most recent log file is displayed at the top of the folder.

Date Modified	Name	Size	Type
1/06/2010 9:56 AM	STRONGBAD-20100601-0955	177 KB	Text Document
31/05/2010 12:31 PM	STRONGBAD-20100531-1223	603 KB	Text Document
31/05/2010 12:23 PM	STRONGBAD-20100531-1213	2,804 KB	Text Document
8/02/2010 3:19 PM	STRONGBAD-20100208-1603	16,464 KB	Text Document
8/02/2010 3:15 PM	PSCDiagnostics_2_8_2010_16_3_38_770_986798137	3,744 KB	Text Document
8/02/2010 3:14 PM	Upgrade	303 KB	Text Document
8/02/2010 3:02 PM	STRONGBAD-20100208-1602	263 KB	Text Document
8/02/2010 3:01 PM	STRONGBAD-20100208-1601	263 KB	Text Document
8/02/2010 3:00 PM	STRONGBAD-20100208-1559	274 KB	Text Document
8/02/2010 2:59 PM	STRONGBAD-20100208-1558a	289 KB	Text Document
8/02/2010 2:58 PM	STRONGBAD-20100208-1558	291 KB	Text Document
8/02/2010 2:57 PM	STRONGBAD-20100208-1557	283 KB	Text Document
8/02/2010 2:56 PM	STRONGBAD-20100208-1556	290 KB	Text Document
8/02/2010 2:55 PM	STRONGBAD-20100208-1555	273 KB	Text Document
8/02/2010 2:54 PM	STRONGBAD-20100208-1554	273 KB	Text Document
8/02/2010 2:53 PM	STRONGBAD-20100208-1553	273 KB	Text Document
8/02/2010 2:53 PM	STRONGBAD-20100208-1552	281 KB	Text Document
8/02/2010 2:52 PM	STRONGBAD-20100208-1551a	280 KB	Text Document
8/02/2010 2:51 PM	STRONGBAD-20100208-1551	284 KB	Text Document
8/02/2010 2:50 PM	STRONGBAD-20100208-1539	6,686 KB	Text Document
8/02/2010 2:49 PM	PSCDiagnostics_2_8_2010_15_38_13_309_242381355	4,518 KB	Text Document
8/02/2010 2:39 PM	STRONGBAD-20100208-1538	693 KB	Text Document

22 objects 38.6 MB My Computer

Analyzing the Log Files

Locating pertinent information in the SharePoint log files can be challenging due to the sheer content of information in the log. When searching for information from the SharePoint Connector in the log, you should search for lines that contain the text "Atlassian Confluence"; which will prefix every line generated by the SharePoint Connector.

The example belows shows a log message generated by the SharePoint Connector:

```
01/01/2001 12:00:23.23 w3wp (0x18F8) 0x0390 Atlassian Confluence Web Part Error CS!z Exception
System.Web.Services.Protocols.SoapException: com.atlassian.confluence.rpc.RemoteException: The user 'test' does not exist.
```

Tracing the SharePoint Feature

To troubleshoot or debug the SharePoint feature you can enable tracing and then view the trace with a tool such as DebugView.

Enabling Tracing

To enable tracing, you will need to add a node to the `web.config` file for your SharePoint web application:

1. Locate the `web.config` for your SharePoint web application. For example, you may find it at the following location:
C:\Inetpub\wwwroot\wss\VirtualDirectories\80
2. Edit the `web.config` file and add or update the `<system.diagnostics>` node within the root `<configuration>` node as follows:
 - If there is already an existing `<system.diagnostics>` node, replace it with the following node.
 - If there is no existing `<system.diagnostics>` node, add the following node just above the last line in the file that contains `</configuration>`.

web.config snippet

```
<switches>
  <!-- 0=none, 1=errors, 2=warnings, 3=info, 4=verbose -->
  <add value="4" name="Atlassian.Confluence.SharePoint.Trace"/>
</switches>

]]>
```

3. Save the config file.
4. Reset IIS.

Problems with Flushing Trace Output

In some cases, the trace output does not flush properly. If you think this is the case for you, you can try tracing to a particular file and making sure the trace is flushed regularly. Here is an example of how to do this. Note that with this approach the trace file will continue to get larger over time. You can uncomment the `<remove name="Default" />` by simply removing the leading `<!--` and trailing `-->` portions if you want traces to only go to the file and **not** make them available to DebugView.

web.config snippet with autoflush

```
<switches>
  <!-- 0=none, 1=errors, 2=warnings, 3=info, 4=verbose -->
  <add value="4" name="Atlassian.Confluence.SharePoint.Trace" />
</switches>
<trace indentsize="4" autoflush="true">
  <listeners>
    <add type="System.Diagnostics.TextWriterTraceListener" initializedata="
c:\SharePointConnector.log" name="myListener" />
    <!--<remove name="Default" /> -->
  </listeners>
</trace>

]]>
```

Tracing the Confluence Search Administration Pages

Note that if you want to trace the custom Confluence search administration pages, you need to enable tracing for the `web.config` used for your SSP web application. This is typically not the '80' directory as used in the example above nor is it the same directory/web application for SharePoint Central Administration.



Note that the search administration tracing note above also applies to seeing the search security trimmer tracing when clicking the 'view scopes' link within search administration. The scopes will currently always show as a count of zero items because the security trimmer does not have context into Confluence from the search administration pages. It does not know the Confluence server URL or how to log into Confluence. This is **not** an indication that you have a search configuration problem.

Viewing the Trace

The easiest way to view the trace is to download [DebugView](#) onto your SharePoint web server. When using this tool, make sure you go to the 'Capture' menu and choose 'Capture Win32'.

After you have updated your `web.config`, performed an IISRESET and started DebugView, you can navigate to pages within SharePoint and you should see trace messages related to the SharePoint Connector for Confluence.

Troubleshooting the SharePoint Configuration in Confluence

When the SharePoint Connector configuration is set up properly it just works. However when it does not work it can be tricky to diagnose the problem, given the two different platforms trying to authenticate, authorise, and communicate across different servers. Here are some things to check on the Confluence side.

On this page:

- [Using a SharePoint Domain User Account or Local User Account](#)
- [Checking the Permissions for SharePoint Account used by Confluence](#)
- [Checking your SharePoint Server URL](#)
- [Making Sure You have Matching Versions of the Connector on Confluence and on SharePoint](#)

Using a SharePoint Domain User Account or Local User Account

You can log in to SharePoint with any user authorised to use SharePoint. Microsoft recommends that you use Active Directory domain accounts. However, you can only use domain accounts if the SharePoint server(s) are part of the domain.

Checking the Permissions for SharePoint Account used by Confluence

Make sure the account provided on the [Confluence 'SharePoint Admin' screen](#) is a SharePoint site administrator for the lists in all sites that the sp-list macro will access. For example, use a site collection administrator account.

Checking your SharePoint Server URL

Does your SharePoint URL resolve to something else? For example, if you type this into your browser:

<http://my-sharepoint-server>

Does it then resolve or get forwarded to something like this:

<http://my-sharepoint-server/site>

If yes, then the 'SharePoint Site URL' setting on your [Confluence 'SharePoint Admin' screen](#) needs to be: `*my-sharepoint-server/site`

See the [forum discussion thread](#).

Making Sure You have Matching Versions of the Connector on Confluence and on SharePoint

To see the latest version of the plugin, check the [latest release notes](#).

To see the version installed on your Confluence server:

1. Go to '**Confluence Admin**' and click '**Plugins**'.
2. Find and click the '**SharePoint Connector**'.
3. The version information will appear at the top of the screen in the middle.

To find out which version of the SharePoint Connector you have installed in SharePoint, go to the 'Confluence Administrative Settings' page in SharePoint:

1. Go to the top level site within the site collection.
2. Select '**Site Actions**' (at the top-right) -> '**Site Settings**' -> '**Modify All Site Settings**'.
3. On the 'Site Settings' page, choose '**Confluence Settings**'.
4. On the 'Confluence Administrative Settings' page, copy the value for the '**Connector Version**' (in the section labelled 'Confluence Site').

Using the CSI Diagnostics Tool to Test Confluence and SharePoint Connectivity

If you are having trouble connecting to SharePoint from Confluence or to Confluence from SharePoint, you may want to perform some diagnostics to see what the problem is. Attached is a tool called '**CSI Diagnostics**' which you can use to test the web services used to connect from SharePoint to Confluence and vice-versa.

The CSI Diagnostics Tool must be run on a Windows computer with the .NET Framework 2.0 installed.

1. Download the [attached zip file](#).
2. Unzip it.
3. Run `CSIDiagnostics.exe`.

Below are guidelines the options that the tool provides.

On this page:

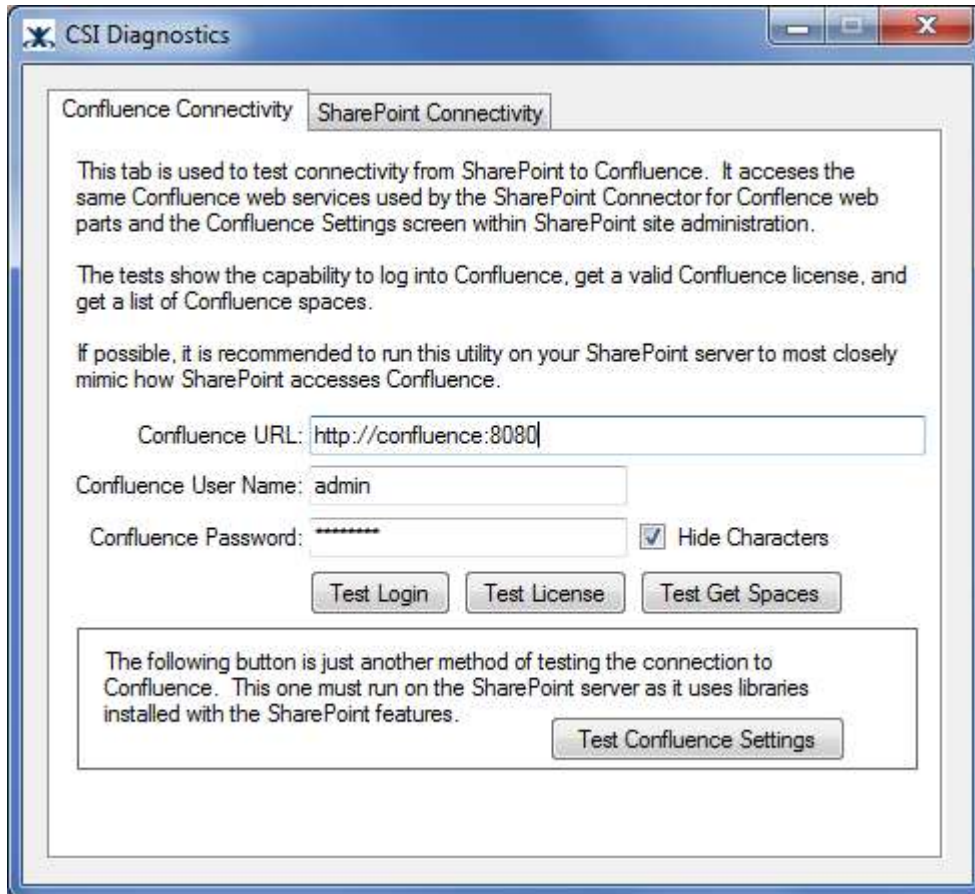
- [Testing SharePoint's Ability to Connect to Confluence](#)
- [Testing Confluence's Ability to Connect to SharePoint](#)

Testing SharePoint's Ability to Connect to Confluence



For the most realistic diagnosis, run this tool on your **SharePoint server** when trying to diagnose Confluence connectivity.

[Screenshot: Testing Confluence connectivity](#)



Use the '**Confluence Connectivity**' tab to test connectivity issues when SharePoint cannot connect to Confluence.

For example, use this tab when you encounter problems on the following SharePoint pages:

- The 'Test Confluence Configuration' button on SharePoint's [Confluence Administrative Settings](#) page gives an error.
- The [SharePoint web parts](#) give an error.

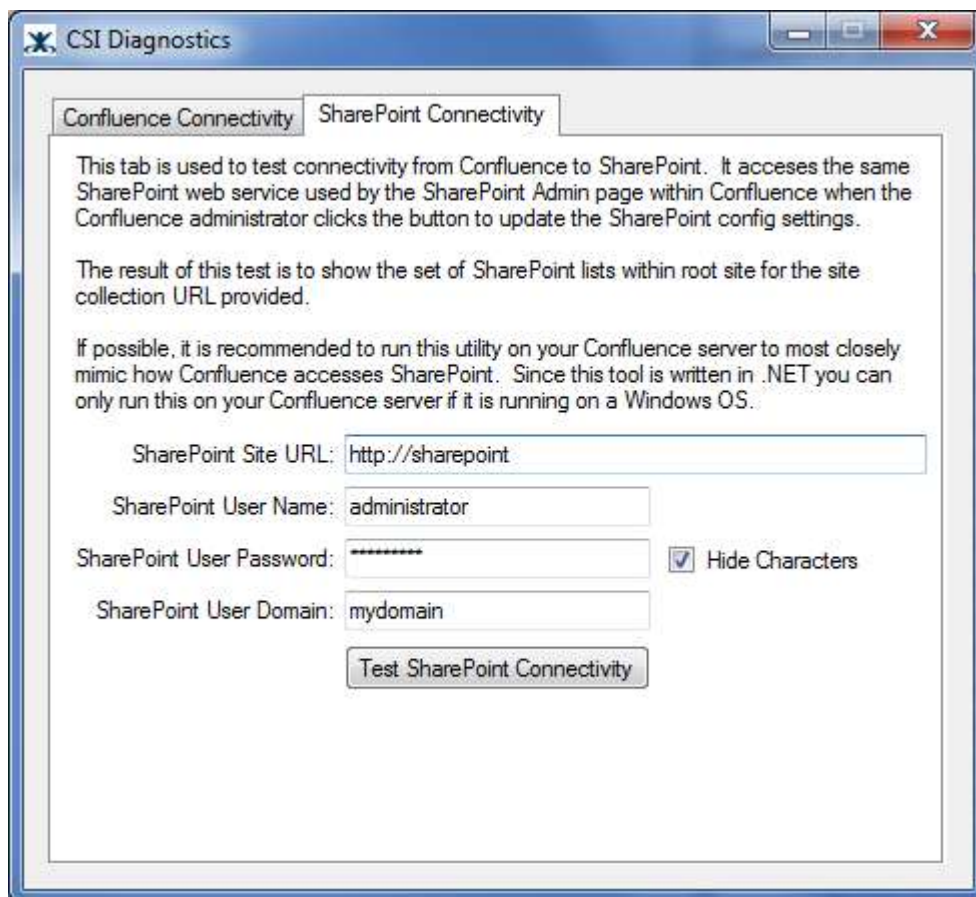
The '**Test Confluence Settings**' button uses the helper API built into the SharePoint feature to test the settings to Confluence. To run this test you must be running this tool on the SharePoint server with the SharePoint Connector features installed.

Testing Confluence's Ability to Connect to SharePoint



For the most realistic diagnosis, run this tool on your **Confluence server** when trying to diagnose SharePoint connectivity. If your Confluence server is not running on a Windows operating system, then run this tool on any Windows computer in your network that is 'close' (with regards to network hardware) to your Confluence Server.

Screenshot: Testing SharePoint connectivity



Use the '**SharePoint Connectivity**' tab to test connectivity issues when Confluence cannot connect to SharePoint.

For example, use this tab when you encounter problems on the following Confluence pages:

- The 'Test Connection' button on Confluence's [SharePoint Admin screen](#) gives an error.
- The [sp-list macro](#) gives an error.



This tool is not the best at diagnosing problems with SharePoint connectivity because the tool uses .NET libraries (web service proxies) to communicate to SharePoint whereas the plugin uses Java libraries. For that reason, you may find that the tool can communicate with SharePoint but the plugin still has problems.

Determining which NTLM version is used

It is useful to be able to find out which NTLM versions your SharePoint site is configured to use. This applies if you are using the IWA (NTLM only) configuration. See our guides [for SharePoint 2007](#) and [for SharePoint 2010](#).

You can find which NTLM version is used in your registry key:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\LSA\LMCompatibilityLevel.

Once you have the registry open, determine the value data (0 - 5):

Level	Group Policy Name	Sends	Accepts	Prohibits Sending
0	Send LM and NTLM Responses	LM, NTLM	NTLMv2 Session Security is negotiated	LM, NTLM, NTLMv2 NTLMv2 Session Security (on Windows 2000 below SRP1, Windows NT 4.0, and Windows 9x)
1	Send LM and NTLM---use NTLMv2 session security if negotiated	LM, NTLM NTLMv2 Session Security is negotiated	LM, NTLM, NTLMv2	NTLMv2
2	Send NTLM response only	NTLM NTLMv2 Session Security is negotiated	LM, NTLM, NTLMv2	LM and NTLMv2

3	Send NTLMv2 response only	NTLMv2 Session Security is always used	LM, NTLM, NTLMv2	LM and NTLM
4	Send NTLMv2 response only/refuse LM	NTLMv2 Session Security	NTLM, NTLMv2	LM
5	Send NTLMv2 response only/refuse LM and NTLM	NTLMv2, Session Security	NTLMv2	LM and NTLM

Source Microsoft TechNet Magazine

More detailed discussion can be found [here](#).

Enable Detailed Logging for the SharePoint Connector NTLM Proxy

The SharePoint Connector NTLM proxy is a .NET executable that allows Confluence to communicate with SharePoint using the full range of Integrated Windows Authentication methods (including NTLMv2 and Kerberos).

If the authentication process fails, or there appears to be some problem with the proxy component, you can enable additional logging in order to help diagnose the problem.

How to Enable or Disable Diagnostic Logging


To toggle the logging level for the proxy component, open a web browser and go to `<CONFLUENCE_BASE_URL>/admin/sharepoint-admin/proxy-admin.action`.

Screenshot 1: Proxy Administration Screen

Proxy Configuration

Configure the behaviour of the SharePoint Connector's NTLM SOAP Proxy, which allows Confluence to communicate with SharePoint using the full range of Windows authentication methods (eg. NTLMv2, Kerberos). This feature is only functional when Confluence is run on a Windows server and Microsoft .NET Framework 2.0 is installed on the Confluence server.

Proxy State	<input checked="" type="checkbox"/> Enabled [Disable]
Confluence Server Compatibility	<input checked="" type="checkbox"/> Proxy is compatible with your Confluence Server.
Current Status	<input checked="" type="checkbox"/> Proxy is running; no problems detected.
Debug Logging	Debug Logging is disabled. [Enable]
Listen Port	<input type="text" value="56000"/> <input type="button" value="Update"/>

Go to  [SharePoint Admin](#)

If the Debug Logging setting is not currently enabled, you can click the **'Enable'** link to turn it on. If the Debug Logging setting is already enabled, you can click the **'Disable'** link to turn it off.



Note that enabling or disabling the logging setting will cause the proxy component to restart.

This could lead to a brief disruption in the communications between Confluence and SharePoint.

Locating the Log File

You can locate the log file for the proxy in the same directory as the proxy executable. Both the executable and log the file may be found in the temporary directory of the application server hosting your Confluence instance.

For example, if you are running Confluence stand-alone, the log file may be found in this location, where CONFLUENCE_HOME is your configured Confluence data directory:

```
CONFLUENCE_HOME\temp\SimpleSoapProxy.log
```

If you are running the WAR edition of Confluence, then the temporary directory's location may vary.

SharePoint Connector Installation and Upgrade Guide

- [Release Notes](#)
- [Installing the SharePoint Connector](#)
- [Upgrading the SharePoint Connector](#)
- [Applying Specific Confluence Configurations](#)
- [Deploying the SharePoint Connector to More SharePoint Sites](#)

Release Notes

This section contains release notes and change logs for the Confluence SharePoint Connector.



Latest version of the Confluence SharePoint Connector

Confluence SharePoint Connector 1.3 has now been released. See the [SharePoint Connector 1.3 Release Notes](#).

- [SharePoint Connector 1.3 Release Notes](#)
- [SharePoint Connector 1.2.1 Release Notes](#)
- [SharePoint Connector 1.2 Release Notes](#)
- [SharePoint Connector 1.1.1 Release Notes](#)
- [SharePoint Connector 1.1 Release Notes](#)
- [SharePoint Connector 1.0 Release Notes](#)

SharePoint Connector 1.3 Release Notes

23 February 2011

Atlassian is proud to present the **Confluence SharePoint Connector 1.3**.

This release includes a number of end user features and administration improvements. Most notably, the Confluence Page web part and a Confluence Tree View web part now support web part 'Connections.' This means that you can configure the Confluence Page web part to dynamically update when a user clicks within the Tree View web part. In addition, the Confluence Page web part now displays any comments associated with that page, allowing SharePoint users to view threaded discussions happening in Confluence.

Our developers have managed to squeeze in a number of other improvements too. Better sub-folder support in the SharePoint List macro, full support for row-level security, improved handling of anonymous users in Confluence, and a nicer integrated search experience are just a handful of the extra goodies in this release.

To see the full picture, take a look at the list of improvements below.

Highlights of this release:

- [Support for Web Part Connections](#)
- [Bring Confluence Discussions into SharePoint](#)
- [Search SharePoint From Any Space](#)
- [Improved SharePoint List macro](#)
- [Plenty of Improvements](#)

We love your feedback:

Keep logging your votes and issues. They help us decide what needs doing!



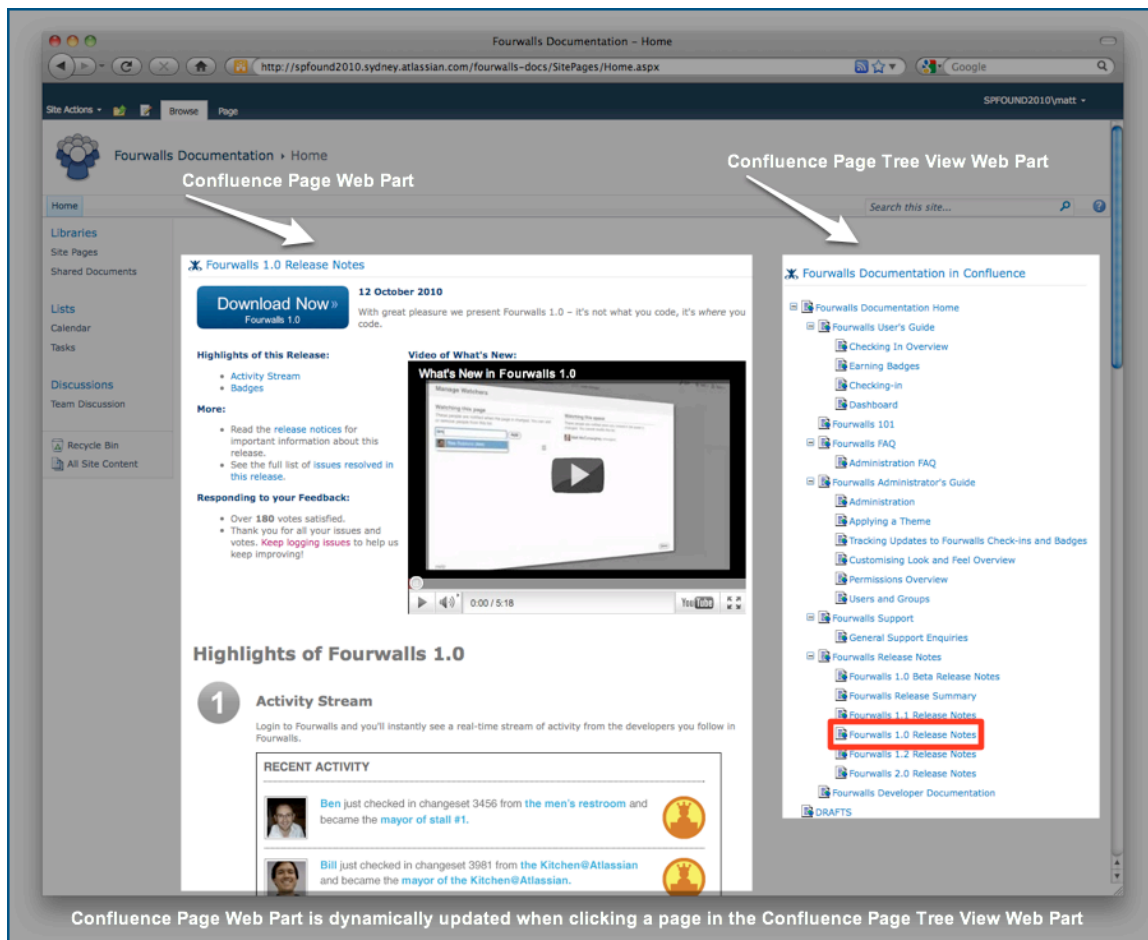
Upgrading from a previous version of the SharePoint Connector

Please refer to the [SharePoint Connector 1.3 Upgrade Notes](#) for essential information about factors affecting your upgrade.



Support for Web Part Connections

The Confluence web parts now support web part 'Connections'. This allows users to browse the pages in a Confluence space without leaving SharePoint. Setting up the connection is easy – just edit the SharePoint page and use the menus to connect the web parts together.

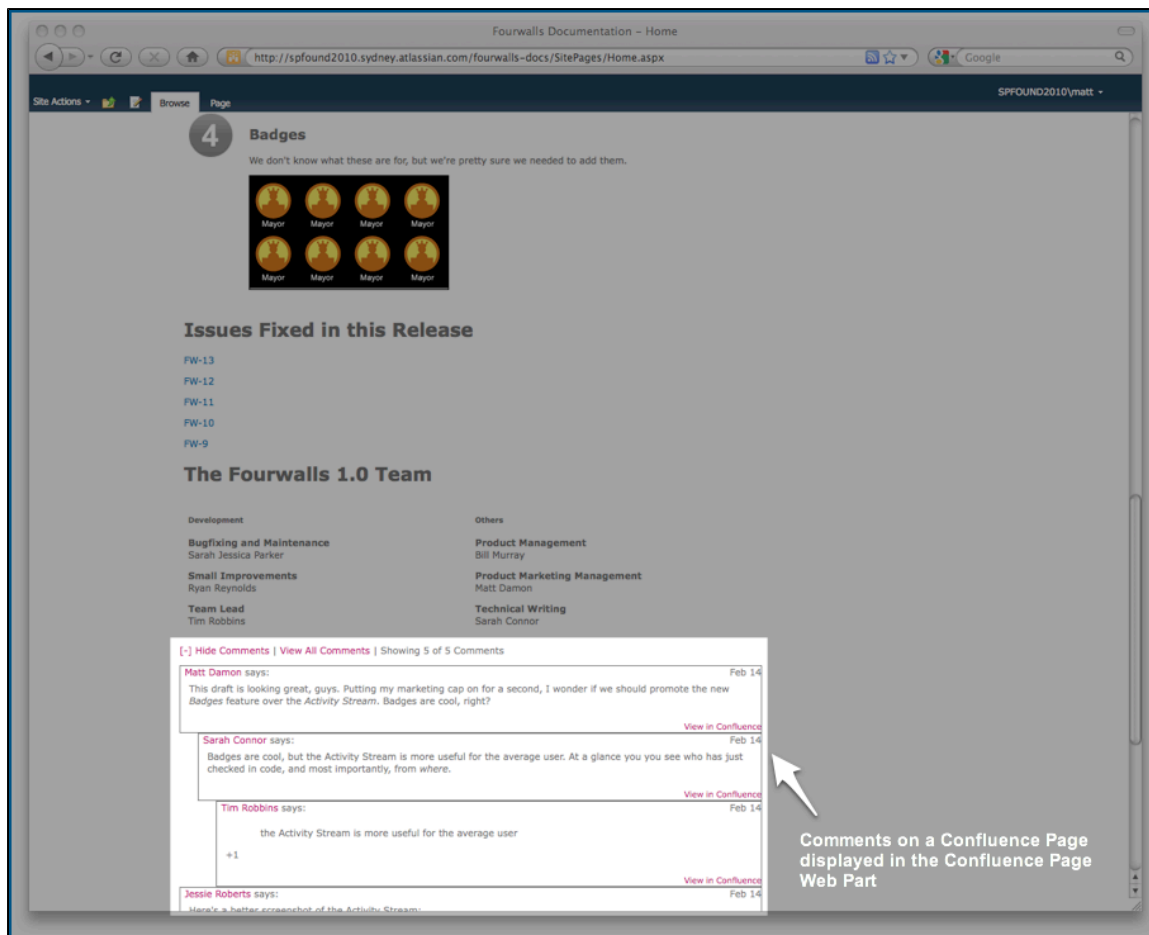


Confluence Page Web Part is dynamically updated when clicking a page in the Confluence Page Tree View Web Part

2

Bring Confluence Discussions into SharePoint

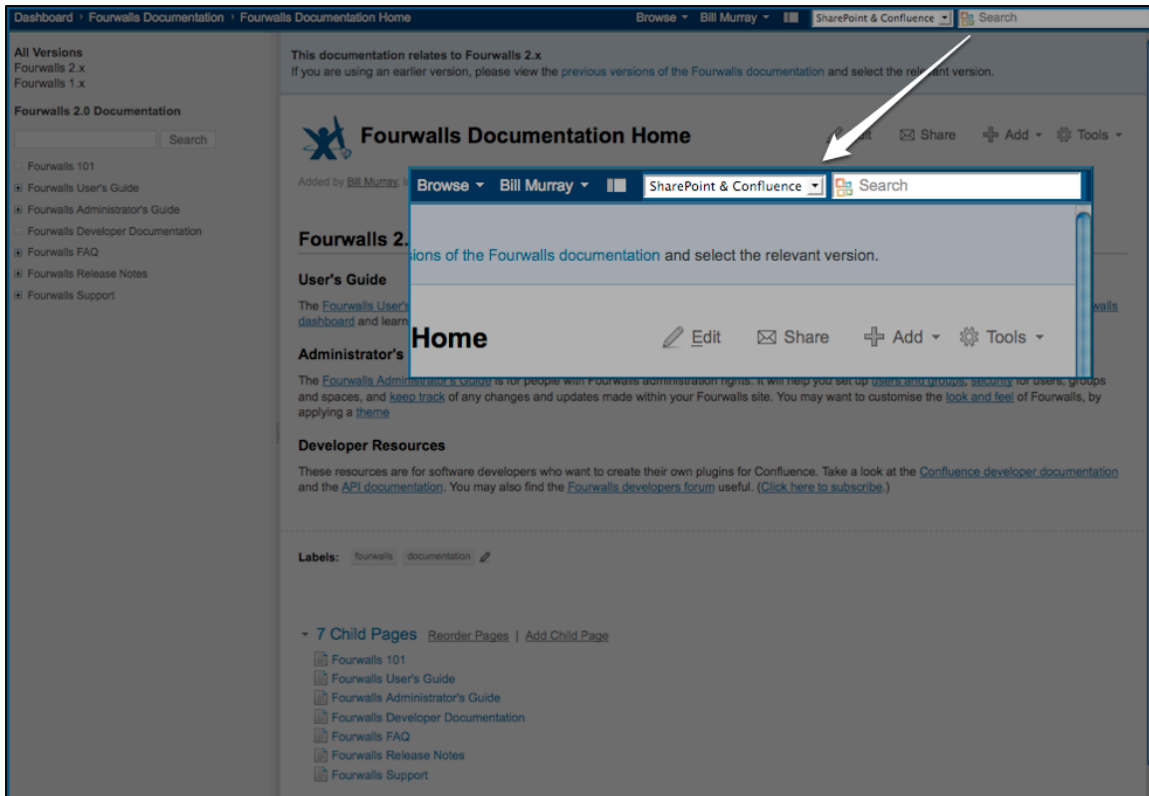
A new option in the Confluence Page web part allows users to toggle the display of comments on a Confluence page within the web part. If you use comments to discuss your Confluence content, this discussion can now automatically be displayed in SharePoint.



3

Search SharePoint From Any Space

One of the best features of the SharePoint Connector is the ability to search Confluence and SharePoint at the same time. Prior to SharePoint Connector 1.3, you needed to use the SharePoint Decorators theme if you wanted to search SharePoint from your Confluence space. In 1.3 we've eliminated this dependency so that you can now add integrated SharePoint search to any Confluence space, regardless of the theme you're using.



4

Improved SharePoint List macro

SharePoint Connector 1.3 gives you more flexibility and security when embedding SharePoint lists into your Confluence page:

- The SharePoint List macro can now display any sub folder in your SharePoint List or Document Library. Check out our guide to [Using the SharePoint List Macro](#) for more information.
- The SharePoint List macro (`{sp-list}`) now fully respects any row-level permissions applied to list items and documents, offering greater security for your SharePoint content. (CSI-217)

[insert screenshot of a Confluence page just showing a subfolder - maybe show the full folder in sharepoint with an arrow pointing to the subfolder in Confluence.]

5

Plenty of Improvements

Here's a selection of the other improvements in this release:

- The Confluence Permission Checker RPC plugin is no longer required for the SharePoint Connector. The same functionality has now been rolled into the core SharePoint Connector plugin, providing a more streamlined installation and upgrade experience. (CSI-217)
- When embedding Confluence content into SharePoint, administrators can now configure the SharePoint Connector to access the SharePoint user's email address for logging in to Confluence. This was a feature request from a number of customers who use email-addresses as login names for Confluence (CSI-285).
- Administrators can now customise the timeout value for Confluence web service calls (CSI-60).

The SharePoint Connector 1.3 Team

Development

Elwist Ng
Kang Leng Ong

Product Management

Bill Arconati

Product Marketing Management

Matthew Hodges

Support

Roy Hartono

Adam Laskowski

Azwandi Mohd Aris

Team Lead

Joseph Clark

External Contributions













































Atlassian gratefully acknowledges the contributions of these external developers, who contributed software patches that were incorporated into this release

Mohd Sukri (CustomWare)

Vikas Sharma

Complete List of Fixes in this Release

JIRA Issues (41 issues)			
Key	Summary	Priority	Status
CSI-554	sp-list macro is unable to render sub-folders that are multiple levels deep		 Resolved
CSI-507	SharePoint Connector returns errors after reinstallation of plugin		 Resolved
CSI-217	Update SharePoint Permission Checker (permcheck.asmx) web service to support item-level security		 Resolved
CSI-678	SharePoint Connector 1.2 installation fails when upgrading from a previous version		 Resolved
CSI-679	Confluence integration tests failing on build server		 Resolved
CSI-670	SimpleSoapProxy concatenates URL paths incorrectly		 Resolved
CSI-696	"Show Comments" hyperlink doesn't work in Firefox 3.6		 Resolved
CSI-699	Initial load of Confluence Page Webpart with Web Part Connections enabled is always blank		 Resolved
CSI-431	StringIndexOutOfBoundsException showing up in the logs		 Resolved
CSI-627	Upgrade Confluence plugin to Plugins-2		 Resolved
CSI-632	Upgrade Confluence plugin to Plugins-2		 Resolved
CSI-667	Selecting the "select a space" option in the Tree View Webpart space list causes an error		 Resolved
CSI-136	Pages Tree View Web Part - Allow Selection of Page		 Resolved
CSI-285	Allow the web parts to authenticate with Confluence using the email address of the user for the user name		 Resolved
CSI-605	Allow administrators to customise the timeout value for Confluence web service calls		 Resolved
CSI-624	Remove the need for the "Permission Checker" plugin		 Resolved
CSI-471	Display Confluence Comments in webparts		 Resolved
CSI-487	PermCheck Plugin throws Exceptions		 Resolved
CSI-571	Hyperlinks are not underlined when created with the sp-link macro		 Resolved

CSI-575	Breadcrumbs are not displayed when using IE8 and the SharePoint Decorators theme		 Resolved
CSI-576	Confluence page preview does not work when using SharePoint Decorators theme		 Resolved
CSI-597	SharePoint Connector Theme's footer is not anchored to the bottom of the page		 Resolved
CSI-647	Confluence plugin has exploded in size since 1.2.0 release		 Resolved
CSI-671	Add diagnostic logging to the SimpleSoapProxy		 Resolved
CSI-673	SimpleSoapProxy does not handle zero length responses from SharePoint correctly		 Resolved
CSI-674	Upgrade NUnit dependency to latest version		 Resolved
CSI-682	Provide an option for bypassing Confluence permission checking for SharePoint Web Parts		 Resolved
CSI-693	Sharepoint-integrated search plugin module should be disabled by default		 Resolved
CSI-697	The new "Display Comments" option in the Confluence Page webpart should be enabled by default		 Resolved
CSI-698	When "Display Comments" is enabled, the comments should be expanded by default		 Resolved
CSI-548	Use something other than a global SharePoint theme to deploy the custom search box for the SharePoint Connector		 Resolved
CSI-676	Documentation updates for SharePoint Connector 1.3		 Resolved
CSI-664	Allow specification of SharePoint site in sp-link macro		 Resolved
CSI-494	Prompt the user to save changes to Confluence configuration in SharePoint		 Resolved
CSI-550	When no Sharepoint locations are configured in Confluence, an uninformative error message is displayed when using the sp-list macro		 Resolved
CSI-502	"Confluence Page" WebPart in SharePoint links to incorrect admin URL		 Resolved
CSI-536	Remove dependence on SOAP Permissions Checker Plug-in		 Resolved
CSI-614	The word "Dashboard" in breadcrumb is misaligned		 Resolved
CSI-655	If search settings are not configured properly, federated search results web part remains blank		 Resolved
CSI-551	Confluence "Anti-XSS" feature destroys the SharePoint plugin when it is deployed to WEB-INF\lib		 Resolved
CSI-672	SimpleSoapProxy Assembly Information refers to the component as "SimpleWebProxy"		 Resolved

SharePoint Connector 1.3 Upgrade Notes

Below are some important notes on upgrading to **SharePoint Connector 1.3** from an earlier version of the connector. For details of the new features and improvements in this release, please read the [SharePoint Connector 1.3 Release Notes](#).

On this page:

- [Upgrade Notes](#)
 - Minimum Requirement is Confluence 3.0.2 or Later
 - Deprecated "SharePoint Decorators" Theme
 - Deprected Permission Checker RPC Plugin

- [Upgrade Procedure](#)

Upgrade Notes

Minimum Requirement is Confluence 3.0.2 or Later

With the release of version 1.2, the SharePoint Connector no longer supports Confluence 2.10.x. The minimum requirement is Confluence 3.0.2 or later. Please refer to the full details of the [supported platforms for SharePoint 2007](#) and [for SharePoint 2010](#)

Deprecated "SharePoint Decorators" Theme

The "SharePoint Decorators" Theme that was shipped in previous versions of the SharePoint Connector has been removed from the product. In its place is the a new plugin module that can be enabled with any Confluence theme.

If you have enabled the SharePoint Decorators theme in one or more Confluence spaces, the spaces will automatically revert to use the global theme after upgrading the SharePoint Connector to version 1.3. If you have enabled the SharePoint Decorators theme as your global Confluence theme, then your instance will revert to use the default Confluence look & feel after upgrading to version 1.3.

Deprected Permission Checker RPC Plugin

Previous versions of the SharePoint Connector required an additional Confluence plugin to be installed; the "Confluence Permission Checker RPC Plugin". This functionality has been rolled into the core SharePoint Connector plugin and the Permission Checker plugin is no longer required.

When upgrading to version 1.3 of the SharePoint Connector, any installed versions of the Permission Checker plugin will automatically be un-installed in order to prevent any compatibility clashes.

Upgrade Procedure

There are two upgrade procedures to choose from:

- **Option 1: Upgrade your SharePoint Connector on SharePoint 2010.** This procedure assumes that you have upgraded your SharePoint server to Microsoft SharePoint 2010. To upgrade the connector, you will install the latest version of the SharePoint Connector plugin in Confluence and upgrade the SharePoint feature in Microsoft SharePoint 2010. See the [instructions](#).
- **Option 2: Upgrade your SharePoint Connector on SharePoint 2007.** This procedure assumes that you are running the SharePoint Connector on Microsoft SharePoint 2007. To upgrade the connector, you will install the latest version of the SharePoint Connector plugin in Confluence and upgrade the SharePoint feature in Microsoft SharePoint 2007. See the [instructions](#).



Need help?

If you encounter a problem during the upgrade, please create a [support ticket](#) and one of our support engineers will assist you through the process.

RELATED TOPICS

[SharePoint Connector 1.3 Release Notes](#)

SharePoint Connector 1.2.1 Release Notes

6 August 2010

Atlassian is proud to present the **Confluence SharePoint Connector 1.2.1**.

Version 1.2.1 of the SharePoint Connector has been tested with and is compatible with [Confluence 3.3](#).

This release resolves all the issues reported since the release of the SharePoint Connector 1.2. In particular, we have fixed two problems with the [SharePoint List macro](#). One issue was that the macro displayed invalid values, such as `null ` or `$item.ToString()`, for some SharePoint fields containing dates or empty values. The other issue was that the connector ignored paths specified in a macro parameter, causing an error when you tried to display a list from a SharePoint subsite.

Don't have Confluence SharePoint Connector 1.2 yet?

Take a look at the new features and other highlights in the [SharePoint Connector 1.2 release notes](#) then follow our [installation guide](#).

Upgrading from a previous version of the SharePoint Connector

Please read the [SharePoint Connector 1.2 Upgrade Notes](#).

Updates and Fixes in this Release

JIRA Issues (17 issues)			
Key	Summary	Priority	Status

CSI-628	sp-list macro ignores site path parameter		Resolved
CSI-648	Federated Search Results WebPart is not updated during upgrade		 Resolved
CSI-677	Security Vulnerability in Confluence Permission Checker RPC Plugin		 Resolved
CSI-639	Web service cache in Confluence plugin does not expire		 Resolved
CSI-641	Cached Web Service proxies should be configured for multi-threaded access		 Resolved
CSI-642	Investigate problem with SafeControl entries not being added automatically		 Resolved
CSI-391	Document SharePoint Deployment Steps for Deploying to New Site Collections		 Resolved
CSI-481	Pages Tree View Web Part does not display in Webpart installer 1.0.7		 Closed
CSI-633	"debug" parameter in the sp-list macro no longer works		 Resolved
CSI-634	Cell values in sp-list macro have incorrect values ("null ", "\$item.ToString()").		 Resolved
CSI-640	NTLM SOAP Proxy connections have no suitable timeout		 Resolved
CSI-644	Confluence 3.3 Compatibility		 Resolved
CSI-650	Create Knowledge Base Article for working around problem where Confluence Federated Search Results are not formatted		 Resolved
CSI-578	Provide SharePoint Connector source code to enterprise customers		 Resolved
CSI-629	When restarting the Windows NTLM SOAP Proxy via the confluence admin page, the proxy is still listed as "connection failed", even though it is now running.		 Resolved
CSI-630	The Windows NTLM SOAP Proxy requires .NET 2.0, but if this is not installed on the Confluence server, then it fails silently when the plugin is installed		 Resolved
CSI-631	Remove instruction to install SPC jar from "confluence/WEB-INF/lib" from readme.txt		 Resolved

SharePoint Connector 1.2 Release Notes

7 June 2010

Atlassian is proud to present the **Confluence SharePoint Connector 1.2**.

The two big features of this release are SharePoint 2010 support and the much improved support for Integrated Windows Authentication (IWA). With version 1.2 of the Confluence SharePoint Connector, you can now connect Confluence to Microsoft SharePoint 2010 as well as SharePoint 2007. In addition, the connector offers full support for all the IWA protocols, now including NTLMv2 and Kerberos.

There are a number of other improvements too. You can now deploy the connector to additional SharePoint site collections at any time. The connector supports multiple AD domains, since it can now distinguish between two identical usernames in different domains. To see the full picture, take a look at the list of improvements below.

Highlights of this release:

- Support for SharePoint 2010
- Integrated Windows Authentication
- Easy Connection to Additional SharePoint Site Collections
- Multiple AD Domains
- Plenty of Improvements

We love your feedback:

Please fill out our short survey to help us understand how you use the Confluence SharePoint Connector.

Keep logging your votes and issues. They help us decide what needs doing!



Upgrading from a previous version of the SharePoint Connector

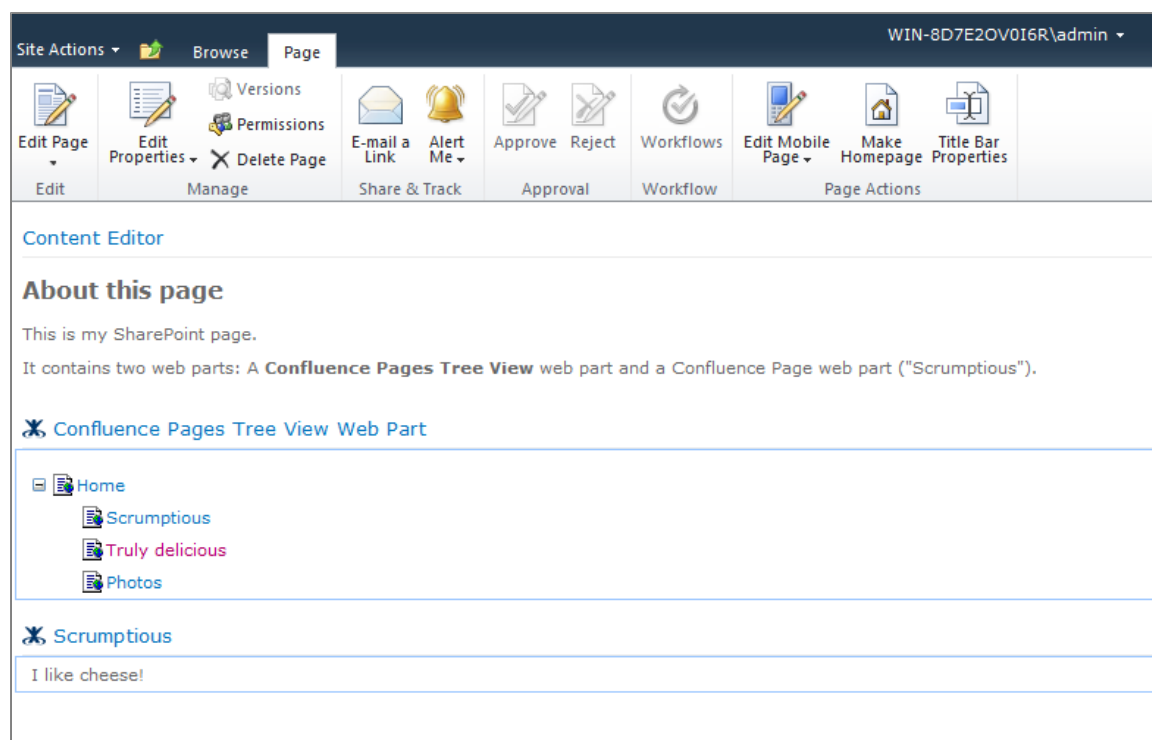
Please refer to the [SharePoint Connector 1.2 Upgrade Notes](#) for essential information about factors affecting your upgrade.

1

Support for SharePoint 2010

The SharePoint Connector now supports SharePoint 2010 as well as SharePoint 2007. The connector offers the same features for both versions of SharePoint:

- Embed Confluence pages and page trees into a SharePoint page, using the Confluence web parts. Click through from SharePoint to Confluence.
- Embed SharePoint lists and documents into a Confluence page, using Confluence's sp-list and sp-link macros. Click through from Confluence to SharePoint. Edit Office documents directly from Confluence and save them back to SharePoint.
- Enjoy automatic login (single sign-on) between Confluence and SharePoint.
- Search Confluence and SharePoint content together, retrieving a unified set of results.



2

Integrated Windows Authentication

The SharePoint Connector offers a number of options for configuring authentication between Confluence and SharePoint. Version 1.2 of the connector adds support for **NTLMv2 and Kerberos**. This means that the connector supports all of the Integrated Windows Authentication protocols. We have created handy guides and decision charts to help you choose the configuration that suits your environment, and detailed documentation about setting up each configuration.

Connecting from SharePoint to Confluence:

- The connector supports all of the IWA protocols (LM, LMv2, NTLM, NTLMv2, Kerberos).
- You can use IIS or Jespa.

Connecting from Confluence to SharePoint:

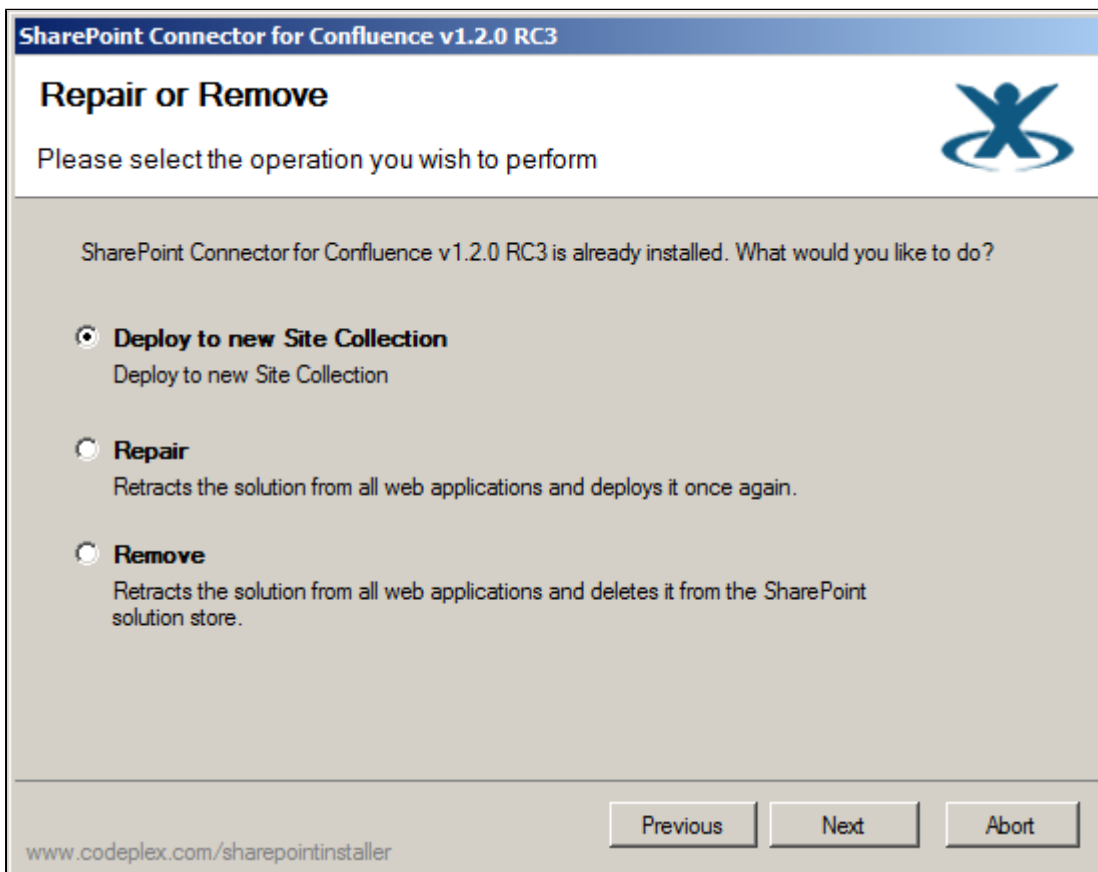
- Confluence on Windows can connect to SharePoint using **all** of the IWA protocols (LM, Mv2, NTLM, NTLMv2, Kerberos), using our new .NET NTLM proxy.
- When Confluence is not running on Windows, it can connect to SharePoint using LM or NTLM.

See our cool new guides to planning your environment with [SharePoint 2007](#) and [SharePoint 2010](#).

3

Easy Connection to Additional SharePoint Site Collections

At any time after the initial installation, you can now deploy the SharePoint Connector to more site collections. Just run the SharePoint Connector installer (Setup_WebParts.exe) and select 'Deploy to new Site Collection'. See our [documentation](#).



4

Multiple AD Domains

You can configure Confluence to connect to a number of Active Directory domains. With the latest release of the SharePoint Connector, you can configure the connector to pass the domain as well as the username when checking the user's permissions in Confluence. This means that the connector can distinguish between two users who have the same username in different domains. See our [documentation for SharePoint 2007](#) and for [SharePoint 2010](#).

☒ Customise permission checking format (optional)

This setting is useful if you have configured Confluence to connect to multiple Active Directory domains.

User Name Format:

5

Plenty of Improvements

You'll notice that things just work better with the latest version of the SharePoint Connector.

- We have fixed a problem in the Confluence Pages Tree View web part. Before this release, SharePoint would automatically check out the page when a user changed the selection in the space dropdown list. Under certain circumstances, this could cause an error. The web part now displays a 'Make Default' option when the user changes the selection in the space dropdown. If the user selects the option, SharePoint will check out the page if necessary. Otherwise, SharePoint will not attempt to check out the page.
- When sending authentication credentials to Confluence, the SharePoint Connector now correctly passes credentials entered in the format 'DOMAIN\Username'. Before this release, the connector sent such credentials with an empty domain and the username set to 'DOMAIN\Username', which caused the authentication to fail. This bug is now fixed.
- See the complete list of fixes below.

The SharePoint Connector 1.2 Team

Development

Jonathan Gilbert
Joseph Clark

Product Management

Sherif Mansour

Product Marketing Management

Bill Arconati
Matthew Hodges

Quality Assurance

Mark Hrynczak
Marlena Compton

Support

Roy Hartono
Maleko Taylor
Azwandi Mohd Aris

Team Lead





















































Per Fragemann





















































Technical Writing














Sarah Maddox

Complete List of Fixes in this Release

JIRA Issues (67 issues)			
Key	Summary	Priority	Status
CSI-612	Confluence plugin has hard-coded text for "MOSS Search Integration settings", which is not correct when connecting to SP2010		Closed
CSI-611	The SSO Tickets generated by the Secure Store Service are too long to be embedded in the URLs		Closed
CSI-610	Unhandled Exception thrown when trying to configure a Confluence Page Web Part and Secure Store Service is active		Closed
CSI-609	When the SharePoint Installer system checks are run twice, all subsequent screens in the wizard get duplicated.		Closed
CSI-608	Please fix help link on 'Finished' screen of installer		Closed
CSI-607	If both SharePoint 2007 and SharePoint 2010 are installed, the installer defaults to install the SharePoint 2007 solution file, and this behaviour cannot be modified		Closed
CSI-606	Minor improvements to ConfluenceSettings.aspx for 1.2		Closed
CSI-604	Fix the documentation links on the SharePoint "Confluence Administrative Settings" screen		Closed

CSI-601	Following instructions for installing the Confluence plugins causes a licence-inconsistency error state		 Closed
CSI-600	Unhandled exception if SharePoint solution installer cannot start the SharePoint Administrative Service		 Closed
CSI-599	SharePoint Connector 1.2 cannot be installed on Confluence 3.2		 Closed
CSI-598	Invalid JavaScript causes Confluence Page Web Part to not load in Firefox 3.6/SharePoint 2010		 Closed
CSI-595	new "Confluence User Name Format" field in ConfluenceSettings.aspx is not persisted after sp2010 merge.		 Closed
CSI-594	SharePoint feature installer deletes the WSP file from disk after installing it into the SharePoint solution store		 Closed
CSI-593	SharePoint feature installer refers to "SharePoint 2007" when installing on SharePoint 2010 Server.		 Closed
CSI-591	On uninstall the log page is skipped causing the Installer to crash		 Closed
CSI-587	Add the Atlassian "Charlie" icon to the SharePoint Connector icon		 Closed
CSI-586	Running the SharePoint Connector Installer requires administrative privileges		 Closed
CSI-585	Enhance the installer to detect SharePoint 2007/2010 and install the correct solution		 Closed
CSI-584	Add support for deploying SharePoint Connector to new site collections		 Closed
CSI-583	SharePoint installer files should be embedded resources		 Closed
CSI-582	Do not show installer log screen if installation was successful		 Closed
CSI-581	Create links to start SharePoint services if the Installer detects that they are not running		 Closed
CSI-580	Evaluate documentation impact of Version 1.2 Changes		 Closed
CSI-573	Please add and fix documentation links in Macro Browser for the sp-link and sp-list macros		 Closed
CSI-567	Verify support for Confluence 3.2		 Closed
CSI-566	CSI Diagnostics tool is out of date		 Closed
CSI-565	CSI Diagnostics documentation incorrectly states that the diagnostic tool can only run on 32-bit machines; this is false.		 Closed
CSI-564	SharePoint Connector installation instructions do not specify that the Remote API for Confluence must be enabled.		 Closed
CSI-563	Support SharePoint 2010		 Closed
CSI-560	SharePoint Decorator Theme: Unable to use Macro Browser		 Closed
CSI-556	SharePoint Plugin contains some undefined modules		 Closed
CSI-552	Macro Browser does not load when SharePoint Decorators Theme is enabled		 Closed
CSI-549	Confluence credentials stored in SharePoint (in DOMAIN\Username format) fails to connect to Confluence		 Closed
CSI-547	Domain name gets stripped off when using Basic Authentication (Confluence -> SharePoint)		

			Closed
CSI-545	Improve CI Build Time		 Resolved
CSI-543	CAT.NET reports errors for Atlassian.Confluence.SharePoint.dll		 Closed
CSI-542	SPDisposeCheck reports errors for Atlassian.Confluence.SharePoint.dll		 Closed
CSI-540	Modifying "space list" drop-down in Confluence tree view web part causes page check-out		 Closed
CSI-537	Please change the online help link on the Confluence 'SharePoint Admin' screen		 Closed
CSI-535	Basic Authentication (Confluence -> SharePoint) doesn't work when username is <Domain>\<User>		 Closed
CSI-532	client-config.wsdd on CAC has moved		 Closed
CSI-530	Sharepoint Connector is using Apache HTTP client, hence it can only send LM authentication		 Closed
CSI-527	Improve the messaging around what the Sharepoint Connector can and cannot do		 Closed
CSI-516	Please update the text in the "readme.txt" bundled with "SharePointConnector" zip file		 Closed
CSI-513	client-config.wsdd is not written out correctly in some cases yet again		 Closed
CSI-512	Wording for "Confluence Access URL Enabled" option could do with some clarification.		 Closed
CSI-510	Tree View web part displays error when selecting first option in space list		 Closed
CSI-506	Modifying a Confluence Web Part clears the previous page selection		 Closed
CSI-498	sp-list macro throws an NPE when listname and column are blank		 Closed
CSI-493	Remove the second "Confirm Password" field on the Confluence Settings page in SharePoint		 Closed
CSI-491	WebParts installer does not rerun System Check when expected		 Closed
CSI-488	Failing connection to Confluence in WebPart can bring down whole Sharepoint Page		 Closed
CSI-485	Session cannot be accessed in WSS		 Closed
CSI-461	Distinguish the same user of multiple domains		 Closed
CSI-452	Drop JCIFS support		 Closed
CSI-443	the Confluence plugin to authenticate SOAP calls to SP with NTLMv2		 Closed
CSI-418	improve error message when client-config.wsdd is not written properly by the plugin		 Closed
CSI-413	Licensing service returns a "401 Unauthorized" when using JCIFS for authentication in Confluence		 Closed
CSI-406	Update recommended browser settings for Firefox 3.0		 Closed
CSI-393	Allow user to set web part title and icon		

			Closed
CSI-225	Allow for Kerberos and/or Certificates between SharePoint and Confluence		 Resolved
CSI-222	Update SSO FAQ items as appropriate		 Resolved
CSI-198	Confluence Settings Validation Refresh Issue		 Closed
CSI-167	Make the methods found in SSOHelper instance methods vs. static methods		 Closed
CSI-166	Move SSO "GetCredentials" code currently found in ConfluenceSettings to a new SharePoint-hosted web service		 Closed
CSI-152	SharePoint Installer - Hide Logs if Successful		 Closed

SharePoint Connector 1.2 Upgrade Notes

Below are some important notes on upgrading to **SharePoint Connector 1.2** from an earlier version of the connector. For details of the new features and improvements in this release, please read the [SharePoint Connector 1.2 Release Notes](#).

On this page:

- [Upgrade Notes](#)
 - [Minimum Requirement is Confluence 2.10.0 or Later](#)
 - [Configuration Settings in SharePoint 2010 must be Reapplied](#)
 - [One Installer](#)
- [Upgrade Procedure](#)

Upgrade Notes

Minimum Requirement is Confluence 2.10.0 or Later

With the release of version 1.2, the SharePoint Connector no longer supports Confluence 2.8.x or 2.9.x. The minimum requirement is Confluence 2.10.0 or later. Please refer to the full details of the [supported platforms for SharePoint 2007](#) and [for SharePoint 2010](#)

Configuration Settings in SharePoint 2010 must be Reapplied

The configuration settings applied to Confluence during the installation of previous versions of the SharePoint Connector will remain untouched and will continue to apply to the new version of the Connector once you have installed it.

If you are upgrading to the latest version of the SharePoint Connector but remaining on Microsoft SharePoint 2007, then the configuration settings in SharePoint will also survive the upgrade.

If you are moving to Microsoft SharePoint 2010, you will need to reapply the configuration settings in SharePoint. See the [upgrade guide](#) for instructions.

One Installer

The SharePoint Connector zip file provides one installer (`Setup_WebParts.exe`) that works for both SharePoint 2007 and SharePoint 2010. The installer will detect the version of SharePoint installed on your machine.

Upgrade Procedure

There are two upgrade procedures to choose from:

- **Option 1: Upgrade your SharePoint Connector on SharePoint 2010.** This procedure assumes that you have upgraded your SharePoint server to Microsoft SharePoint 2010. To upgrade the connector, you will install the latest version of the SharePoint Connector plugin in Confluence and upgrade the SharePoint feature in Microsoft SharePoint 2010. See the [instructions](#).
- **Option 2: Upgrade your SharePoint Connector on SharePoint 2007.** This procedure assumes that you are running the SharePoint Connector on Microsoft SharePoint 2007. To upgrade the connector, you will install the latest version of the SharePoint Connector plugin in Confluence and upgrade the SharePoint feature in Microsoft SharePoint 2007. See the [instructions](#).



Need help?

If you encounter a problem during the upgrade, please create a [support ticket](#) and one of our support engineers will assist you through the process.

RELATED TOPICS

[SharePoint Connector 1.2 Release Notes](#)

SharePoint Connector 1.1.1 Release Notes

7 April 2010

Atlassian is proud to present the **Confluence SharePoint Connector 1.1.1**.

This release fixes a bug that affected the display of Confluence tree views on a SharePoint page. If the page contained more than one tree view from the same Confluence space, the second and following tree views did not work. This problem is now solved.

Previous versions of the SharePoint Connector gave users too much detail about certain error conditions. The connector now writes the detailed exception information to unified SharePoint logs instead. We have also fixed a memory leak. As a result of these two fixes, the SharePoint Connector is suitable for installation within the SharePoint Online hosted solution from Microsoft Online Services.

Don't have the Confluence SharePoint Connector yet?

Take a look at the new features and other highlights in the [SharePoint Connector 1.1 release notes](#) then follow our [installation guide](#).

Upgrading from a previous version of the SharePoint Connector

Please read the [SharePoint Connector 1.1 Upgrade Notes](#).

Updates and Fixes in this Release

JIRA Issues (6 issues)			
Key	Summary	Priority	Status
CSI-452	Drop JCIFS support		Closed
CSI-485	Session cannot be accessed in WSS		Closed
CSI-506	Modifying a Confluence Web Part clears the previous page selection		Closed
CSI-542	SPDisposeCheck reports errors for Atlassian.Confluence.SharePoint.dll		Closed
CSI-543	CAT.NET reports errors for Atlassian.Confluence.SharePoint.dll		Closed
CSI-567	Verify support for Confluence 3.2		Closed

SharePoint Connector 1.1 Release Notes



This release fixes a security flaw. Please refer to the [security advisory](#) for details of the security vulnerabilities, risk assessment and mitigation strategies.

18 January 2009

Atlassian is proud to present the **Confluence SharePoint Connector 1.1**.

This release of the SharePoint Connector supports federated searches of Confluence content in SharePoint. This replaces the original index search feature, which 'crawled' through cached content in Confluence. Federated searches use Confluence's own search engine to retrieve up-to-date and relevant matches, providing more accurate results than index searches.

You can now configure the SharePoint Connector to access a SharePoint site via an alternative URL, such as a URL that is only available from behind a firewall or VPN. This URL may therefore be different from the SharePoint address that is publicly available.

The SharePoint Connector requires **Confluence 2.8.0 or later**.

Upgrading from a previous version of the SharePoint Connector

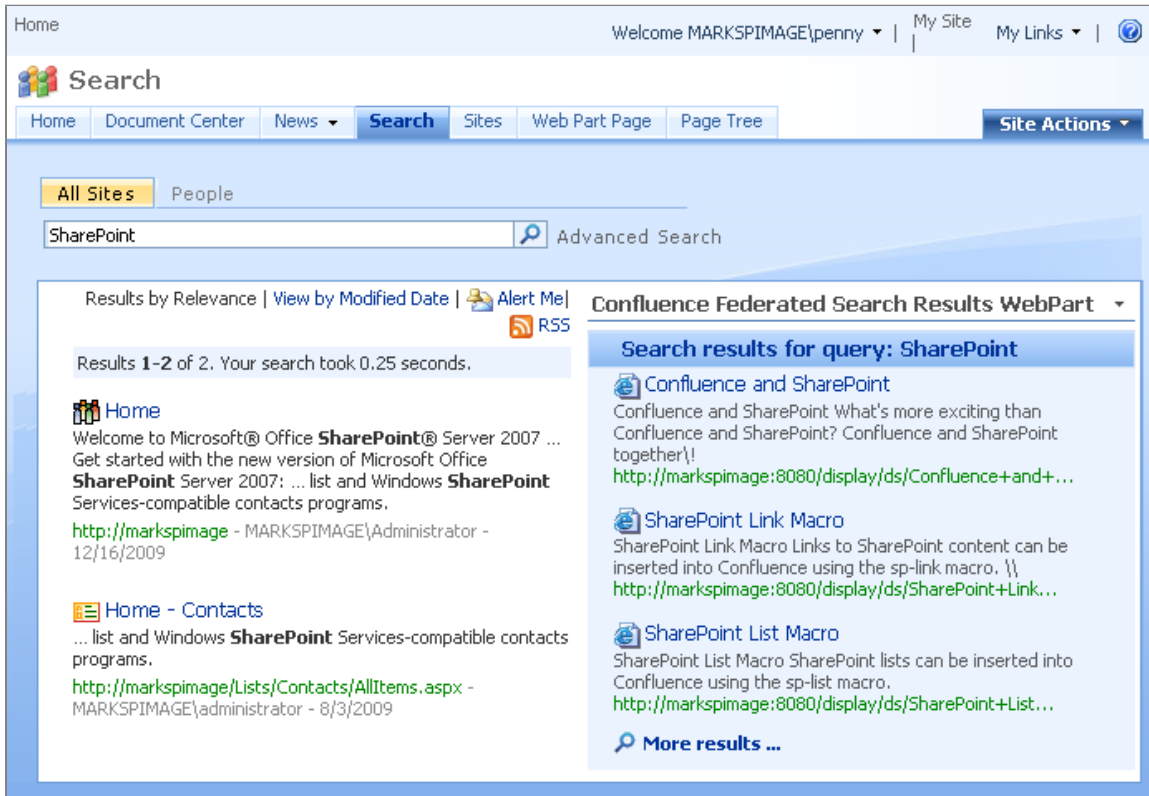
Please refer to the [SharePoint Connector 1.1 Upgrade Notes](#) for essential information about factors affecting your upgrade.



Enhanced Federated Search

The new search allows SharePoint to conduct improved federated searches on Confluence content. It completely replaces the old 'integrated index search' feature in previous versions of the SharePoint Connector. The new search brings several improvements:

- **More accurate and relevant results:** The old index search feature performed searches on Confluence's cached search indexes. Now the federated searches use Confluence's own search engine to conduct 'live' searches, resulting in more accurate, better ordered and more relevant search results.
- **More comprehensive searches:** Federated searches include Confluence metadata such as page labels, author details and comments.
- **Improved Confluence performance:** The old index search feature 'crawls' through Confluence's cached search indexes, which can impact Confluence's performance significantly. The new federated search feature only requires Confluence to perform a live search when a search is issued in SharePoint. This has much less impact on Confluence's performance.
- **Confluence permissions respected:** The new federated search function 'trims' search results more accurately than the old integrated index search feature. A 'trimmed' search result shows only Confluence content that the current user has permission to view through their Confluence account. This feature works across multiple Confluence installations too.



2





















































Alternative URL for Accessing SharePoint















You can now configure an 'alternative access URL' for SharePoint. This allows the SharePoint Connector to access a SharePoint site via an alternative URL, such as a URL that is only available from behind a firewall or VPN. This URL may therefore be different from the SharePoint address that is typically available to users or is publicly available.

The alternative URL also resolves problems where the SharePoint installation uses an authentication protocol not supported by Confluence, such as **NTLMv2** or **Kerberos**. You can configure SharePoint to run on a separate port that bypasses the unsupported authentication protocol, and then allow Confluence to communicate with SharePoint via this alternative URL.

Complete List of Fixes in this Release

JIRA Issues (36 issues)				
Key	Summary	Priority	Status	
CSI-522	Change "alternate" to "alternative" for alternative URL on SharePoint Integration Administration screen	↑	✓	Closed
CSI-521	Confluence navigation bar generates corrupt HTML when no default Sharepoint site is configured	⚠	✓	Closed
CSI-517	The SharePoint Admin screen in Confluence generates a "System Error" when editing existing SharePoint Sites.	⚠	✓	Closed

CSI-515	The "SharePoint Plugin" for Confluence does not appear in Confluence Administration Console's Plugin Repository Client.		 Closed
CSI-508	sp-link macro is frequently automatically disabled in Confluence		 Closed
CSI-504	SharePoint Theme in Confluence does not wrap the header correctly in IE7		 Closed
CSI-501	sp-list macro provides openings for XSS attacks		 Closed
CSI-497	SharePoint Federated Search is not authenticating with Confluence using Basic Authentication		 Closed
CSI-496	Example MOSS search URL in the Confluence SharePoint Admin UI is incorrect		 Closed
CSI-475	All Sharepoint settings in Confluence may be lost upon Confluence restart		 Closed
CSI-474	NTLM Authentication not passed through Sharepoint		 Closed
CSI-465	Confluence Page Web Part does not use Confluence server base URL		 Closed
CSI-462	SharePoint theme for Confluence 2.8+ is broken in Confluence 3.0		 Closed
CSI-456	Drop Sharepoint 2.7+ Theme		 Closed
CSI-455	Drop Support for Confluence < 2.8		 Closed
CSI-453	Federated Search Sharepoint -> Confluence		 Closed
CSI-452	Drop JCIFS support		 Closed
CSI-446	Seeing rapid reload in Internet Explorer when using Sharepoint Theme 2.8+ with AJAX pagetree plugin version 1.11		 Closed
CSI-444	Add Configuration for a Sharepoint External Base URL		 Closed
CSI-438	Crawl result returns labels concatenated in a single url separated by spaces (%20)		 Closed
CSI-436	"Must explicitly set a SearchContext to use when one cannot be inferred implicitly (typically from the HttpContext)." error when creating Sharepoint Search		 Closed
CSI-435	Allow Sharepoint evaluation licenses to be used with Commercial Confluence licenses		 Closed
CSI-434	pagetreesearch macro prevents Confluence page web part from functioning at all.		 Closed
CSI-410	Allow security trimmed federated search results		 Closed
CSI-406	Update recommended browser settings for Firefox 3.0		 Closed
CSI-381	pagetree macro does not work within Confluence Page web part		 Closed
CSI-249	Sharepoint Searchbox adds query twice to Confluence search form		 Closed
CSI-238	Feature Rich MOSS Search		 Closed
CSI-209	SharePoint REAMDE.TXT Format		 Closed

CSI-171	Use session properties for security trimmer web service connection		 Closed
CSI-159	Fix problem with configuring SharePoint crawl rule using Windows Authentication against Confluence running under IIS		 Closed
CSI-149	Showing Confluence 2.8 Tasklist in Web Part Breaks SharePoint Page		 Closed
CSI-148	SharePoint Search Configuration - Crawl Actions and Crawl Schedule		 Closed
CSI-140	Delete SharePoint Crawl Rule if we error out when creating a Confluence Search Source		 Closed
CSI-109	Security Trimmer Connection Configuration for Searching Across Multiple Confluence Installations		 Closed
CSI-14	Show Confluence icon for Confluence search results		 Closed

SharePoint Connector 1.1 Upgrade Notes

Below are some important notes on upgrading to **SharePoint Connector 1.1** from an earlier version of the connector. For details of the new features and improvements in this release, please read the [SharePoint Connector 1.1 Release Notes](#).



Instructions in this guide assume that you are upgrading from **SharePoint Connector 1.0.7**. If you are upgrading from an earlier version, your experience may be slightly different. Please contact [Atlassian support](#) for assistance if you need it.

On this page:

- [Upgrade Notes](#)
 - Minimum Requirement is Confluence 2.8.0 or Later
 - Good To Know: Configuration Settings Survive the Upgrade
- [Upgrade Procedure](#)
 - [Step 1: Move to the New Federated Search](#)
 - [Step 1.1: Remove the Old Crawled Search](#)
 - [Step 1.2: Check your SharePoint Updates and Upgrade SharePoint if Necessary](#)
 - [Step 1.3: Install OpenSearch Plugin into Confluence](#)
 - [Step 2: Upgrade the SharePoint Connector Plugin in Confluence](#)
 - [Step 3: Upgrade the SharePoint Connector Feature in SharePoint](#)
 - [Step 4: Set New Configuration Options](#)
 - [Step 4.1: Configure the Federated Search in SharePoint](#)
 - [Step 4.2: Configure the Alternative Access URL in Confluence](#)

Upgrade Notes

Minimum Requirement is Confluence 2.8.0 or Later

With the release of version 1.1, the SharePoint Connector no longer supports Confluence 2.7.x. The minimum requirement is **Confluence 2.8.0 or later**.

Good To Know: Configuration Settings Survive the Upgrade

The configuration settings applied to both Confluence and SharePoint during the installation of previous versions of the SharePoint Connector will remain untouched and will continue to apply to the new version of the Connector once you have installed it. :-)

Upgrade Procedure

Step 1: Move to the New Federated Search



You need MOSS. (WSS is not enough.)

Only Microsoft Office SharePoint Server ('MOSS') supports the new federated search. Plain Windows SharePoint Services ('WSS') does not support federated search. Please go to [step 2](#) if you do not plan to enable the new search feature.

If you would like to enable the new federated search feature, you will need to uninstall the crawled search feature installed by previous versions of the SharePoint Connector. Otherwise your search results will contain duplicate entries from Confluence.

Step 1.1: Remove the Old Crawled Search

1. Start the Windows SharePoint Services Administration Service.

- Run **Setup_Search.exe** from the previous SharePoint Connector version's installation package.



Setup_Search.exe is no longer included in the SharePoint Connector installer from version 1.1 onwards. If you need to get a fresh copy of the installer, you can download it from [the Atlassian download site](#).

- When prompted, select the '**Remove**' option to uninstall the feature from your SharePoint server. Wait for the uninstall to complete.
- Open your SharePoint Central Administration site and open the page for the Shared Services Provider (e.g. 'SharedServices1') that hosts the Confluence crawled search index.
- Delete the crawl rule for your Confluence instance.
- Delete the search scope for your Confluence instance.
- Delete the content source for your Confluence instance. (You may need to stop any in-progress crawls first, which could take several minutes to stop.)
- Select the '**reset all crawled content**' action.
- Perform a test search to ensure that Confluence entries no longer appear in your search results.

Step 1.2: Check your SharePoint Updates and Upgrade SharePoint if Necessary

The new federated search feature in SharePoint Connector 1.1 relies on new functionality in SharePoint. At least one of the following updates to SharePoint must be installed on your MOSS Server(s):

- Search Server 2008 Infrastructure Update (<http://blogs.msdn.com/sharepoint/archive/2008/07/15/announcing-availability-of-infrastructure-updates.aspx>).
- Service Pack 1 (<http://blogs.msdn.com/sharepoint/archive/2007/12/11/announcing-the-release-of-wss-3-0-sp1-and-office-sharepoint-server-2007-sp1>)).
- Service Pack 2 (<http://blogs.msdn.com/sharepoint/archive/2009/04/28/announcing-service-pack-2-for-office-sharepoint-server-2007-and-windows-sha>)).

We recommend **Service Pack 2**, which is the most recent update. If you need to install one of these updates, you should schedule this upgrade of SharePoint **before** proceeding with the SharePoint Connector 1.1 installation.


Step 1.3: Install OpenSearch Plugin into Confluence

- Install the Atlassian-supported [OpenSearch plugin](#) on the Confluence instance, if not already installed. You can install this plugin via your Confluence Plugin Repository.

Step 2: Upgrade the SharePoint Connector Plugin in Confluence

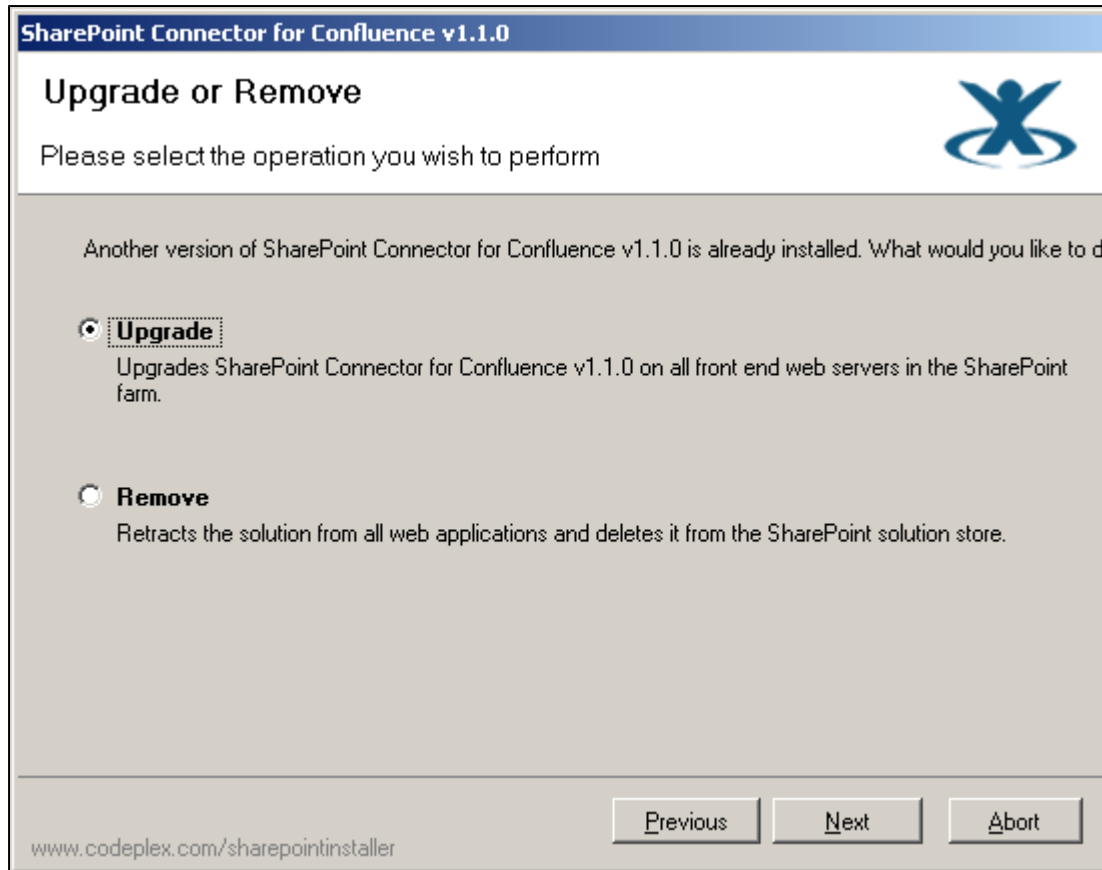
- Upgrade the SharePoint Connector plugin via the Confluence Plugin Repository:
 - Go to the Confluence '**Administration Console**'. To do this:
 - Open the '**Browse**' menu and select '**Confluence Admin**'. The 'Administration Console' view will open.
 - Click '**Plugin Repository**' in the 'Configuration' section of the left-hand navigation panel to open the 'Atlassian Plugin Repository' page.
 - Scroll down to the row indicating '**SharePoint Plugin**' and click '**Upgrade**'.
- You may need to restart Confluence after upgrading the Confluence SharePoint Connector plugin.

If you do not see the '**Upgrade**' option, please follow these steps instead:

- Click '**Plugins**' in the 'Configuration' section of the left-hand navigation panel (not 'Plugin Repository').
 - Select the '**SharePoint Connector for Confluence**' plugin.
 - Click '**Uninstall**' to remove the plugin from your Confluence site.
 - Click '**Plugin Repository**' in the 'Configuration' section of the left-hand navigation panel to open the 'Atlassian Plugin Repository' page.
 - Scroll down to the row for the '**SharePoint Plugin**' and click '**Install**'.
-  Provided you do not restart Confluence after uninstalling the old version of the plugin, you will not lose your configuration settings and SharePoint Connector license details.

Step 3: Upgrade the SharePoint Connector Feature in SharePoint

- Download the SharePoint component from the [SharePoint Connector download centre](#).
- Extract the contents of the downloaded `SharePointConnector` zip file and open the `SharePoint Installer` directory.
- Upgrade the SharePoint features by running **Setup_WebParts.exe**. Select the option to '**Upgrade**' the SharePoint Connector. Follow the prompts by selecting '**Next, Next, ..., Finish**'.



4. You may need to restart IIS after upgrading the Sharepoint Connector feature.

Step 4: Set New Configuration Options

Step 4.1: Configure the Federated Search in SharePoint



Required only if using the new federated search

Please go to [step 4.2](#) if you do not plan to enable the new search feature.

1. Follow [these instructions](#) to configure a new federated search location for Confluence.

Step 4.2: Configure the Alternative Access URL in Confluence

SharePoint Connector 1.1 contains a new configuration option in Confluence that was not available in the previous version. This option allows Confluence to access SharePoint via a secondary URL.

1. Review the [documentation for the alternative access URL](#).
2. Apply the setting to your environment if required.



Need help?

If you encounter a problem during the upgrade, please create a [support ticket](#) and one of our support engineers will assist you through the process.

RELATED TOPICS

[SharePoint Connector 1.1 Release Notes](#)

SharePoint Connector 1.0 Release Notes

This is the first officially supported version of the Confluence SharePoint Connector.


































Highlights of features and enhancements in this release:

- Confluence and Web Part version information was added to the Confluence Settings screen.
- The location of validation messages for the test button on the Confluence Settings screen was updated.
- The assembly version information for the first non-beta release was updated.

Notable bug fixes in this release:

- An issue with the internal SharePoint version check (MOSS vs. WSS) was resolved.
- The Confluence Settings screen would not load successfully due to a false positive when checking for MOSS. This occurred with an installation running WSS 3.0 with Project Server.
- Many styling issues with Confluence 2.8 were resolved.

List of updates and fixes in this release:

JIRA Issues (11 issues)					
Type	Key	Summary	Priority	Status	Resolution
	CSI-227	SharePoint Forms Based Authenticated Users Cannot Show Confluence Content		 Closed	Fixed
	CSI-223	Update support FAQ items as appropriate		 Closed	Fixed
	CSI-213	Installing Hotfix over Remote Desktop		 Closed	Fixed
	CSI-211	Installation order is confusing		 Closed	Fixed
	CSI-210	Authentication Configuration - put recommendations near top		 Closed	Fixed
	CSI-208	Remove all references to ThreeWill and "twiki" from documentation		 Closed	Fixed
	CSI-177	A user is not presented with an option to correct their stored SSO password if the password was originally entered incorrectly		 Closed	Fixed
	CSI-84	make sure that the client-config.wsdd needed for NTLM is optionally written out to the classes dir by this plugin		 Closed	Fixed
	CSI-35	Confluence Permission Checker does not work when loaded dynamically		 Closed	Fixed
	CSI-31	Add site level configuration in addition to space level config		 Closed	Fixed
	CSI-18	Check Permissions before showing Edit Page link		 Closed	Fixed

For a changelog of updates and fixes in subsequent Confluence SharePoint Connector 1.0 bug fix releases, please refer to the [SharePoint Connector 1.0 Changelog](#).

For support-related issues, see refer to our [Support site](#).

SharePoint Connector 1.0 Changelog

This page is a changelog of updates and fixes in Confluence SharePoint Connector 1.0 bug fix releases.







On this page:





































- [Versions 1.0.6 - 1.0.7](#)
- [Version 1.0.5](#)
- [Version 1.0.4](#)
- [Version 1.0.3](#)
- [Version 1.0.2](#)

Versions 1.0.6 – 1.0.7**19th August 2009**

The macro browser implementation of the SharePoint list macro has been improved, with enhanced descriptions and previewing functionality.







This release includes the following updates and fixes:

JIRA Issues (14 issues)					
Type	Key	Summary	Priority	Status	Resolution
	CSI-467	Confluence and Sharepoint on different machines causes IE7 XSS failure		 Closed	Fixed
	CSI-464	sp-list macro should work with the Macro Browser in Confluence 3.0		 Closed	Fixed

	CSI-448	Support display of folder and its contents for document library		 Closed	Fixed
	CSI-447	Failure to send auth request to Confluence results in complete web part failure		 Closed	Fixed
	CSI-440	Incorrect Priority in Admin Field Validation		 Closed	Fixed
	CSI-439	Selecting space for Web Part fails for subsequent selections		 Closed	Fixed
	CSI-417	sp-list not properly displaying the contents of a document folder		 Closed	Fixed
	CSI-403	Allow SharePoint to federate its search to Confluence		 Closed	Fixed
	CSI-402	Casing error when creating a confluence search source		 Closed	Fixed
	CSI-394	Broken links in Confluence Page web part may be caused by Server base URL		 Closed	Fixed
	CSI-298	Update Confluence Settings screen in SharePoint to show file build version number		 Closed	Fixed
	CSI-240	Allow entry of page name or URL for the Confluence Page web part		 Closed	Fixed
	CSI-205	Allow for search security trimming diagnostics		 Closed	Fixed
	CSI-204	Allow for configuring a Confluence Search Source without using a security trimmer		 Closed	Fixed




Version 1.0.5

This release included the following updates and fixes:

JIRA Issues (2 issues)					
Type	Key	Summary	Priority	Status	Resolution
	CSI-403	Allow SharePoint to federate its search to Confluence		 Closed	Fixed
	CSI-399	Update Sharepoint Connector on the Sharepoint side to use Axis RPC Web services on Confluence rather than the outdated Glue ones.		 Closed	Fixed

Version 1.0.4

This release included the following updates and fixes:

JIRA Issues (1 issues)					
Type	Key	Summary	Priority	Status	Resolution
	CSI-61	Allow Confluence to integrate with multiple SharePoint servers		 Closed	Fixed










Version 1.0.3

This release included the following updates and fixes:

JIRA Issues (1 issues)					
Type	Key	Summary	Priority	Status	Resolution
	CSI-242	sp-list links may include double "http://http/"		 Closed	Fixed

Version 1.0.2

This release included the following updates and fixes:

JIRA Issues (3 issues)					
Type	Key	Summary	Priority	Status	Resolution
	CSI-251	Searchbar isn't working correctly		 Closed	Fixed
	CSI-230	Plugin instruction inconsistencies		 Closed	Fixed
	CSI-147	Plugin cannot access SharePoint if SharePoint is using SSL		 Closed	Fixed

Installing the SharePoint Connector

This page describes the requirements and installation procedures for the **SharePoint Connector 1.3**.

- [Installing the SharePoint Connector on SP 2007](#)
- [Installing the SharePoint Connector on SP 2010](#)

Installing the SharePoint Connector on SP 2007

This page describes the requirements and installation procedures for the **SharePoint Connector 1.3** on **SharePoint 2007**.

Prerequisites and Planning your Configuration

1. Check the [system requirements and supported platforms](#).
2. Plan your configuration, using our [guidelines on selecting a supported authentication configuration](#).

Installation and Configuration

Install and configure the components in this order:

1. [Configure the access to SharePoint](#).
2. [Install and configure the plugins in Confluence](#).
3. [Configure the access to Confluence](#).
4. [Install and configure the feature in SharePoint](#).

Planning your Environment with SP 2007

This section provides guidelines on planning the infrastructure and configuration necessary to support your installation of the Confluence SharePoint Connector.

These instructions apply if you are using the connector with **SharePoint 2007**. If you have SharePoint Foundation 2010 or SharePoint Server 2010, please refer to the [planning guide for SharePoint 2010](#).

On this page:

- [Prerequisites and Supported Platforms](#)
- [Supported Configurations](#)
 - [Configuring Access to SharePoint](#)
 - [Selecting your Configuration for Access to SharePoint](#)
 - [Configuring Access to Confluence](#)
 - [Selecting your Configuration for Access to Confluence](#)
- [Unsupported Configurations](#)
 - [Atlassian Crowd](#)
 - [SiteMinder and other Single Sign-On Management Solutions](#)
 - [SharePoint Forms-Based Authentication](#)
- [Next Step](#)

Prerequisites and Supported Platforms

Please ensure you read through and comply with the following requirements before installing the SharePoint Connector.

Windows

The Confluence SharePoint Connector supports the same Windows operating system requirements as those specified by Microsoft for SharePoint.

Confluence

The latest version of the SharePoint Connector supports **Confluence 2.10.0 and later**. You can download Confluence from the [Confluence download centre](#).



.NET Framework required on Windows

Note that if you are running Confluence on a Windows Server, you should ensure that the Microsoft .NET Framework 2.0 is installed. Microsoft .NET is required for Confluence in certain configurations (see the guide on [Configuring Access to SharePoint with SP 2007](#) for more information).

You can download the .NET Framework 2.0 [here](#) (for the 32-bit version) or [here](#) (for the 64-bit version).

SharePoint



These instructions apply if you are using the connector with **SharePoint 2007**. If you have SharePoint Foundation 2010 or SharePoint Server 2010, please refer to the [planning guide for SharePoint 2010](#).

All released versions of the SharePoint Connector support the 2007 Microsoft Office Server System. This includes Windows SharePoint Services ('WSS') 3.0 and Microsoft Office SharePoint Server ('MOSS') 2007. For a quick guide to the different SharePoint versions available,

see our [comparison of SharePoint versions and editions](#). Some features of the SharePoint Connector are only available when using MOSS, as described below.









1. You will need **Windows SharePoint Services (WSS) 3.0**.
 - To check if WSS is installed, go to **Start -> All Programs -> Administrative Tools -> SharePoint 3.0 Central Administration**. If you can see 'SharePoint 3.0 Central Administration', then WSS 3.0 has already been installed.
2. (Optional) For added functionality, you need **Microsoft Office SharePoint Server (MOSS) 2007** (Standard or Enterprise)
 - MOSS is **required** for the following features:
 - a. For the Federated Search feature. For more information, see [Configuring the SharePoint Federated Search on SP 2007](#).
 - b. For Single Sign-On (SSO) functionality from SharePoint using Windows Integrated Authentication to Confluence via Forms Based Authentication. For more information, see the [Microsoft product information](#).
 - For the Confluence SharePoint Connector, it makes no difference whether you have MOSS Standard or MOSS Enterprise edition.

Checking whether you have WSS or MOSS

To determine whether you have WSS 3.0 or MOSS 2007 installed, go to Windows **Start -> Control Panel -> Add/Remove Programs**.

- If you see 'Microsoft Office SharePoint Server 2007' in the list, then MOSS 2007 has been installed.
- If you see only 'Microsoft Windows SharePoint Services' in the list (and not 'Microsoft Office SharePoint Server 2007') then you only have WSS 3.0 installed.

Table: SharePoint Connector feature compatibility matrix

Feature	Supported in WSS	Supported in MOSS
Embed Confluence content in SharePoint (Web Parts)		
Embed SharePoint content in Confluence (Macros)		
Integration with Microsoft Single Sign-On		
Federated Search		



We recommend separate server machines for Confluence and SharePoint

Due to the substantial memory and CPU requirements of SharePoint, we recommend that you run Confluence and SharePoint on separate machines. For evaluation purposes, it is OK to run them both on the same machine.

Supported Configurations

Next, please decide which of the supported configurations is best suited to your environment. There are two areas to consider when setting up the SharePoint Connector and deciding which authentication methods to use:

- Configuring access to SharePoint
- Configuring access to Confluence

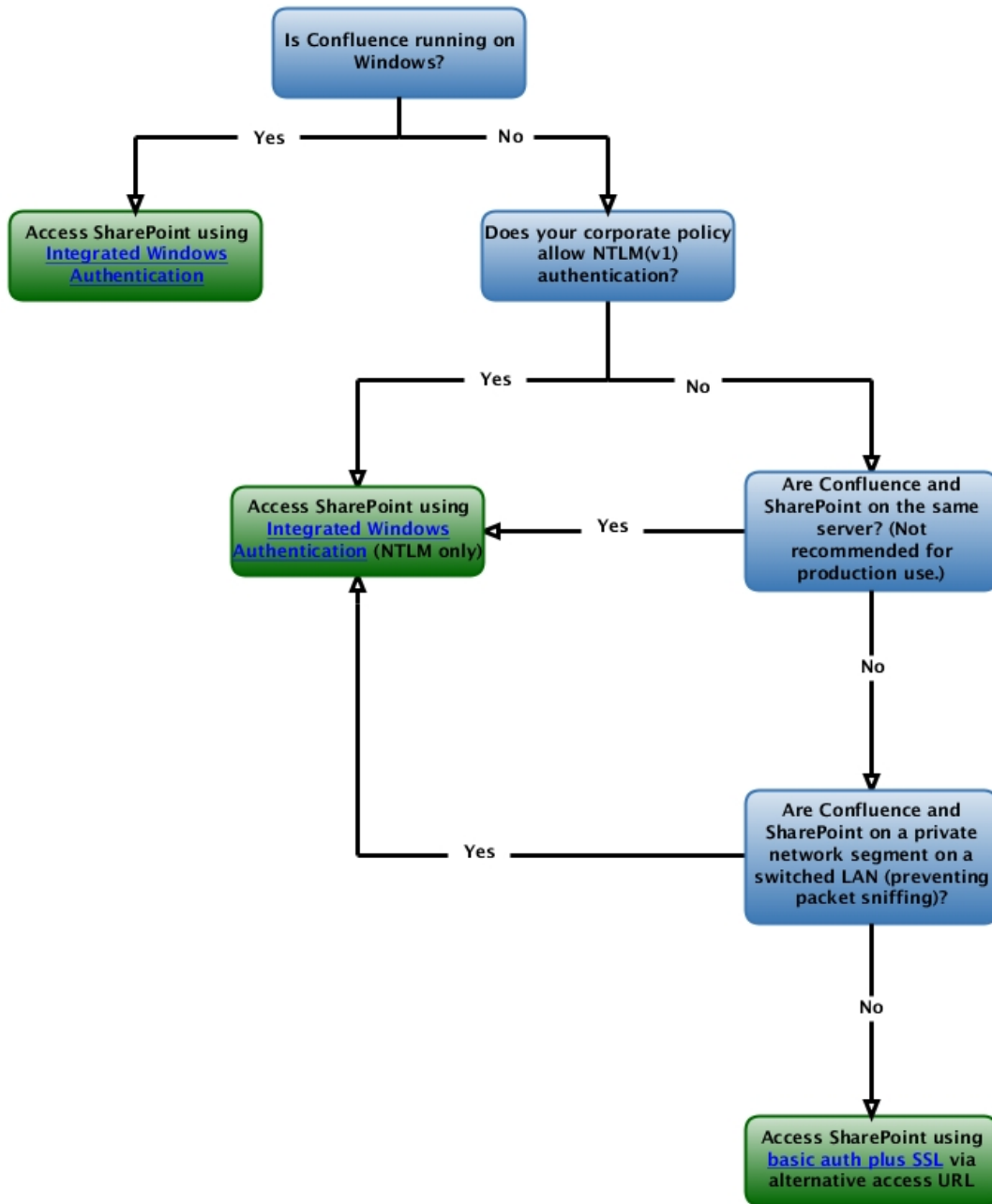
Configuring Access to SharePoint

These configurations control the authentication method used by the Confluence server and client browsers when requesting content from the SharePoint server.

- [Access SharePoint using Integrated Windows Authentication with SP 2007](#)
- [Access SharePoint using Integrated Windows Authentication \(NTLM Only\) with SP 2007](#)
- [Access SharePoint using Basic Authentication and SSL \(via Alternative Access URL\) with SP 2007](#)

Selecting your Configuration for Access to SharePoint

Configuring the Access to Microsoft SharePoint 2007 When Using the SharePoint Connector



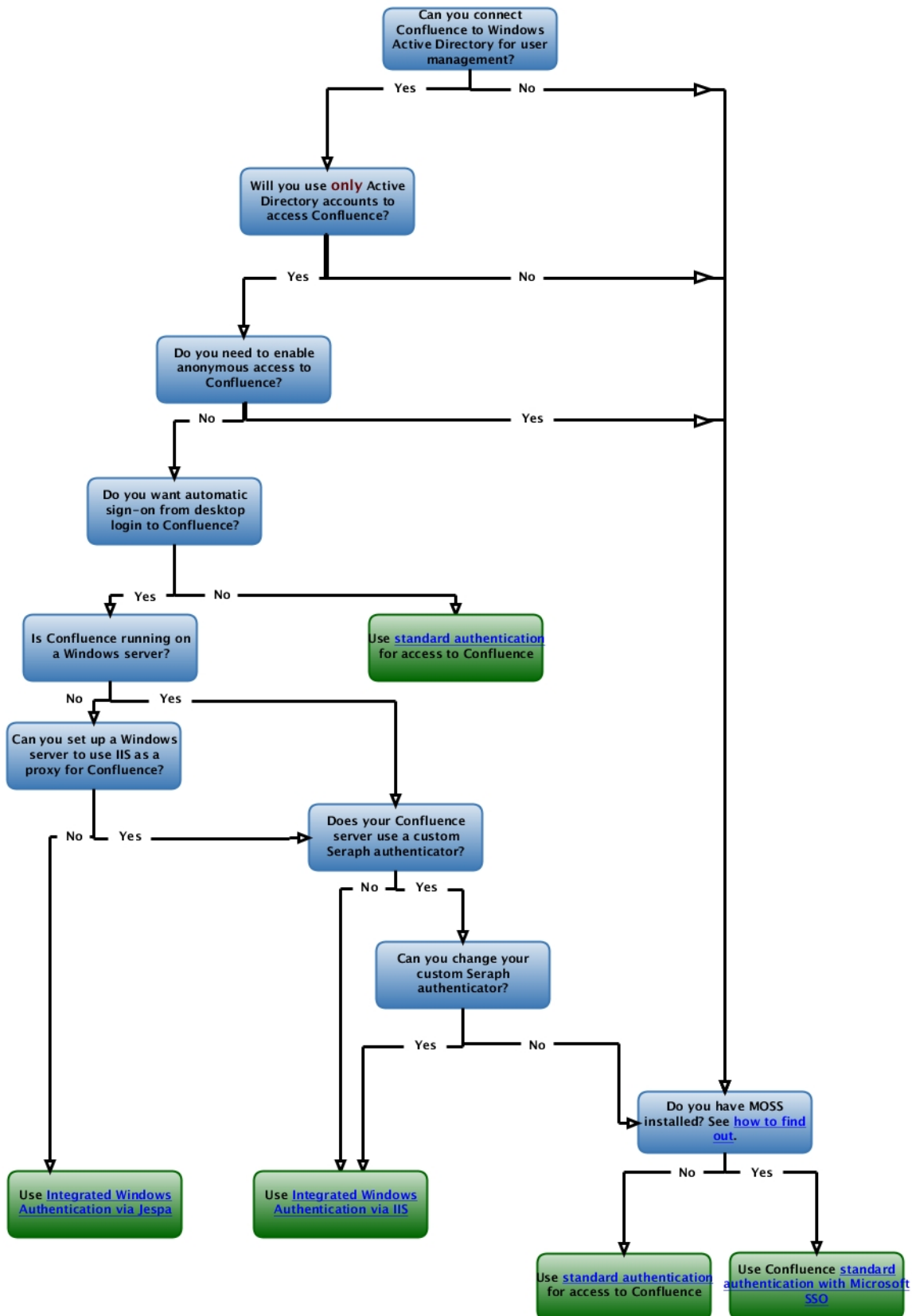
Configuring Access to Confluence

These configurations control the authentication method used by the SharePoint server and client browsers when requesting content from the Confluence server.

- Access Confluence using Integrated Windows Authentication via IIS with SP 2007
- Access Confluence using Integrated Windows Authentication via Jespa with SP 2007
- Access Confluence using Standard Authentication with SP 2007
- Access Confluence using Standard Authentication with Microsoft SSO on SP 2007

Selecting your Configuration for Access to Confluence

Configuring the Access to Confluence When Using the SharePoint Connector with SP 2007



Unsupported Configurations

Atlassian support does not cover the configurations listed below.

Atlassian Crowd



Not supported:

Crowd is Atlassian's single sign-on (SSO) and user management solution. For the initial release of the SharePoint Connector, we made a decision to delay full support for Crowd in favour of Microsoft's Single Sign-On Service (Microsoft SSOsrv). At the time, we felt that Microsoft SSOsrv's tight integration with SharePoint was a more compelling feature for SharePoint customers.

As the SharePoint Connector matures, we are now looking at expanding our support to reach a broader customer base. We hope to support Crowd for SSO in the future.

If you are interested in this feature, we encourage you to vote for the feature request in our JIRA issue tracker: [CSI-588](#).

SiteMinder and other Single Sign-On Management Solutions



Microsoft SSO and Secure Store Service are supported:

We have tested the connector with the following single sign-on solutions from Microsoft:

- Single Sign-On Service, provided with MOSS 2007.
- Secure Store Service provided with SharePoint Server 2010 (available with version 1.2 and later of the SharePoint Connector).



Not supported:

We have not tested any other single sign-on products. If you are interested in support for other SSO solutions, we encourage you to vote for the relevant request if it already exists in our JIRA issue tracker or create a new request. When voting or adding a request, please describe your environment.

- Request for SiteMinder integration: [CSI-218](#)

SharePoint Forms-Based Authentication



Not supported:

The SharePoint Connector cannot connect to SharePoint sites that use an ASP.NET Forms authentication provider. We may add support for this configuration in the future. If you are interested in this feature, we encourage you to vote for the feature request in our JIRA issue tracker: [CSI-590](#).

Next Step

To continue with the installation of the SharePoint Connector, please [configure the access to SharePoint](#).

Configuring Access to SharePoint with SP 2007

This section describes the methods which may be used to **configure access to SharePoint** for the SharePoint Connector. You should complete one of the supported configuration guides before proceeding further with the SharePoint Connector installation. If you have not already seen our guide to [planning your environment](#), please refer to it now for information that will help you select the best configuration for your environment. These instructions apply to SharePoint 2007.

Please follow one of these configuration guides:

- [Access SharePoint using Integrated Windows Authentication with SP 2007](#)
- [Access SharePoint using Integrated Windows Authentication \(NTLM Only\) with SP 2007](#)
- [Access SharePoint using Basic Authentication and SSL \(via Alternative Access URL\) with SP 2007](#)

Next Step

To continue with the installation of the SharePoint Connector, please [install and configure the Confluence plugins](#).

Access SharePoint using Integrated Windows Authentication with SP 2007

This page is part of the installation guide for the **Confluence SharePoint Connector**. It tells you about accessing SharePoint via Integrated Windows Authentication. These instructions apply to SharePoint 2007.

On this page:

- [Overview](#)
- [Installation Instructions](#)
- [Next Step](#)

Overview

In this configuration, both Confluence and client browsers authenticate against SharePoint using Integrated Windows Authentication (IWA).

Use this Configuration when...

- Confluence is running on a Windows server.

If you have not already seen our guide to [planning your environment](#), you can refer to it for information that will help you select the best configuration for your environment.

Installation Instructions

IWA is the default configuration for your SharePoint server. No additional configuration to SharePoint is required.

However, you must ensure that Microsoft .NET Framework 2.0 is installed on your Confluence server. You can download the .NET Framework 2.0 [here](#) (for the 32-bit version) or [here](#) (for the 64-bit version).

Next Step

To continue with the installation of the SharePoint Connector, please [install and configure the Confluence plugins](#).

You can download the .NET Framework 2.0 [here](#) (for the 32-bit version) or [here](#) (for the 64-bit version).

Access SharePoint using Integrated Windows Authentication (NTLM Only) with SP 2007

This page is part of the installation guide for the **Confluence SharePoint Connector**. It tells you how to configure access to SharePoint using Integrated Windows Authentication (NTLM only). These instructions apply to SharePoint 2007.

On this page:

- [Overview](#)
- [Caveats](#)
 - [NTLM Only](#)
 - [Additional Layers of Security](#)
- [Installation Instructions](#)
 - [Domain or Local?](#)
 - [LAN Manager Authentication Level](#)
 - [Reboot Your SharePoint Server](#)
- [Next Step](#)

Overview

In this configuration, both Confluence and client browsers authenticate against SharePoint using Integrated Windows Authentication (NTLM only).

Use this Configuration when...

- Confluence is **not** running on a Windows server. (If Confluence is running on Windows, you can use [full IWA](#).)
- There is minimal risk of eavesdropping on the network traffic from Confluence to SharePoint. Examples of scenarios involving minimal risk include:
 - The Confluence and SharePoint applications are on the same physical server. (For production use, we recommend that you run Confluence and SharePoint on separate machines, but you may choose to run them on the same server for evaluation purposes.)
 - The SharePoint site(s) are accessed using HTTP Secure (HTTPS).
 - The Confluence and SharePoint servers are on a private network segment.

If you have not already seen our guide to [planning your environment](#), you can refer to it for information that will help you select the best configuration for your environment.

Caveats

NTLM Only

When configuring authentication for a top-level SharePoint site, the **SharePoint Central Administration** application allows administrators to select Integrated Windows Authentication using NTLM or Kerberos (or both).

Due to the limited number of authentication methods supported by the SharePoint Connector's Java components (see the section on additional layers of security [below](#)), in order for a site collection to be accessible from Confluence, the NTLM authentication option **must** be selected.

Additional Layers of Security

If you are concerned about the possibility of password hashes sent from Confluence to SharePoint being captured and decoded by a third party, Atlassian recommends that you apply additional layers of security (such as HTTP Secure) if you use this configuration.

Because Confluence is written in Java, it has a dependency on the Sun Java Virtual Machine's (JVM's) internal NTLM implementation to decode NTLM challenge messages from the server and issue encoded NTLM responses. Our testing of the SharePoint Connector with recent versions of the Sun JVM (1.6.*) indicate that the JVM is only able to reliably work with the NTLM and LAN Manager (LM) Windows Authentication protocols. Newer (and more secure) protocols such as NTLMv2 and Kerberos are not supported in this configuration.

LM authentication and to a lesser extent, NTLM, are regarded as weak authentication mechanisms and there are widely accessible tools for deciphering passwords encrypted with LM and NTLM. Atlassian recommends that you apply additional layers of security (such as HTTP Secure) if you use this configuration.

Installation Instructions

Domain or Local?

If your Windows user accounts are stored in Active Directory, then the configuration steps listed here must be applied to all **Domain Controllers**. If your user accounts are local accounts on the SharePoint Server, then the configuration steps must be applied to your **SharePoint server**.

LAN Manager Authentication Level

The LAN Manager Authentication Level controls what network authentication methods are supported by Windows clients and servers. The authentication level is controlled via a registry entry (called **LMCompatibilityLevel**) or a group policy setting (called **Network Security: LAN Manager Authentication Level**).

In order for Confluence to successfully authenticate against the SharePoint server, the LAN Manager Authentication Level must be set to one of the following values:

Registry Key Value	Group Policy Value
0	Send LM & NTLM responses
1	Send LM & NTLM - use NTLMv2 session security if negotiated
2	Send NTLM response only
3	Send NTLMv2 response only
4	Send NTLMv2 response only. Refuse LM

For more information on how to alter this setting and greater detail on what the value of each setting entails, please consult this [Microsoft TechNet article](#).

Note that this registry value does not need to be modified on the Confluence server. Confluence uses a Java HTTP client that is unaware of the Windows configuration.

Symptoms of Unsupported LM Authentication Level

Using an unsupported LAN Manager Authentication Level will have the following results:

- SharePoint will return an error: `'HTTP 401.1 Unauthorised: Access is denied due to invalid credentials'`.
- The error message you may see in Confluence is: `'org.apache.cxf.Interceptor.Fault: Could not send Message'`.

Reboot Your SharePoint Server

We strongly recommend that you restart your SharePoint server after applying any of these configuration settings in order to ensure that they take effect.

Additionally, changes to your group policy may take a short while to propagate through your domain. Please keep this in mind when testing your configuration.

Next Step

To continue with the installation of the SharePoint Connector, please [install and configure the Confluence plugins](#).

Access SharePoint using Basic Authentication and SSL (via Alternative Access URL) with SP 2007

This page is part of the installation guide for the **Confluence SharePoint Connector**. It tells you how to configure access to SharePoint using basic authentication and SSL via an alternative access URL in SharePoint. These instructions apply to SharePoint 2007.

On this page:

- [Overview](#)
- [Caveats](#)

- [Server Certificate](#)
- [Installation Instructions](#)
 - [Configuring SharePoint](#)
 - [Step 1: Extend the SharePoint Site to Another IIS Web Site](#)
 - [Step 2: Configure the IIS Authentication Providers](#)
 - [Step 3: Configure the Alternate Access Mappings](#)
 - [Step 4: Import the SSL Certificate into IIS](#)
 - [Step 5: Restrict the IIS Web Site to Confluence](#)
 - [Configuring Confluence](#)
 - [Step 1: Trust SharePoint's SSL Certificate](#)
 - [Step 2: Configure the Alternative URL in Confluence](#)

Overview

In this configuration, client browsers authenticate against SharePoint using Integrated Windows Authentication (NTLM or Kerberos). Confluence however, authenticates against SharePoint on a separate port that is configured to use basic authentication over Secure Sockets Layer (SSL). This is accomplished using SharePoint's capability to extend a site collection over multiple web applications. Using alternative access mappings in SharePoint, all hyperlinks in the SharePoint content direct users back to the primary SharePoint site.

This configuration method offers a greater level of security than the method that [accesses SharePoint using Integrated Windows Authentication \(NTLM Only\)](#). The configuration procedure is, however, more complex. You should review the security measures of your internal network before deciding which method is most appropriate for your environment.

Use this Configuration when...

- Confluence is **not** running on a Windows server.
- Your corporate security policy prohibits the use of NTLM(v1) authentication, which is necessary for the [NTLM](#) configuration.
- Your SharePoint site(s) is/are not configured to use Secure HTTP (HTTPS) and you are concerned about the possibility of packet sniffing or eavesdropping.

If you have not already seen our guide to [planning your environment](#), you can refer to it for information that will help you select the best configuration for your environment.

Caveats

Server Certificate

Enabling SSL requires the installation of a certificate on the SharePoint server. Depending on the way in which you source the certificate, this could involve either an additional financial cost or a number of additional configuration steps.

Installation Instructions

Configuring SharePoint



Use IE7+ when Configuring SharePoint

We recommend that you use Internet Explorer 7 or later to perform the configuration steps described on this page. You may experience unusual behaviour if you use FireFox or other browsers on some SharePoint administrative pages.



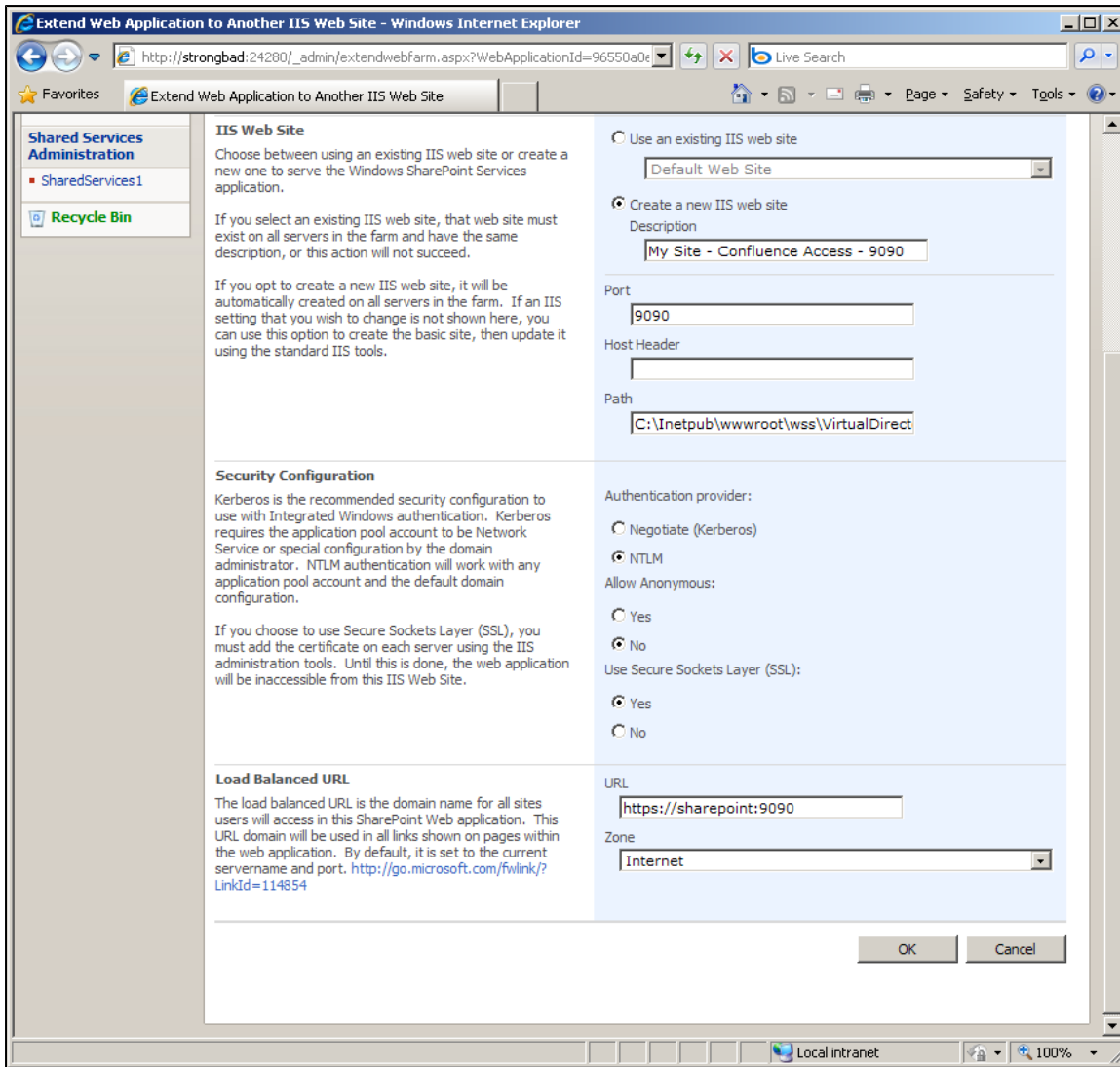
Configure all SharePoint Top-Level Sites used by Confluence

You will need to perform these configuration steps for each SharePoint top-level site that is exposed to Confluence.

Step 1: Extend the SharePoint Site to Another IIS Web Site

1. Log in to SharePoint Central Administration and select the '**Application Management**' portal.
2. In the '**SharePoint Web Application Management**' section, select '**Create or extend Web application**'.
3. Select '**Extend an existing Web application**'.
4. Set the '**Web Application**' field to the IIS web application that is hosting the SharePoint site you wish to extend.
5. Fill out the details of the new web application:
 - Ensure that the IIS web site is assigned a unique port that is not currently in use on your SharePoint server.
 - Ensure that '**Allow Anonymous**' is set to '**No**'.
 - Ensure that '**Use Secure Sockets Layer (SSL)**' is set to '**Yes**'.
 - Make a note of the '**Zone**' that is set for the '**Load Balanced URL**'. You will need to know this zone in step 2 [below](#).
6. Click '**OK**'.

[Screenshot: Extending the SharePoint site to another IIS web site](#)



Step 2: Configure the IIS Authentication Providers

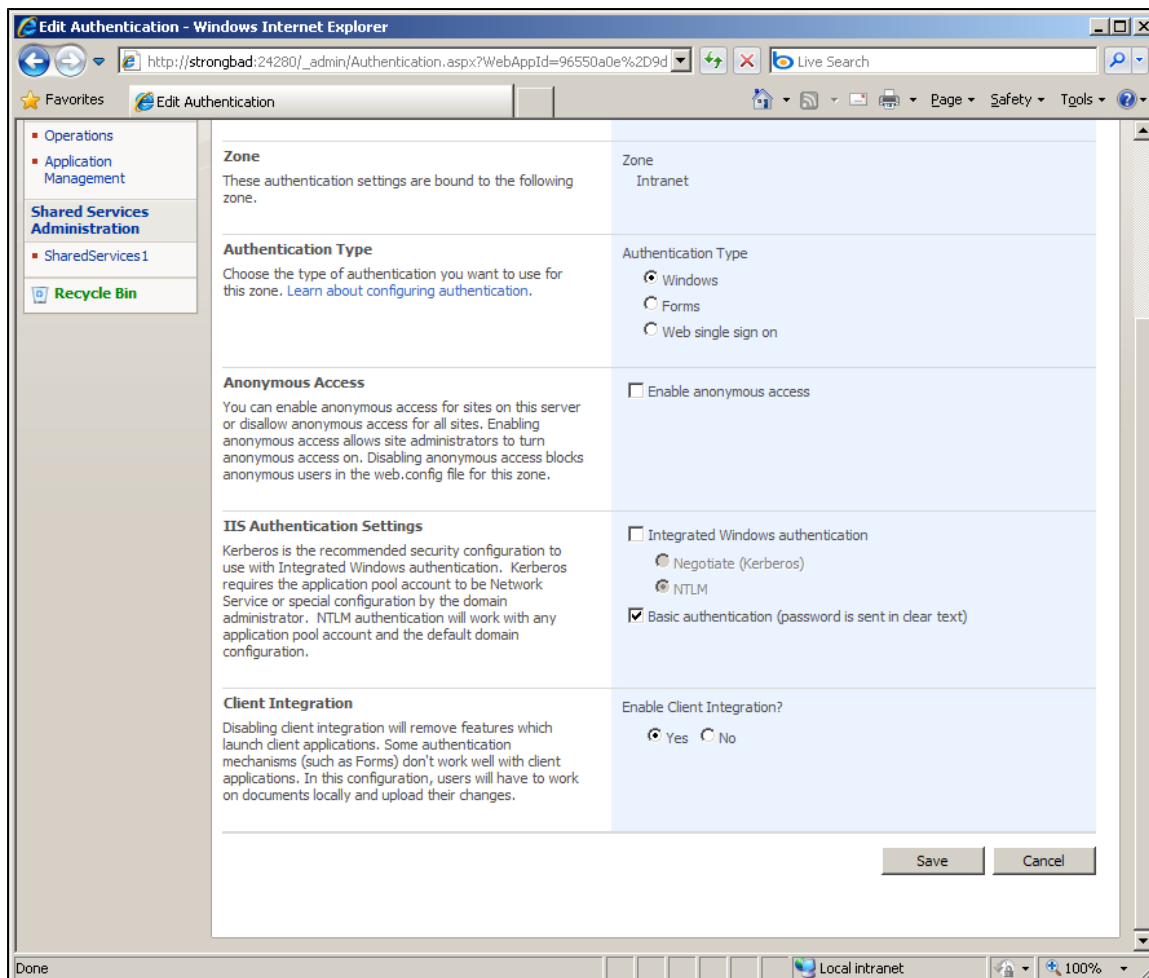
1. Go back to SharePoint Central Administration and select the '**Application Management**' portal.
2. In the '**Application Security**' section, select '**Authentication providers**'.
3. Click the **Zone** that you used to extend the SharePoint site in step 1 above.
4. In the '**IIS Authentication Settings**' section, ensure that '**Integrated Windows authentication**' is not selected and '**Basic authentication (password is sent in clear text)**' is selected.
5. Click '**Save**'.



SSL will secure the password information

Because this endpoint will be using Secure Sockets Layer (SSL), the password will not be sent in clear text even though basic authentication is used.

Screenshot: Editing the IIS authentication settings

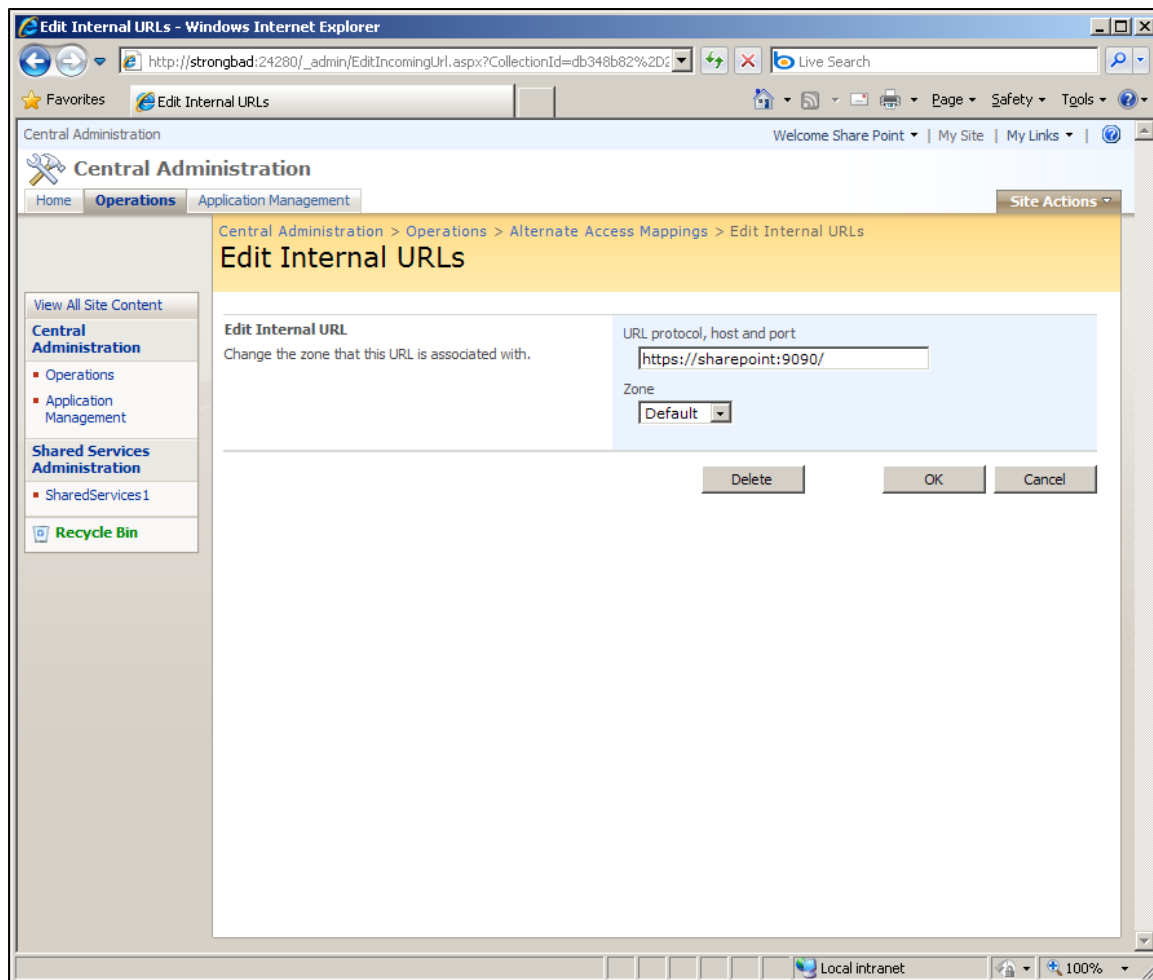


Step 3: Configure the Alternate Access Mappings

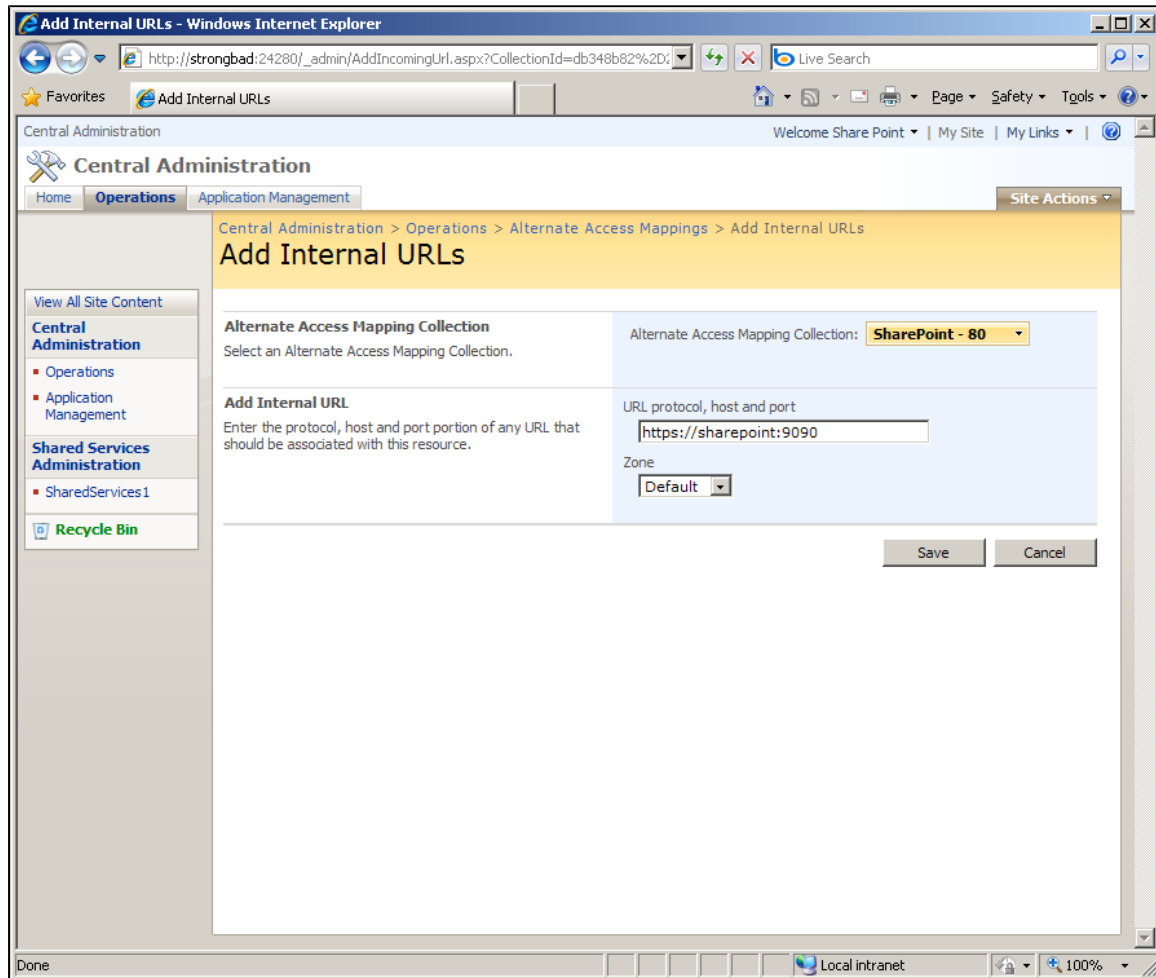
In this step you will remove the default public URL that SharePoint created during the previous step and replace it with an internal URL mapping.

1. Go back to SharePoint Central Administration and select the '**Operations**' portal.
2. In the '**Global Configuration**' section, select '**Alternate Access Mappings**'.
3. Locate the '**Internal URL**' that represents the newly-created IIS web site defined in step 1 above and click the link.
4. Click the '**Delete**' link to remove this mapping.

Screenshot: Deleting the alternate access mapping



5. Click '**Add Internal URLs**'.
6. Select the '**Alternate Access Mapping Collection**' that represents the root SharePoint site that you are extending.
7. Set the '**URL protocol, host and port**' to the URL that directs to the newly-created IIS web site defined in step 1 [above](#).
8. Click '**Save**'.

Screenshot: Adding the alternate access mapping

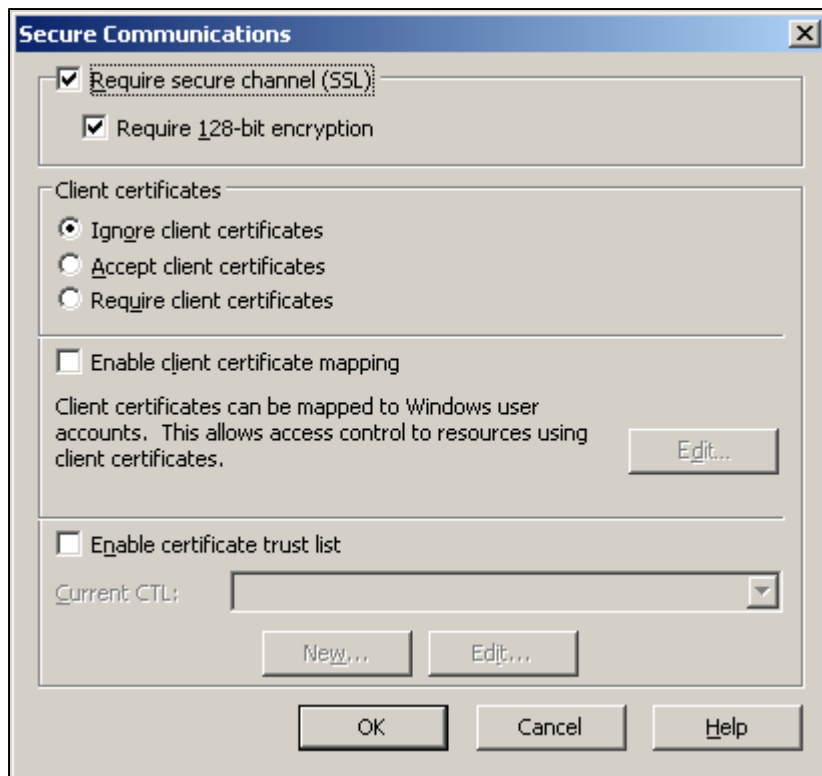
Step 4: Import the SSL Certificate into IIS

In this step you will ensure that your IIS web site is configured for SSL and import an SSL certificate into the IIS web site.

Step 4.1: Make Sure the IIS Web Site is Configured for SSL

1. Log in to your SharePoint server with a Windows account that has permission to administer IIS.
2. Run the **'Internet Information Services (IIS) Manager'**.
3. Expand the **'Web Sites'** folder and locate the IIS web site that you created in step 1 above. You can identify this web site by looking at the **'Description'** field.
4. Right-click the target web site and select **'Properties'**.
5. Select the **'Directory Security'** tab.
6. In the **'Secure communications'** section, click **'Edit...'**.
7. Ensure that the **'Require secure channel (SSL)'** and **'Require 128-bit encryption'** fields are both selected.

Screenshot: Requiring SSL



8. Click 'OK'.

Step 4.2: Obtain or Create a Certificate



SharePoint already accepting SSL?

If your SharePoint Server already accepts SSL traffic, then you already have a certificate installed on your SharePoint server. If this is the case, please skip ahead to step 4.3 [below](#).

You need an X.509 certificate that you can import into IIS. IIS will use the certificate to encrypt the SSL channel and prove the server's identity to clients. In the table below are the two ways of obtaining a certificate.



Disclaimer

Atlassian does not endorse or represent any of the example certificate issuers listed below.

Atlassian cannot accept responsibility for the veracity of any digital certificate issued by a third party. You should ensure that any certificate you use is from a provider that you trust.

Option	Example Provider	Benefit	Drawback
Obtain a certificate from a trusted certificate authority	Thawte Consulting Verisign	Most major certificate authorities are automatically trusted by most modern operating systems, so no configuration is required on the client to trust your certificate.	The certificate authority may charge a fee for issuing the certificate and/or an annual renewal fee.
Generate your own certificate	x509Builder Java keytool	Free	Client computers may require configuration to trust your certificate's authenticity.

Step 4.3 Import the Certificate into IIS

Once you have generated or obtained a certificate, you will usually receive:

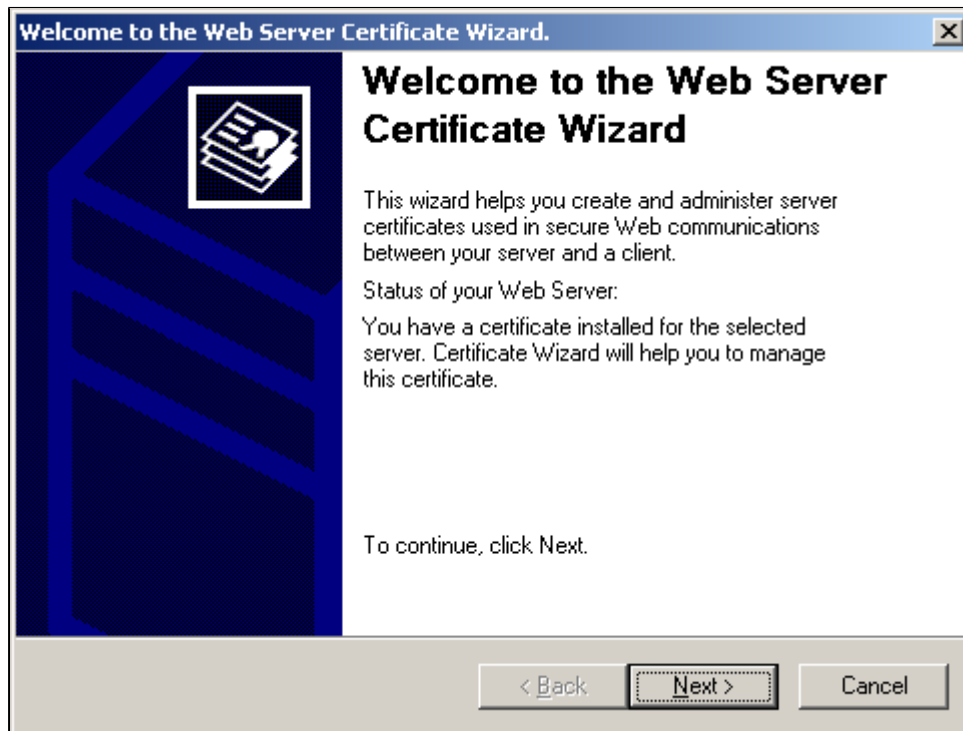
- The certificate stored in a file format such as `pfx`.
- A password that encrypts the file.

Follow these instructions to import the certificate into IIS:

1. Copy the certificate file to your SharePoint server.
2. Log in to your SharePoint server with a Windows account that has permission to administer IIS.
3. Run the '**Internet Information Services (IIS) Manager**'.

4. Expand the **'Web Sites'** folder and locate the IIS web site that you created in step 1 [above](#). You can identify this web site by looking at the **'Description'** field.
5. Right-click the target web site and select **'Properties'**.
6. Select the **'Directory Security'** tab.
7. Click **'Server Certificate...'**. The **'Web Server Certificate Wizard'** opens:

Screenshot: Web server certificate wizard



8. Click **'Next'**.
9. Select **'Import a certificate from a .pfx file'** and click **'Next'**.
10. Click **'Browse...'** to locate your certificate file and select it.
11. Click **'Next'**.
12. Enter the **'Password'** for your certificate and click **'Next'**.
13. Ensure the **'SSL port'** matches the port you selected in step 1 [above](#).
14. Click **'Next'**.
15. Click **'Next'**.
16. Click **'Finish'**.
17. Go to the SSL-secured web site in your web browser and ensure that it is accessible.

Step 5: Restrict the IIS Web Site to Confluence

As an additional layer of security, you should configure your SSL-secured web site to allow access from the Confluence server only.

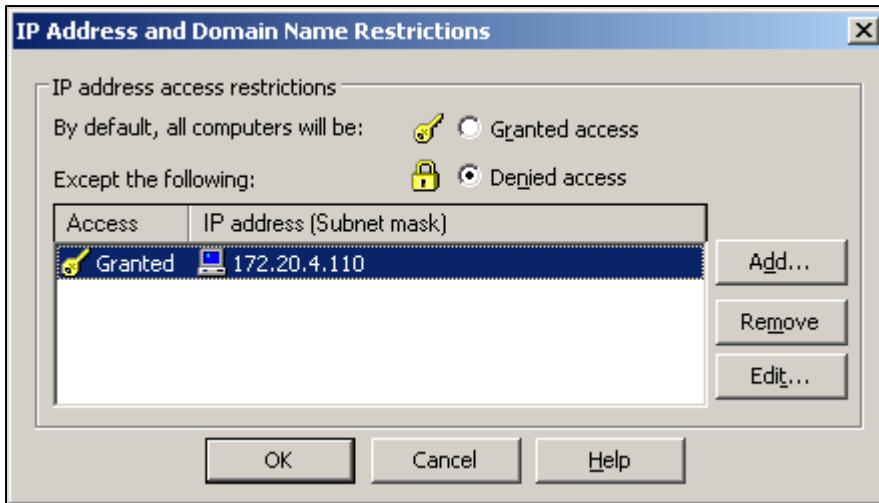


Confluence must have a static IP address or DHCP lease reservation

You will only be able to perform this step if your Confluence server has a static IP address. If your Confluence server has a dynamic IP address, then speak to your network administrator about adding a static IP address or a DHCP lease reservation for the Confluence server.

1. Note the IP address of your Confluence server.
2. Log in to your SharePoint server with a Windows account that has permission to administer IIS.
3. Run the **'Internet Information Services (IIS) Manager'**.
4. Expand the **'Web Sites'** folder and locate the IIS web site that you created in step 1 [above](#). You can identify this web site by looking at the **'Description'** field.
5. Right-click the target web site and select **'Properties'**.
6. In the **'IP address and domain name restrictions'** section, click **'Edit...'**.
7. Ensure that by default, all computers will be **'Denied access'**.
8. Click **'Add...'**.
9. Select the **'Single computer'** option.
10. Enter the IP address of your Confluence server in the **'IP address'** field.
11. Click **'OK'**.
12. Click **'OK'**.

Screenshot: IP restriction on IIS web site



Configuring Confluence

Step 1: Trust SharePoint's SSL Certificate



Skip all of step 1 if you obtained a certificate from a trusted CA

If you purchased a certificate from a trusted certificate authority, then your certificate is already trusted by the Confluence server and you can skip this step. Go to step 2 below. If you generated your own certificate or obtained one from a less well-known certificate authority, please follow the steps below.

To configure Confluence to trust the certificate on your SharePoint server, you must add the certificate's public key to the Java runtime's Certificate Authority keystore as described below.

Step 1.1: Create a .cer File



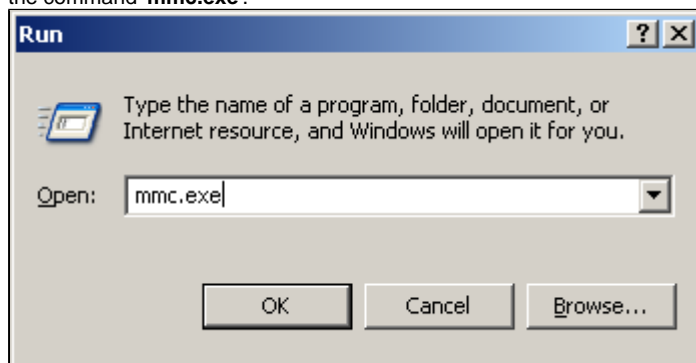
Skip step 1.1 if you already have a .cer file

The certificate's public key must be imported into the Java keystore as a certificate file in .cer file format. If you already have a .cer file you can skip this step and go to step 1.2 below. If you only have a .pfx file and need to create the .cer file, read on!

A simple way to create the required file is to import and export the certificate in and out of the Windows certificate store. This works because the export operation allows you to choose the export format.

The first step is to import the certificate into Windows:

1. Using a Windows computer, open the Microsoft Management Console by clicking the 'Start' button, selecting 'Run' and then running the command 'mmc.exe'.



2. In the Microsoft Management Console, select 'Add/Remove Snap-in...' from the 'File' menu.
3. Click 'Add...'.
4. Highlight the 'Certificates' snap-in from the list and click 'Add'.
5. Ensure that 'My user account' is selected and then click 'Finish'.
6. Click 'Close'.
7. Click 'OK'.
8. Expand the tree from 'Console Root' to 'Certificates - Current User' to 'Personal'.
9. Right-click 'Personal' and select 'Import...' from the 'All Tasks' menu.
10. When the 'Certificate Import Wizard' is displayed, click 'Next'.

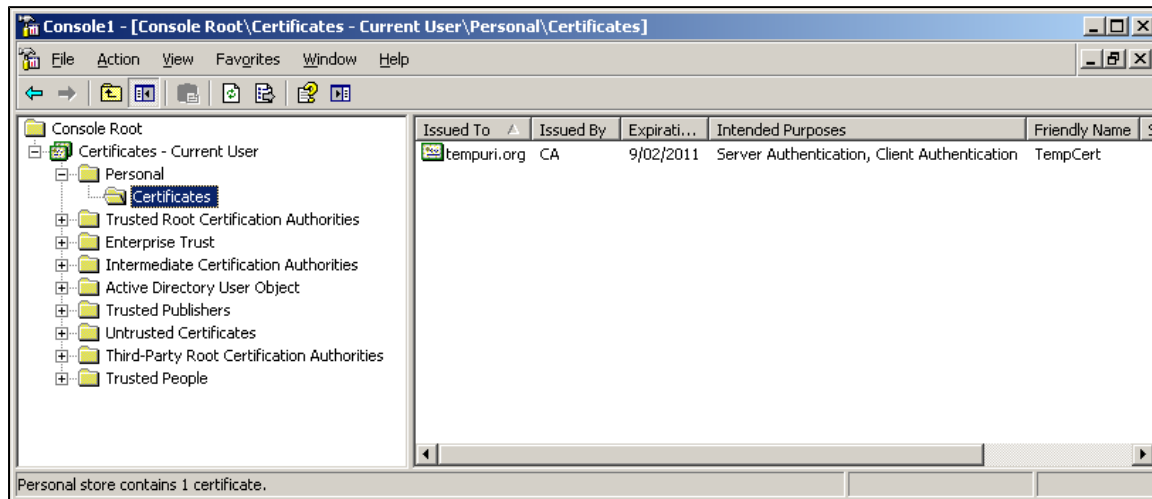
Screenshot: The certificate import wizard



11. Click '**Browse...**' and select the .pfx certificate file. (You may need to set the '**Files of type**' filter to '**Personal Information Exchange (.pfx, *.p12)***').
12. Click '**Next**'.
13. Enter the '**Password**' for the certificate.
14. Ensure that the '**Mark this key as exportable**' option is selected.
15. Click '**Next**'.
16. Click '**Next**'.
17. Click '**Finish**'.

At this point, your certificate should appear in the '**Personal**' folder of the 'Certificates' snap-in.

Screenshot: Personal certificates



Now you can export the certificate in the desired .cer format:

1. Right-click the certificate and select '**Export...**' from the '**All Tasks**' menu.
2. When the Certificate Export Wizard opens, click '**Next**'.
3. Ensure that the '**No, do not export the private key**' option is selected.
4. Click '**Next**'.
5. Ensure that the '**DER encoded binary X.509 (.CER)**' option is selected.
6. Click '**Next**'.
7. Enter a '**File name**' for the exported certificate (such as '{{}}C:\cert.cer').
8. Click '**Next**'.
9. Click '**Finish**'.

Step 1.2: Import the .cer File onto the Confluence Server

We have provided a batch script (see below) for Windows environments. If you are running Confluence on UNIX, please perform the import manually. The batch script uses the Java runtime's **keytool** command to import the certificate into the required location on the Confluence server. The script will add the certificate to the root Java Secure Sockets Extensions keystore, which is located in your Java Runtime Environment's (JRE's) `lib\security` directory with the name `jssecacerts`. This is the required location in order for the certificate to be trusted by Confluence.



Requirements

This script assumes the following about your environment:

- You are using a Confluence stand-alone installation running on the Sun JVM.
- Your `%JAVA_HOME%` environment variable has been set correctly.
- You have copied the `.cer` file created in step 1.1 [above](#) to the `C:` drive of your Confluence server.

Copy and execute this batch script (Windows) to add the certificate to the keystore:

.....

Step 2: Configure the Alternative URL in Confluence

The final step is to configure your Confluence server to communicate via the new URL you have set up.

- If you are installing the SharePoint Connector for the first time, please continue with the [next step of the installation procedure](#). In one of the later steps, you will configure the alternative URL in Confluence.
- If you have already installed and configured the Confluence plugins, please follow the instructions now to [configure the alternative URL in Confluence](#).

Installing and Configuring the Confluence Plugins for SP 2007

This page tells you how to install and configure the Confluence plugins that you need for the SharePoint Connector. These instructions apply to the connector for SharePoint 2007.

On this page:

- [1. Install the Confluence Plugins](#)
- [2. Configure Confluence and the Plugins](#)
 - [Enabling Confluence Remote API](#)
 - [Configuring Confluence to Work with a SharePoint Site](#)
 - [Configuring an Alternative SharePoint URL for Confluence](#)
 - [Configuring Confluence to Share Search Results with SharePoint MOSS](#)
- [Editing an Existing SharePoint Site's Settings](#)
- [Next Step](#)

1. Install the Confluence Plugins

To install the plugins into Confluence:

Go to the Confluence '**Administration Console**'. To do this:

- Open the '**Browse**' menu and select '**Confluence Admin**'. The 'Administration Console' view will open.

Using Confluence earlier than 3.4

1. Click '**Plugin Repository**' in the 'Configuration' section of the left-hand navigation panel to open the 'Atlassian Plugin Repository' page.
2. Scroll down to the row indicating '**The SharePoint Connector for Confluence**' and click '**Install**'. The Confluence plugin will be installed into Confluence.
3. Scroll to the row indicating '**Permission Checker RPC Plugin**' and click '**Install**'. The Permission Checker RPC plugin will be installed into Confluence.
- This plugin is also known as the 'Confluence SOAP Permission Checker Plugin'.
 4. Decide whether you will be able to use the SharePoint Connector's federated search feature. With the federated search, you can share search results between Confluence and SharePoint. It is available only if you have SharePoint MOSS 2007 or SharePoint Server 2010. If you want to use the federated search, you will need the Atlassian-supported OpenSearch plugin. Scroll to the row indicating '**OpenSearch Plugin**' and click '**Install**'. The OpenSearch plugin will be installed into Confluence.

Using Universal Plugin Manager, or using Confluence 3.4 or later

1. Click '**Plugins**' in the 'Configuration' section of the left-hand navigation panel to open the 'Universal Plugin Manager' page.
2. Click on the '**Install**' tab.
3. In the '**Search Plugin Exchange**' search box, enter 'Sharepoint Connector'.
4. Click on the search result to expand. Once expanded, click on '**Install Now**' button.
5. Repeat for '**Permission Checker RPC Plugin**'.
6. If you want to use the SharePoint Connector's federated search feature, you will need the Atlassian-supported OpenSearch plugin. Search for '**OpenSearch Plugin**' and repeat the procedure.

2. Configure Confluence and the Plugins

Once you have installed the required plugins into Confluence, you should then configure the plugins and your Confluence site to work and communicate successfully with a SharePoint site. Follow the instructions below.

Enabling Confluence Remote API

In order for your SharePoint site(s) to communicate with and retrieve content from Confluence, the **Remote API (XML-RPC & SOAP)** must be enabled in Confluence. Check whether the remote API is enabled and if not, enable it. See the instructions in the [Confluence administrator's guide](#).

Configuring Confluence to Work with a SharePoint Site

In this step, you will tell Confluence which SharePoint site(s) it can communicate with.

To configure Confluence to work with a SharePoint site:

1. Go to the Confluence '**Administration Console**'. To do this:
 - Open the '**Browse**' menu and select '**Confluence Admin**'. The 'Administration Console' view will open.
2. Click '**SharePoint Admin**' in the 'Administration' section of the left-hand navigation panel to open the 'SharePoint Integration Administration' screen. On this screen you can configure one or more SharePoint sites to work with your Confluence installation.

Screenshot: The site configuration section of the Confluence 'SharePoint Admin' page

SharePoint Integration Administration

Alias	SharePoint Site URL	Default Site	Login	
MySite	http://win-8d7e2ov0i6r/my		win-8d7e2ov0i6r\admin	- Edit -
QASP	http://win-8d7e2ov0i6r		win-8d7e2ov0i6r\admin	- Edit -

Please set these values correctly to provide access to your SharePoint site.

SharePoint Site Alias

SharePoint Site URL

Confluence Access URL Enabled ☒ No (Use Standard Access URL) ☐ Yes (Use Alternative Access URL)

User Name

Password:

☒ Make this SharePoint Site the default. This means its SharePoint Site Alias need not be specified when referencing SharePoint lists.

☐ Enable sp-list permission trimming - a user can only see a SharePoint list if they have permission to the list under the same username in SharePoint.

Confluence Permission Checker Plugin is installed.

Connection Test: **Success**

Examples: http://sharepoint-server or https://sharepoint-server:8080/sites/sitecollection1
[See documentation on SSL configuration.](#)

This option enables Confluence to access SharePoint using a different URL to users. This may be useful if SharePoint provides different authentication schemes at different URLs.

Example: ATlassian-SERV\Administrator (Note: Please be sure to use a backslash).

3. Enter the appropriate details into the following fields:


Table: SharePoint Site Configuration Fields


|| Field || Description ||

SharePoint Site Alias	Enter a simple name that identifies the SharePoint site easily in Confluence. SharePoint-related Confluence macros use this name as a parameter value to identify the SharePoint site on which to run their queries. Each SharePoint alias must be unique. However, do not modify this field when editing a pre-configured SharePoint site.
SharePoint Site URL	Enter the base URL of the SharePoint site, for example, [http://www.example-sharepoint-server.com]\\ \ \ \ .
Confluence Access URL Enabled	You can choose to configure an alternative SharePoint URL for Confluence to use when accessing SharePoint. See the details below.
User Name	The Windows user account that Confluence will use to access the SharePoint site. Note that this user must be a <i>SharePoint site collection administrator</i> . The user name <i>must</i> follow the syntax SERVERNAME\username, where: <ul style="list-style-type: none"> SERVERNAME is the name of the Windows domain on which the SharePoint site can be accessed. Otherwise, this is the name of the computer hosting SharePoint. username is the username of the Windows user account used to access the SharePoint site.
Password	The password associated with the Windows user account.
Make this SharePoint Site the default.	Selecting this option makes any Confluence SharePoint macros that do not reference a SharePoint Site Alias, query this SharePoint site. If this option is selected, a appears in the 'Default Site' field of the list of configured SharePoint sites (at the top of the SharePoint Admin page).

Enable sp-list permission trimming	Selecting this option filters the SharePoint List macro results to display only content that the user has permission to access in SharePoint.
------------------------------------	---

- Click the **'Test Connection'** button to test that the connection to the SharePoint site is correct.

If the connection was successful, you will see the message  **Connection Test: Success.**

If the connection was not successful, you will see the message  **Connection Test: Server unreachable.** If you see this message, please ensure that your SharePoint site settings are correct, as described in the table above.

- Click **'Update SharePoint Settings'** to save the configuration settings for your SharePoint site.

Configuring an Alternative SharePoint URL for Confluence

The **'Confluence Access URL Enabled'** option on the 'SharePoint Admin' screen allows you to set up a special URL for Confluence to use when accessing SharePoint. There are two choices:

- 'Use Standard Access URL'** – This is the default value. If you choose this option Confluence will query the SharePoint site via the 'SharePoint Site URL' configured above.
- 'Use Alternative Access URL'** – If you choose this option, the **'Confluence Access URL'** field appears on the screen. Enter an alternative URL. Confluence will query the SharePoint site via this URL instead of the 'SharePoint Site URL'.

The alternative access URL allows you to resolve problems where the SharePoint installation uses an authentication protocol not supported by Confluence, such as [NTLMv2](#) or [Kerberos](#). You can configure SharePoint to run on a separate port that bypasses the unsupported authentication protocol, and then allow Confluence to communicate with SharePoint via this alternative URL. See the [recommended configuration for securing Confluence access to SharePoint](#).

To configure Confluence to access SharePoint via an alternative URL:

- Set up an alternative URL in SharePoint. (See the [recommended configuration for securing Confluence access to SharePoint](#).)
- Select **'Use Alternative Access URL'** on the Confluence 'SharePoint Admin' screen shown above.



Which URL will the Confluence macros use?

Confluence's SharePoint macros will query the SharePoint site via the alternative access URL. However, any links returned by these macros that lead back to the SharePoint site will query the standard access URL.



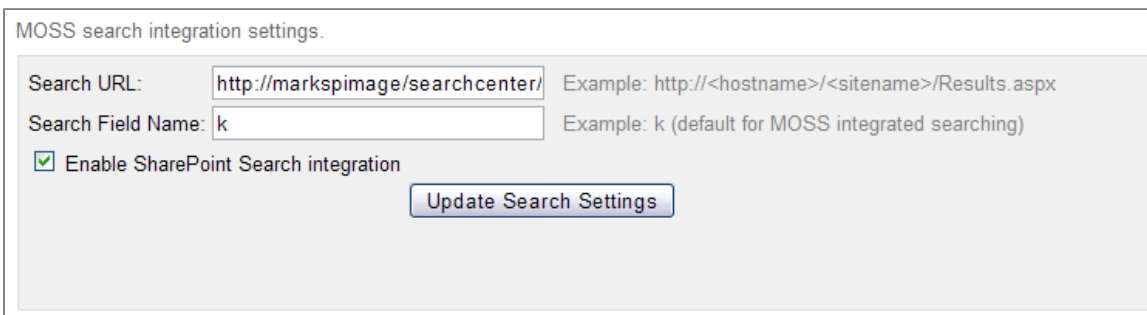
The alternative access URL must be configured externally, as a separate network configuration.

In practice, an alternative access URL would be used in situations where Confluence and SharePoint are hosted in the same private network, either behind a firewall or on the same VPN.

Configuring Confluence to Share Search Results with SharePoint MOSS


If you have a Microsoft Office SharePoint Server (MOSS) instead of just SharePoint WSS, you can configure Confluence to share search results with the MOSS server. This will allow users to search content in both Confluence and SharePoint from Confluence's search features.

Screenshot: The MOSS search integration section of the Confluence 'SharePoint Admin' page

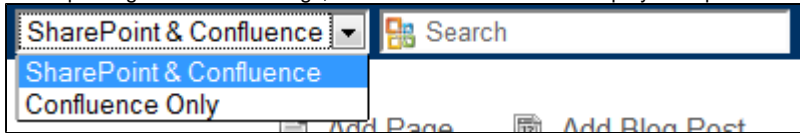


To configure Confluence to share search results with a MOSS server:

- Enter the MOSS server's Search URL into the **'Search URL'** field. This usually has the format `[http://www.example-sharepoint-server.com/searchcenter/Pages/Results.aspx]`.
- Enter the MOSS Search URL's search parameter into the **'Search Field Name'**. This is usually the letter `k` only.
- Click the **'Update Search Settings'** button.

 You will also need to configure the SharePoint side of things. You will come to this step later, as described in [Configuring the SharePoint Federated Search on SP 2007](#).

After updating the search settings, the Confluence theme will display a drop-down menu next to the Confluence search box, looking like this:



The drop-down menu offers two options:

- 'SharePoint & Confluence' – If you select this option when searching for content via the Confluence search, the search results page will open in SharePoint and will show results from both SharePoint and Confluence.
- 'Confluence Only' – If you select this option when searching for content via the Confluence search, the search results page will open in Confluence and will show results from Confluence only.

Editing an Existing SharePoint Site's Settings

This section describes how to edit the settings for a SharePoint site that has already been configured in Confluence.

To edit the existing configuration settings of a SharePoint site in Confluence:

1. Go to the Confluence '**Administration Console**'. To do this:
 - Open the '**Browse**' menu and select '**Confluence Admin**'. The 'Administration Console' view will open.
2. Click '**SharePoint Admin**' in the 'Administration' section of the left-hand navigation panel.
3. In the top list of already-configured SharePoint sites, click the '**- Edit -**' link next to the SharePoint site that you want to update. The fields below the list will be populated with the current settings for that SharePoint site.
4. Edit the field details according to the table above, to the updated settings.
5. If necessary, update the additional options as described above.
6. Test that the connection to the SharePoint site is correct by clicking the '**Test Connection**' button. A message will be displayed, indicating whether or not the connection was successful.
7. Click '**Update SharePoint Settings**' to save the updated configuration settings for your SharePoint site.



Do not change the SharePoint site alias

If you only intend to edit an existing SharePoint site's configuration, do not change the 'SharePoint Site Alias' field. If you do change this value, Confluence adds these settings as a new entry in the list of configured SharePoint sites.

Screenshot: Example List of Configured SharePoint Sites

Alias	SharePoint Site URL	Default Site	Login	
Another	http://another-server		ANOTHER\Administrator	- Edit -
SharePoint	http://sharepoint-server		SHAREPOINTSERV\Administrator	- Edit -

Next Step

To continue with the installation of the SharePoint Connector, please [configure the access to Confluence](#).

Configuring Access to Confluence for SP 2007

This section describes the methods which may be used to **configure access to Confluence** for the SharePoint Connector. You should complete one of the supported configuration guides before proceeding further with the SharePoint Connector installation. If you have not already seen our guide to [planning your environment](#), please refer to it now for information that will help you select the best configuration for your environment. These instructions apply to the connector for SharePoint 2007.

Please follow one of these configuration guides:

- [Access Confluence using Integrated Windows Authentication via IIS with SP 2007](#)
- [Access Confluence using Integrated Windows Authentication via Jespa with SP 2007](#)
- [Access Confluence using Standard Authentication with SP 2007](#)
- [Access Confluence using Standard Authentication with Microsoft SSO on SP 2007](#)

Next Step

To continue with the installation of the SharePoint Connector, please [install and configure the SharePoint feature](#).

Access Confluence using Integrated Windows Authentication via IIS with SP 2007

This page is part of the installation guide for the **Confluence SharePoint Connector**. It tells you how to configure access to Confluence using Integrated Windows Authentication via IIS. These instructions apply to the connector for SharePoint 2007.

On this page:

- [Overview](#)
- [Caveats](#)
 - [Supported Platforms](#)
 - [Additional Dependencies](#)
 - [Custom Seraph Authenticator](#)
 - [Custom ISAPI Filter](#)
 - [Anonymous Access Disabled](#)
 - [Known issues](#)
- [Installation Instructions](#)
 - [Step 1. Configure Confluence for LDAP User Management](#)
 - [Step 2. Configure IIS](#)
 - [Step 3. Configure Confluence for Integrated Windows Authentication](#)
 - [Step 3.1: Set Confluence Path](#)
 - [Step 3.2: Add AJP Connector](#)
 - [Step 3.3: Add Custom Authenticator](#)
 - [Step 3.4: Modify Base URL](#)
 - [Step 4. Set Client Browser Options](#)
- [Next Step](#)

Overview

In this configuration, both SharePoint and client browsers are authenticated against Confluence using Windows authentication provided by a Microsoft Internet Information Services (IIS) server. IIS proxies the pre-authenticated requests through to Confluence and then returns the content to the requester. Confluence and IIS communicate using Apache JServ Protocol (AJP).

Use this Configuration when...

- You want to enable 'pass-through authentication' for your users logged in to a Windows domain.
- All users who access Confluence are members of an Active Directory domain.
- Confluence is running on Windows Server, or you are able to set up Windows Server to act as a proxy for Confluence.

If you have not already seen our guide to [planning your environment](#), you can refer to it for information that will help you select the best configuration for your environment.

Caveats

Supported Platforms

Due to the complex nature of this configuration, Atlassian is only able to provide support if your configuration satisfies these additional conditions:

- Confluence must be installed as a stand-alone Tomcat application server.
- IIS and Confluence must be hosted on the same logical server (unless Confluence is running on a non-Windows system).
- The only supported operating systems for this configuration are Windows Server 2003 and Windows Server 2008.
- The server must be a member of the same Active Directory domain that contains the user records that will be authenticated.
- Confluence must be configured to use LDAP integration to Active Directory for user management.

Additional Dependencies

Using this configuration adds a number of additional dependencies to Confluence, which you should review.

Custom Seraph Authenticator

This configuration requires the use of a specialised Seraph authenticator for Confluence. If you are already using a different custom Seraph authenticator, you may not be able to use this configuration. In this situation, you must either choose a different configuration for the SharePoint Connector or consider developing a new custom Seraph authenticator that aggregates the functionality of both.



No support for custom authenticators

Please note that we are unable to provide support for any custom authenticators not written or explicitly supported by Atlassian.

Custom ISAPI Filter

This configuration requires the use of a custom ISAPI filter for IIS that can communicate using AJP. Atlassian will only support the use of the open source Tomcat Connector provided by the [Apache Tomcat project](#).

**Limited support for third-party software**

Please note that Atlassian is unable to provide in-depth support for problems encountered with the Tomcat Connector, as this software is written and maintained by the [Apache Software Foundation](#). Atlassian will assist with ensuring the correct configuration values are applied and capturing diagnostic information, but any issues encountered with the Tomcat Connector must be raised through the appropriate channels with the [Apache Tomcat project](#) or with another organisation that provides commercial support for Tomcat.

Anonymous Access Disabled

Due to limitations with the custom Seraph authenticator that Confluence requires for this configuration, it is not possible to set up anonymous access for Confluence when using this configuration.

Atlassian is currently reviewing the suitability of using the third-party [NTLM Authenticator for Confluence](#) instead.

Known issues

These are some reported problems with this configuration:

- The user is not able to explicitly log out. Even when they select the logout action, they remain logged-in.
- If you log in using NTLM authentication as a user that does not exist in the AD repository, you will not see the personal menu in Confluence's top navigation bar.
- You cannot fall back to using forms-based authentication or anonymous authentication.

Installation Instructions**Step 1. Configure Confluence for LDAP User Management**

If you have already configured Confluence to connect to your Active Directory domain, then skip ahead to the next step.

Set up your Confluence server to synchronise its user repository with your Windows Active Directory domain. See the Confluence documentation on [LDAP user management](#).

Step 2. Configure IIS

This and following steps guide you through the configuration required to use IIS as an NTLM authenticator for Confluence. NTLM is an authentication format developed by Microsoft. While some third-party implementations are available, IIS provides the most robust and full-featured NTLM authentication support.

Summary of this configuration:

- It places the Tomcat application server running Confluence behind an IIS website configured for Integrated Windows Authentication.
- IIS is then configured with a custom ISAPI handler that communicates directly with the Tomcat server using Apache JServ Protocol to serve the Confluence content back to the user.

Please follow the guide below that matches the version of your Windows Server:

- Windows Server 2003: [Configuring Tomcat-Connector for IIS 6.0 \(Windows Server 2003\)](#)
- Windows Server 2008: [Configuring Tomcat-Connector for IIS 7.0 \(Windows Server 2008\)](#)

Step 3. Configure Confluence for Integrated Windows Authentication

This section of the guide describes the steps necessary to configure Confluence to co-operate with the IIS Web Server.

Throughout this section, '%confluence_install%' refers to your [Confluence installation directory](#).

Step 3.1: Set Confluence Path

This step is only necessary if your IIS instance is already hosting other websites and you want to host Confluence underneath an existing site (for example, if your corporate intranet is hosted at <http://intranet.company.com> and you want to host Confluence at <http://intranet.company.com/confluence>).

1. Edit the %confluence_install%\conf\server.xml file.
2. Find the **Context** element in the file, and then change the **path** value to '/confluence'.
The line should look something like this:

.....

3. Save your changes and close the file.
4. Restart Confluence and verify that it is now accessible from the new path, such as <http://localhost:8080/confluence>.

Step 3.2: Add AJP Connector

Now you will change Tomcat's configuration, replacing the standard Coyote HTTP connector (which allows Tomcat to send and receive HTTP traffic) with a custom AJP connector (which allows Tomcat to communicate using Apache JServ Protocol).

1. Edit the `%confluence_install%\conf\server.xml` file.
2. Locate the **Connector** element and comment it out entirely.
3. Add a new **Connector** element that looks like the one below. The values that must match exactly are **address**, **protocol** and **tomcatAuthentication**:



If IIS is **not** located on the same server as Confluence, then you should not enter the **address** value at all.

4. Ensure that your `server.xml` file now contains only a single Connector definition.
5. Save your changes and close the file.
6. Restart Confluence and ensure that the server initialises successfully.

Step 3.3: Add Custom Authenticator

By default, Confluence will not understand the pre-authenticated requests that come through via the IIS Web Site. In order to allow this authentication information to pass through, you must modify the authenticator module used by Confluence.

1. Download the [customauth-0.4.jar](#) file attached to this page and place it in your `%confluence_install%\confluence\WEB-INF\lib` directory.
2. Edit the `%confluence_install%\WEB-INF\classes\seraph-config.xml` file.
3. Locate the **authenticator** element and comment it out entirely.
4. Add a new **authenticator** element that looks like this:

5. Save your changes and close the file.
6. Restart Confluence and ensure that the server initialises successfully.

Step 3.4: Modify Base URL

The final step in configuring Confluence is to modify the Server Base URL to point to the IIS web site, rather than directly to Confluence. This ensures that any hyperlinks generated within Confluence pages will direct users through the IIS website. For example, if your Tomcat server runs Confluence on <http://intranet.company.com:8080/confluence> and the IIS web site runs on <http://intranet.company.com>, then the Confluence Base URL needs to be changed to <http://intranet.company.com/confluence>.

See the [Confluence documentation](#) for instructions on modifying the Base URL.

Step 4. Set Client Browser Options

In order for users to be automatically logged in to Confluence without being prompted for their username and password, the browser must be correctly configured for pass-through authentication.

Please instruct all users to ensure that the [recommended browser settings](#) are applied.

Next Step

To continue with the installation of the SharePoint Connector, please [install and configure the SharePoint feature](#).

Access Confluence using Integrated Windows Authentication via Jespa with SP 2007

This page is part of the installation guide for the **Confluence SharePoint Connector**. It tells you how to configure access to Confluence using Integrated Windows Authentication via Jespa. These instructions apply to the connector for SharePoint 2007.

On this page:

- [Overview](#)
- [Caveats](#)
 - [Supported Platforms](#)
 - [Anonymous Access](#)
 - [Additional Dependencies](#)
- [About Jespa](#)
 - [Authentication Methods](#)
 - [Cost](#)
- [Installation Instructions](#)
- [Next Step](#)

Overview

In this configuration both SharePoint and client browsers are authenticated against Confluence using Windows authentication provided by [Jespa](#), a third-party implementation written in Java.

Use this Configuration when...

- Your users are logged in to a Windows domain and access Confluence using a web browser that supports automatic pass through of

- Windows credentials. (See the [recommended browser settings](#).)
- You want your users to experience a seamless single sign-on experience when accessing Confluence.
- Your Confluence installation is not running on a Windows server and you do not want to provision a new Windows server to provide an IIS proxy for Confluence (see [Integrated Windows Authentication via IIS](#)).

If you have not already seen our guide to [planning your environment](#), you can refer to it for information that will help you select the best configuration for your environment.

Caveats

Supported Platforms

Due to the complex nature of this configuration and its reliance on third-party products, Atlassian is only able to offer support if your configuration matches these specifications:

- Confluence is installed as a stand-alone Tomcat application server.
- Confluence is configured to use LDAP integration to Active Directory for user management.

Anonymous Access



Anonymous access is not supported

You will not be able to get anonymous access for Confluence working when using this configuration.

When configuring Confluence with Jespa (as described in our [guide](#)) you will not be able to set up a satisfactory anonymous access mechanism, due to the requirements of the custom authenticator and the Confluence Base URL.

Atlassian is currently reviewing the suitability of using the third-party [NTLM Authenticator for Confluence](#) instead.

Additional Dependencies

Please consider the following additional dependencies:

- The configuration requires a custom Seraph authenticator for Confluence. If you are already using a custom Seraph authenticator, you may not be able to use this configuration.
- The configuration requires a third-party library that implements the Windows authentication protocols. See the section on Jespa below for details of this dependency.

About Jespa

Jespa is a Java software library that provides advanced integration between Microsoft Active Directory and Java applications such as Confluence. For more information, visit the [Jespa website](#).

Authentication Methods

Jespa supports the following Windows authentication methods:

- LM
- NTLMv1
- NTLM2 Session Security
- LMv2
- NTLMv2

Cost

Jespa is a commercial software package that has a licensing cost associated with its use. Atlassian does not have a redistribution agreement with IOPlax, the suppliers of Jespa. If you wish to use Jespa, you must arrange a purchase agreement with IOPlax directly.

Purchasing information can be found on the [IOPlax website](#).

Installation Instructions

Follow the instructions on [configuring Confluence to use Jespa for NTLM authentication](#).

Next Step

To continue with the installation of the SharePoint Connector, please [install and configure the SharePoint feature](#).

Access Confluence using Standard Authentication with SP 2007

This page is part of the installation guide for the **Confluence SharePoint Connector**. It tells you how to configure access to Confluence using standard Confluence authentication. These instructions apply to the connector for SharePoint 2007.

On this page:

- [Overview](#)

- [Caveats](#)
 - [User Credentials Must Match](#)
- [Installation Instructions](#)
- [Next Step](#)

Overview

In this configuration, both SharePoint and all client browsers are authenticated using Confluence's built in authentication module, which is a style of forms-based authentication.

Use this configuration when...

- You have no specific authentication requirements for your environment.
- You do not need your users to have pass-through authentication to Confluence via their desktop logins.

If you have not already seen our guide to [planning your environment](#), you can refer to it for information that will help you select the best configuration for your environment.

Caveats

User Credentials Must Match

In order for the SharePoint Connector to seamlessly extract content from Confluence to SharePoint (and vice versa), Confluence's user repository must contain **usernames and passwords that exactly match** the usernames and passwords being used for SharePoint Authentication.

For small installations, you may be happy to maintain the standard Confluence user repository manually.

For larger installations, and if your SharePoint server authenticates users with Active Directory, you may consider synchronising the Confluence user repository with Active Directory.

Installation Instructions

No additional installation steps are necessary beyond following the standard installation guide for Confluence and the SharePoint Connector.

If you wish to synchronise the Confluence user repository with Active Directory, then read the Confluence documentation on [LDAP user management](#).

Next Step

To continue with the installation of the SharePoint Connector, please [install and configure the SharePoint feature](#).

Access Confluence using Standard Authentication with Microsoft SSO on SP 2007

This page is part of the installation guide for the **Confluence SharePoint Connector**. It tells you how to configure access to Confluence using the standard Confluence authentication with Microsoft SSOSrv (Microsoft Single Sign-On Service). These instructions apply to the connector for SharePoint 2007.

On this page:

- [Overview](#)
- [Caveats](#)
 - [Caching of Username and Password](#)
- [Installation Instructions](#)
 - [Step 1. Start the MOSS SSO Service](#)
 - [Step 2. Configure the MOSS SSO Service Settings](#)
 - [Step 3. Configure an SSO Application for Confluence](#)
- [Next Step](#)

Overview

In this configuration, both SharePoint and all client browsers are authenticated using Confluence's built in authentication module, which is a style of Forms-based Authentication. The Microsoft SSO service acts as a "man-in-the-middle", performing mappings between Confluence and SharePoint user accounts.

Use this Configuration when...

- You have no specific authentication requirements for your environment. You do not need your users to have pass-through authentication to Confluence via their desktop logins.
- The usernames and passwords in your Confluence user repository do not exactly match the usernames and passwords in your SharePoint user repository (such as Active Directory)
- You are not able to configure Confluence to synchronise its user repository with Active Directory (see [Confluence LDAP User Management](#)).

If you have not already seen our guide to [planning your environment](#), you can refer to it for information that will help you select the best configuration for your environment.

Caveats

Caching of Username and Password


The Microsoft SSO Service caches users' credentials for external applications such as Confluence. The first time a user accesses Confluence, they will be prompted to enter their username and password. Subsequent logins to Confluence will use the cached credentials.

Installation Instructions

After installing the SharePoint Connector, follow the instructions below to enable Microsoft SSO.

Step 1. Start the MOSS SSO Service

If you already have the Microsoft Office SharePoint Server (MOSS) Single Sign-on (SSO) Service running in your environment, you may skip this step and move on to step 3, configuring an SSO Application for Confluence, [below](#). However, you may want to review the steps to ensure your existing configuration will be compatible regarding domain accounts, general access and permissions.

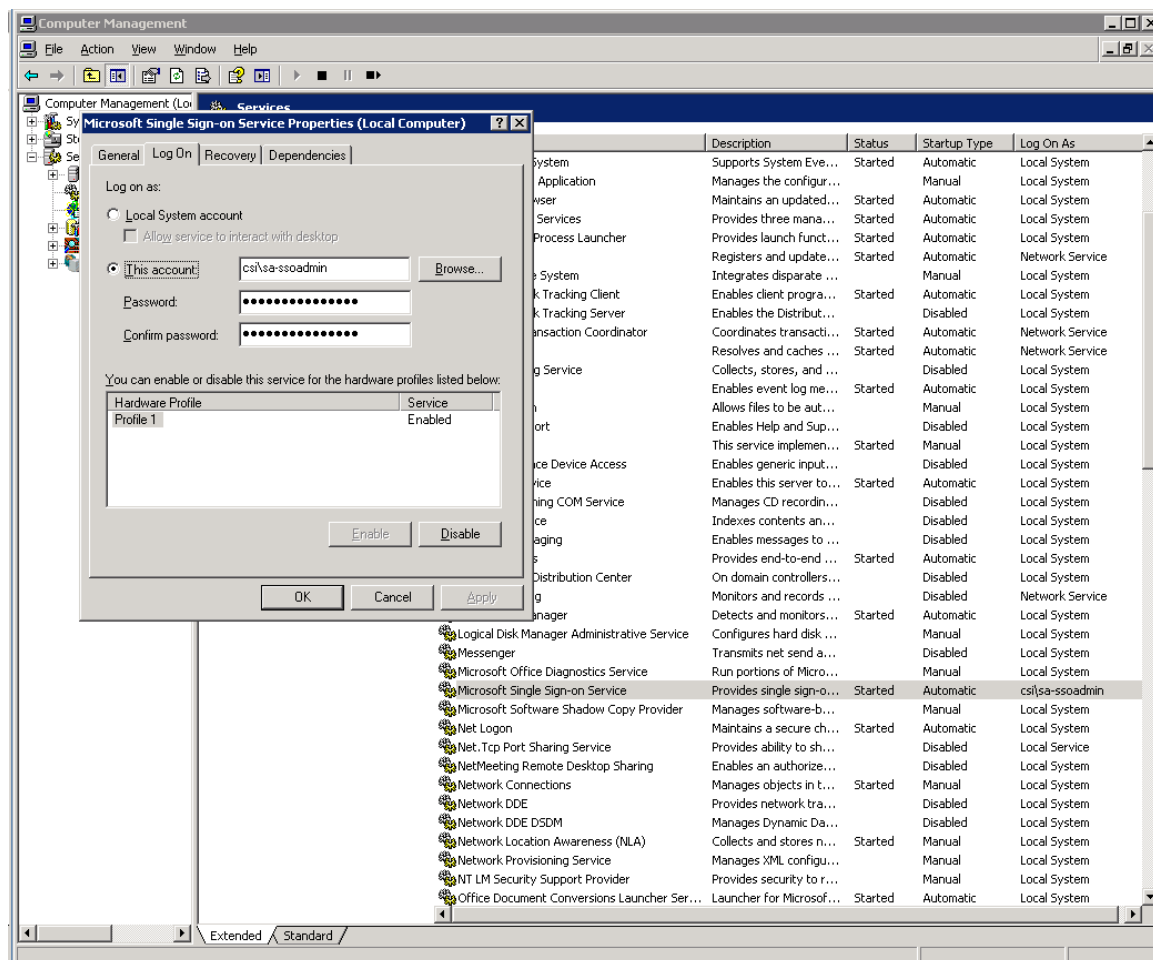
 These instructions are derived from the [Microsoft TechNet documentation](#).

To start the SSO service:

1. Open your Windows 'Administrative Tools' and click 'Services'.
2. Double-click 'Microsoft Single Sign-On Service'.
3. On the 'Log On' tab of the Single Sign-On Service Properties page, click 'This account' and then type the domain, user name, and password that you have used to install and manage your server.




This account should be the same account as used for the SharePoint application pool associated with the SharePoint site that will be using the Single Sign-on Service. The account must be associated with the dbcreator and securityadmin SQL Server roles on the SQL Server that will be used to host the SSO database. See [Dave Wollerman's SharePoint Blog](#).



4. Click 'Apply'.
5. On the 'General' tab of the Single Sign-On Service Properties page, change the startup type to 'Automatic', click 'Start', and then click 'OK'.

Step 2. Configure the MOSS SSO Service Settings

 These instructions are derived from the [Microsoft TechNet documentation](#).

To configure the SSO settings:

1. Log in as the account used in step 1.3 [above](#). This account will be used to create the SSO database.
Note: This user will require SQL Server role assignments for `dbcreator` and `securityadmin` to be able to create the SSO database.
2. Open your Windows '**Administrative Tools**' and open the SharePoint Central Administration Web application.
3. On the Central Administration home page, click '**Operations**'.
4. In the '**Security Configuration**' section, click '**Manage settings for single sign-on**'.
5. On the Manage Settings for Single Sign-On page, click '**Manage server settings**'.
6. In the '**Account Name**' box for the SSO Administrator account, type the same domain and username that you used to configure the Single Sign-On service. If this username is a member of a Windows security group, you can type the name of the Windows security group instead of a username.
7. In the '**Enterprise Application Definition Administrator Account**' box, type the same domain and username that you used to configure the Single Sign-On service.
8. In the '**Server name**' box, type the SQL Server instance name (using the netbios\instance naming convention) to use for the Single Sign-on database.
9. In the '**Database name**' box, type the name for the Single Sign-on database (for example, 'SSO')
10. In the '**Ticket time out**' and '**Delete audit log records older than (in days)**' boxes, leave the default values (recommended).
11. Click '**OK**'.

**SharePoint Farm**

Here are some additional considerations for configuring the SSO service in a SharePoint web farm:

- Make sure the SSO service is running as the correct domain service account. This must be consistent across Web Front End (WFE) servers in the farm.
- Make sure the Single Sign-On 'Service Account' (in 'Central Administration | Operations | Service Accounts') is set to the same domain account as used to actually run the SSO service.

At this point you should have a running instance of the Microsoft SharePoint Single Sign On service. This includes a new database for securely storing SSO user credentials. The next step is to configure an SSO application for Confluence.

Step 3. Configure an SSO Application for Confluence

1. Open your Windows '**Administrative Tools**' and open the SharePoint Central Administration Web application.
2. On the Central Administration home page, click '**Operations**'.
3. In the '**Security Configuration**' section, click '**Manage settings for single sign-on**'.
4. On the Manage Settings for Single Sign-On page, click '**Manage settings for enterprise application definitions**'.
5. Click '**New Item**' and set the following properties*
 - Display Name: Confluence
 - Application Name: Confluence
 - Contact e-mail address: (*Example:* sample.administrator@csi.local)
 - Account type: Individual
 - Authentication type: (Leave 'Windows authentication' unchecked)
 - Username and Password: Leave the default 'Username' and 'Password' in place
6. Click '**OK**'.

Next Step

To continue with the installation of the SharePoint Connector, please [install and configure the SharePoint feature](#). When [configuring the SharePoint web part](#) make sure that you select 'Microsoft Single SignOn (SSO)' as your authentication method.

Installing and Configuring the SharePoint Feature on SP 2007

This page tells you how to install and configure the SharePoint feature, that is, the SharePoint component of the Confluence SharePoint Connector. This component provides the Confluence web parts on the computer running SharePoint. These instructions apply to the connector for SharePoint 2007.


On this page:

- [1. Install the SharePoint Component](#)
- [2. Configure the Confluence Settings for the SharePoint Sites](#)

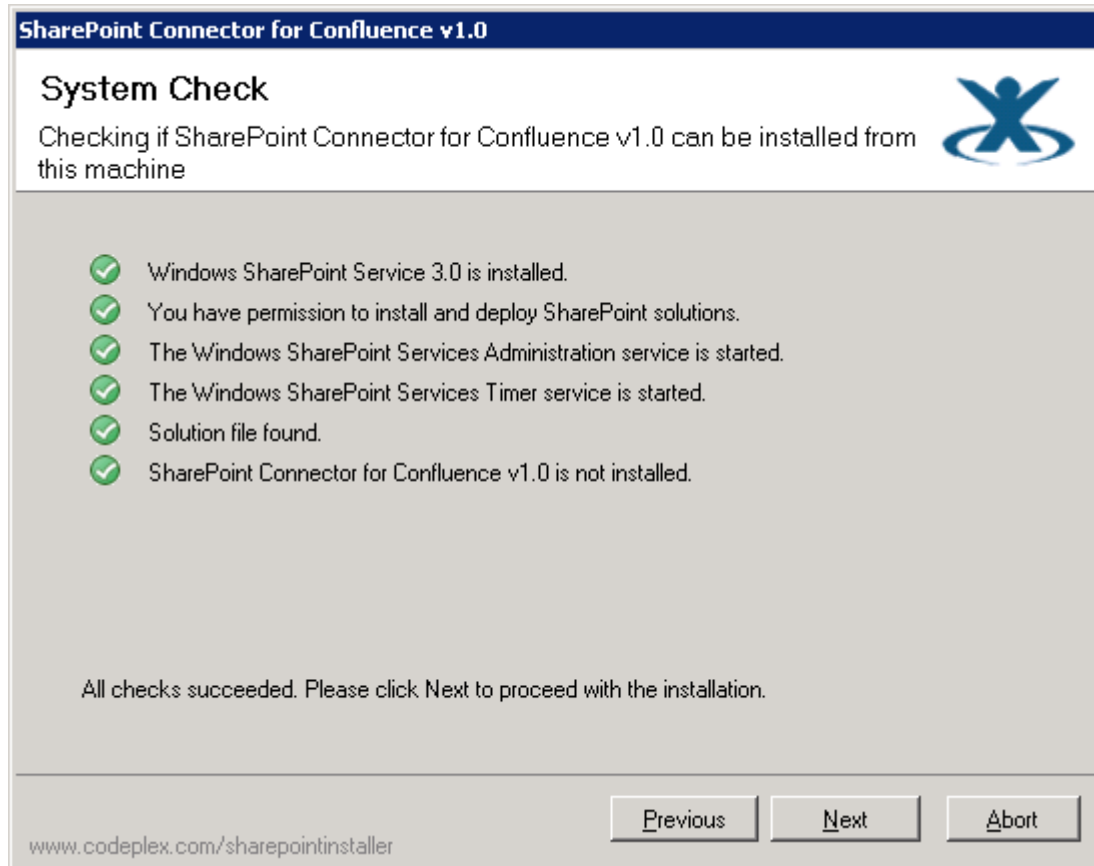
1. Install the SharePoint Component

To install the SharePoint component:


1. Download the SharePoint component from the [SharePoint Connector download centre](#).
2. Extract the contents of the downloaded `SharePointConnector` zip file and open the 'SharePoint Installer' directory.

3. Run the file in this directory named `Setup_WebParts.exe`. This starts the installation wizard for the SharePoint web parts.
 All files in the 'SharePoint Installer' directory must remain intact for the installation of the SharePoint web parts to succeed.
4. After the welcome page loads, click the '**Next**' button to start the installation process.
5. The SharePoint web part installer performs a 'System Check' to ensure that all pre-installation and configuration requirements have been met.

Screenshot: SharePoint Web Part Installer - 'System Check' Step




Click '**Next**' to proceed with the installation wizard. If, however, one or more of the requirements checks fails, you must address those requirements before proceeding.

 The 'Windows SharePoint Services Administration' service in Windows may be stopped by default and if so, the third item in this check list will fail.

To resolve this issue:

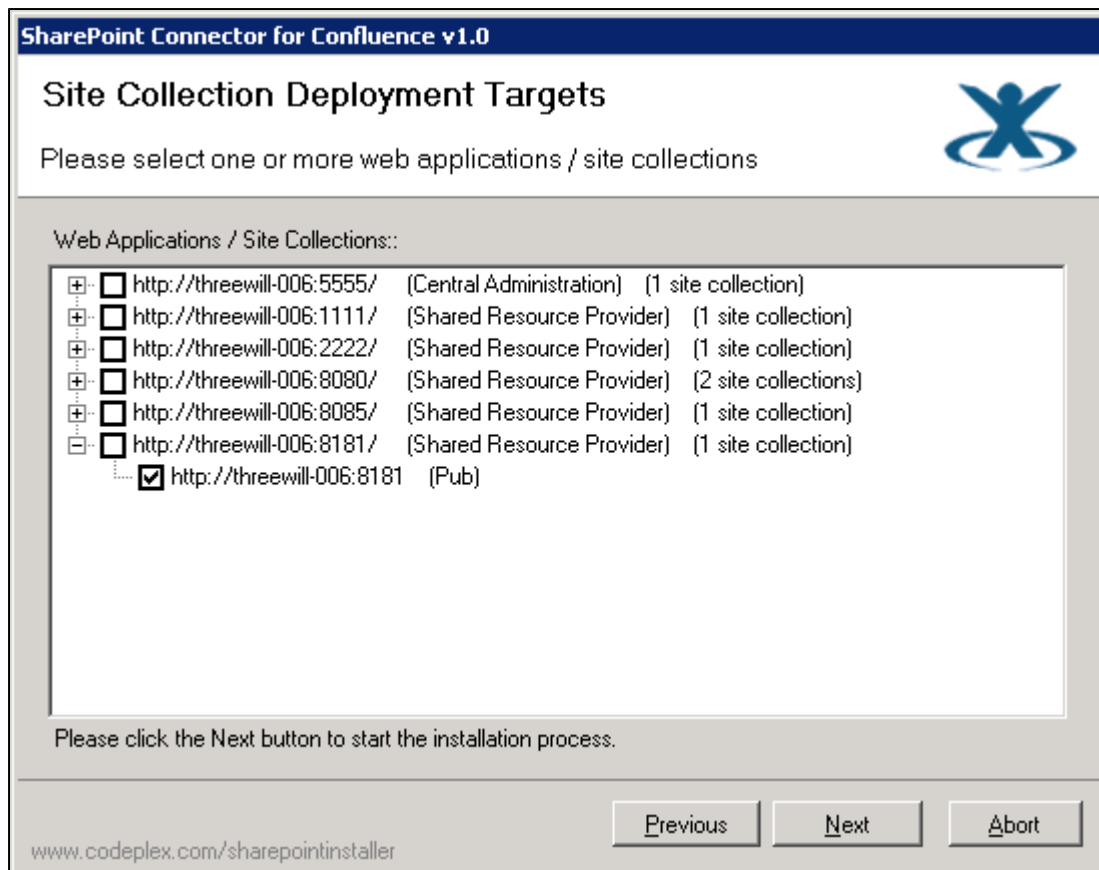
- a. In Windows, go to **Start -> All Programs -> Administrative Tools** and select '**Component Services (or Services)**'.
- b. In the Component Services console, select '**Services (Local)**' then scroll down to the '**Windows SharePoint Services Administration**' option and select it.
- c. Right-click this option and select '**Start**' from the popup menu.
- d. Stop and restart the SharePoint web part installation from step 2 above.

6. The Atlassian End User license agreement is displayed. If you choose to continue, you must accept the license agreement by selecting the check box, then click the '**Next**' button to continue.
7. In the 'Site Collection Deployment Targets' step, select the SharePoint site collections within your SharePoint installation, to deploy the Confluence SharePoint web part. This web part permits Confluence integration with the selected SharePoint site collections.

 Typically, the Confluence SharePoint web part is deployed to one or more SharePoint site collections within a SharePoint installation. The Confluence SharePoint web part is usually not deployed to the 'Central Administration' or 'Shared Resource Providers'/'Shared Service Providers'.

 All selected site collections in your SharePoint installation must be online before proceeding.

Screenshot: SharePoint Web Part Installer - 'Choose SharePoint Site Collections' Step



After selecting one or more Sharepoint site collections / web applications, click the **'Next'** button.

8. The installation process starts, deploying the Confluence SharePoint web part to the chosen SharePoint site collections.

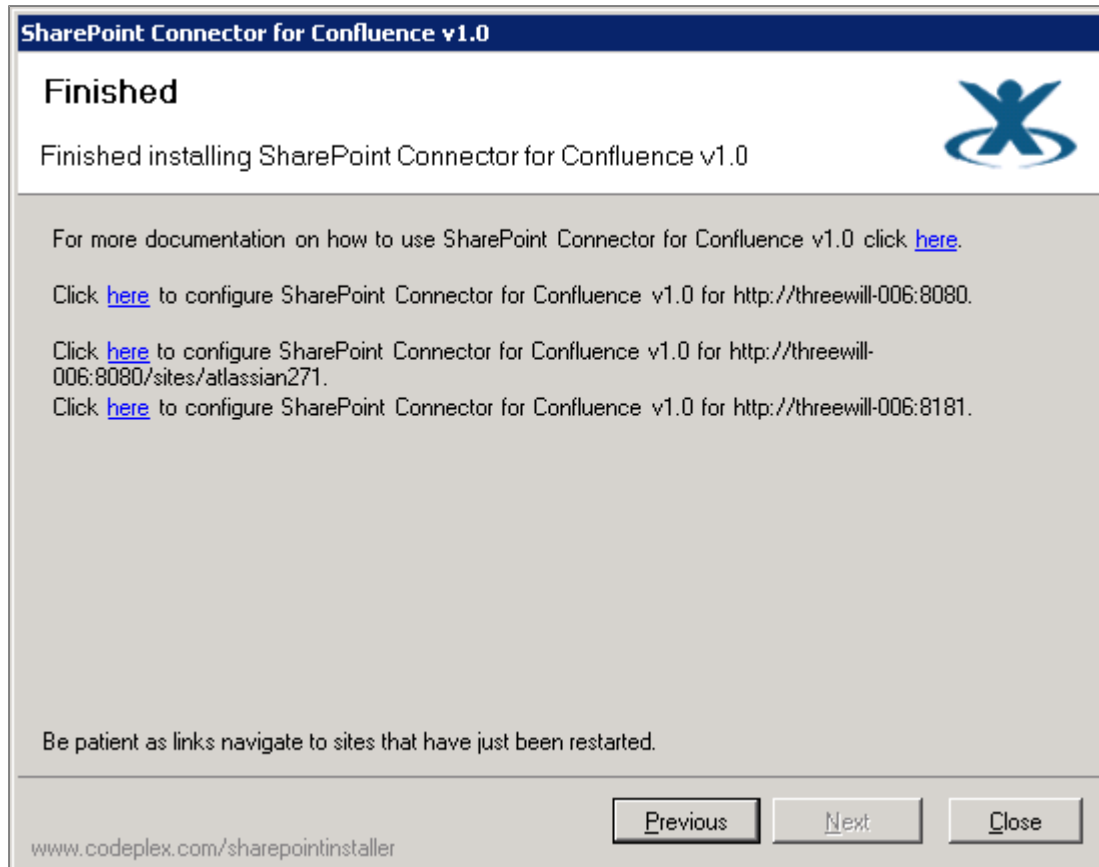
After the installation process is complete, click the **'Next'** button.

9. The **'Installation Successfully Completed'** step of the installation wizard is displayed. This window shows the SharePoint site collections that now have the Confluence SharePoint web parts. Click **'Next'** to continue.
10. The **'Finished'** step of the installation wizard is displayed. This window provides one or more configuration links. Each link points to the Confluence settings page of a SharePoint site with its newly installed Confluence SharePoint web part. Click each of these configuration links in turn to define how the SharePoint sites will connect to Confluence. See [Configuring the SharePoint Web Part on SP 2007](#).



When you click the links in this window, it may take some time for the configuration screens to appear because the SharePoint sites may require time to restart.

Screenshot: SharePoint Web Part Installer - 'Finished' Step



2. Configure the Confluence Settings for the SharePoint Sites

1. Configure the Confluence settings for each SharePoint site collection to which the SharePoint web part was deployed. You can do this by clicking the links on the 'Finished' screen of the installation wizard, as described above, or by navigating to the settings page yourself. See [Configuring the SharePoint Web Part on SP 2007](#) for full details.
2. Configure the SharePoint Federated Search, if required. See [Configuring the SharePoint Federated Search on SP 2007](#).

Configuring the SharePoint Web Part on SP 2007


This page tells you how to configure the Confluence settings for SharePoint. These instructions apply to the connector for SharePoint 2007.

On this page:

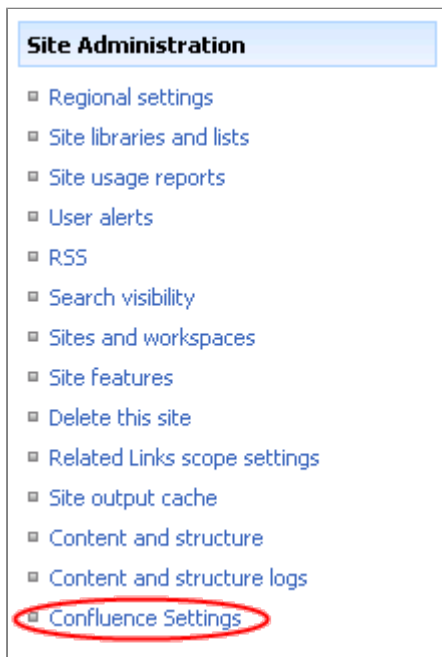
- [Configuring the Confluence Administrative Settings for a SharePoint Site](#)

Configuring the Confluence Administrative Settings for a SharePoint Site

1. Open your web browser and use one of the following methods to open the Confluence settings page of the appropriate SharePoint site collection:
 - Navigate to the top level site within the site collection, select '**Site Actions**' (at the top right) -> '**Site Settings**' -> '**Modify All Site Settings**'. On the 'Site Settings' page, choose '**Confluence Settings**'.

 The 'Confluence Settings' page is available only if the Confluence SharePoint web part was deployed to that SharePoint site.

[Screenshot: 'Site Administration' Section of the 'Site Settings' Page in SharePoint](#)



- Or enter the URL for this page directly, using the format:
`http://<sharepoint-site-collection>/_layouts/Atlassian/ConfluenceSettings.aspx`
- Or use the final step of the web part installer wizard which provides direct links to these pages. For more information, please refer to the instructions on [installing the SharePoint feature](#).

2. The Confluence administration screen appears:

Screenshot: Confluence Administrative Settings in SharePoint

 A screenshot of the 'Confluence Administrative Settings' page in SharePoint. The page has a blue header with 'Home' and 'Site Actions' buttons. The main content area is titled 'Confluence Administrative Settings' and contains several sections:

- Confluence Site:** A text box for 'Supply a valid Confluence URL.' with the value 'http://bluetongue:1990/confluence'. Below it, 'Connector Version: 1.4.0.0' is displayed.
- Authentication Selection:** A section with instructions and radio buttons. The first option, 'Access Confluence with a single master account', is selected. It includes fields for 'Confluence User Name' (admin) and 'Confluence Password' (masked). There are also checkboxes for 'Customise permission checking format (optional)' and 'Authenticate with Confluence using email (optional)'. The second option, 'Access Confluence with the Microsoft Single Sign-On (SSO) Service', is unselected and shows 'SSO is not configured....'.
- Confluence Web Service Settings:** A section with a 'Web Service Timeout' field set to '100'.
- Test Configuration:** A section with a 'Test Confluence Configuration' button.

 At the bottom right, there are 'OK' and 'Cancel' buttons.

3. Enter the base URL of the Confluence site in the '**Confluence Site**' field.
4. Under '**Authentication Selection**', choose the method by which SharePoint will access the Confluence site. See our [planning guide](#) for help with the authentication options.
 - If you choose '**Access Confluence with a single master account**':

- Specify the Confluence **username** that SharePoint will use to access Confluence and enter the password recognised by Confluence for that username. This username must have full *Confluence site administration permissions*.
- Optionally, you can also choose to customise the format of the username used to authenticate against Confluence. Select '**Customise the permission checking format**'. The '**User Name Format**' field will appear. Enter a format, such as this:

```
{domain} \ {username}
```

This example will pass the domain as well as the username when authenticating a user to Confluence. This is useful if you have configured Confluence to connect to multiple Active Directory domains and you therefore need to distinguish between two users with the same username in different domains.

- Optionally, you can also choose to set the format of the username used to authenticate against Confluence to be the SharePoint user's configured Active Directory email address. To do this, select the '**Authenticate with Confluence using email**' field. This is useful if your users log in to Confluence with their email address, rather than their Active Directory username.
 - If you choose '**Access Confluence with the Microsoft Single Sign-On (SSO) Service**':
 - Select the Confluence SSO application in the dropdown box. This is the application that you have already set up when configuring [access to Confluence via the Microsoft SSO service](#).
5. If your Confluence site is especially large, and your users report problems while waiting for the Confluence web parts to load, you can optionally choose to increase the timeout value for retrieving content from Confluence. The default is 100 seconds, but you can increase this to a longer timeout if desired. To do this, enter a new numerical value in the '**Web Service Timeout**' field.
 6. Click the '**Test Confluence Configuration**' button to test your configuration settings.
 7. Click '**OK**' to save your changes.



Settings are inherited by child SharePoint sites

The Confluence settings are automatically inherited by any SharePoint sub-sites. If no Confluence settings have been configured for a SharePoint sub-site, the parent SharePoint site's Confluence settings apply. However, any Confluence settings configured for a sub-site will override the parent site's Confluence settings.

Configuring the SharePoint Federated Search on SP 2007

The Confluence SharePoint Connector provides a federated search, allowing SharePoint to issue search requests to Confluence and display the results it gets back from Confluence. Federated searches use Confluence's own search engine to retrieve up-to-date and relevant results. These instructions apply to the connector for SharePoint 2007.

On this page:

- [Requirements](#)
- [SharePoint Configuration](#)
 - [Step 1: Configure the Federated Search Location](#)
 - [Step 2: Add Web Part to Search Results](#)

Requirements

- **Microsoft Office SharePoint Server (WSS is not enough):** Only Microsoft Office SharePoint Server ('MOSS') supports the new federated search. Plain Windows SharePoint Services ('WSS') does not support federated search.

The federated search feature in SharePoint Connector 1.1 and later relies on new functionality in SharePoint. At least one of the following updates to SharePoint must be installed on your MOSS Server(s):

- [Search Server 2008 Infrastructure Update](#)
- [Service Pack 1](#)
- [Service Pack 2](#)

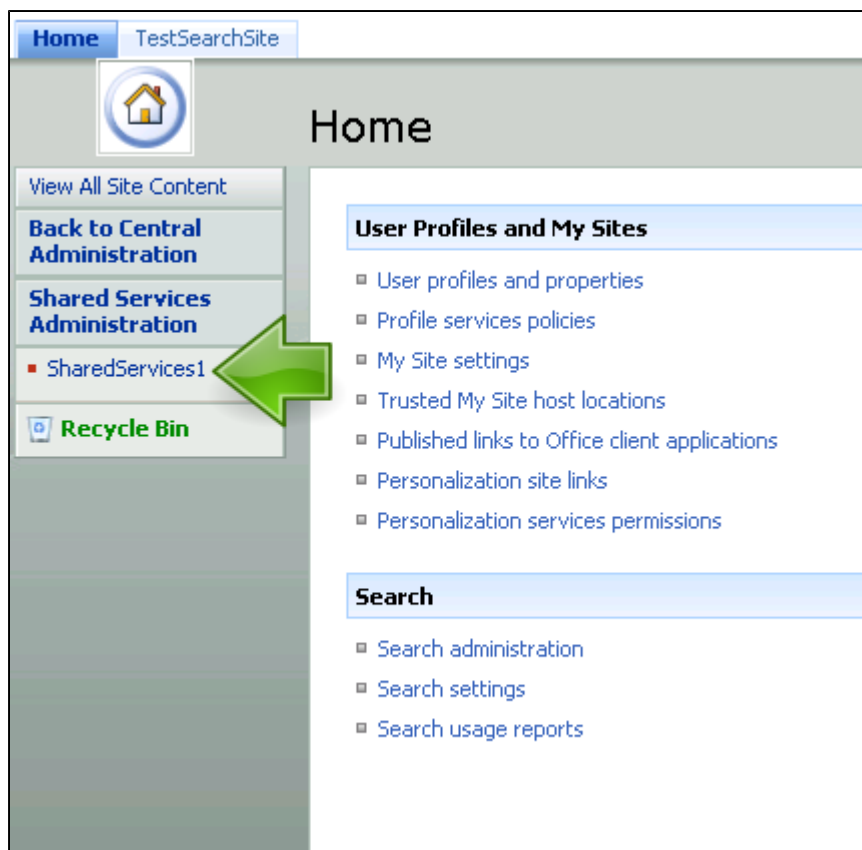
We recommend **Service Pack 2**, which is the most recent update.

- **The Confluence OpenSearch plugin and MOSS search configuration:** Your Confluence installation must include the OpenSearch plugin and must be configured to share search results with MOSS. Optionally, you can also configure Confluence to use the SharePoint Decorators theme. See the [guide to installing the Confluence SharePoint plugins](#).

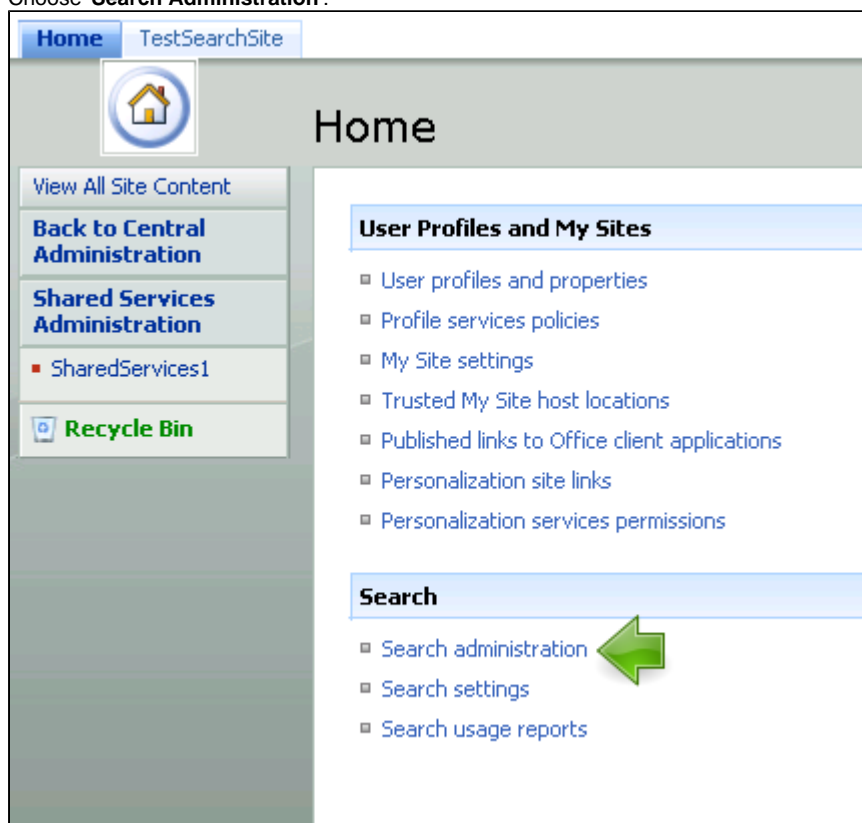
SharePoint Configuration

Step 1: Configure the Federated Search Location

1. Go the SharePoint central administration section and select the shared services for which to add the federated search:



2. Choose 'Search Administration':



3. Choose 'Federated Locations'. Note that this will only be present if the infrastructure update has been installed:

Administration

- Search Administration
- Central Administration

Crawling

- Content sources
- Crawl rules
- Crawl log
- Default content access account
- File types
- Reset all crawled content
- Crawler impact rules
- Proxy and timeouts

Queries and Results

- Authoritative pages
- Federated Locations
- Metadata properties
- Scopes
- Server name mappings
- Search result removal

Usage Reports

- Queries report
- Results report

System Status

Crawl status

Items in index

Server status

Propagation status

Default content access account

Contact e-mail address

Proxy server

Scopes update status

Scopes update schedule

Scopes needing update

Search alerts status

Query logging

Active crawls

Content Source

There are no active crawls.

Recently completed crawls

Content Source

Page 1 of 18

4. Add a federated location:

Shared Services Administration: SharedServices1 > Search Administration > Federated Locations



Manage Federated Locations

By using search federation, users can simultaneously search content in the search index on this server, as well as in other search engines.

To add a new location, visit the [Online Gallery](#), download the location and then import it. Alternatively, you can define a new location manually.

To enable users to search the location in the Search Center, specify the location in the properties in one of the Web Parts.

[Learn more about federated locations](#)

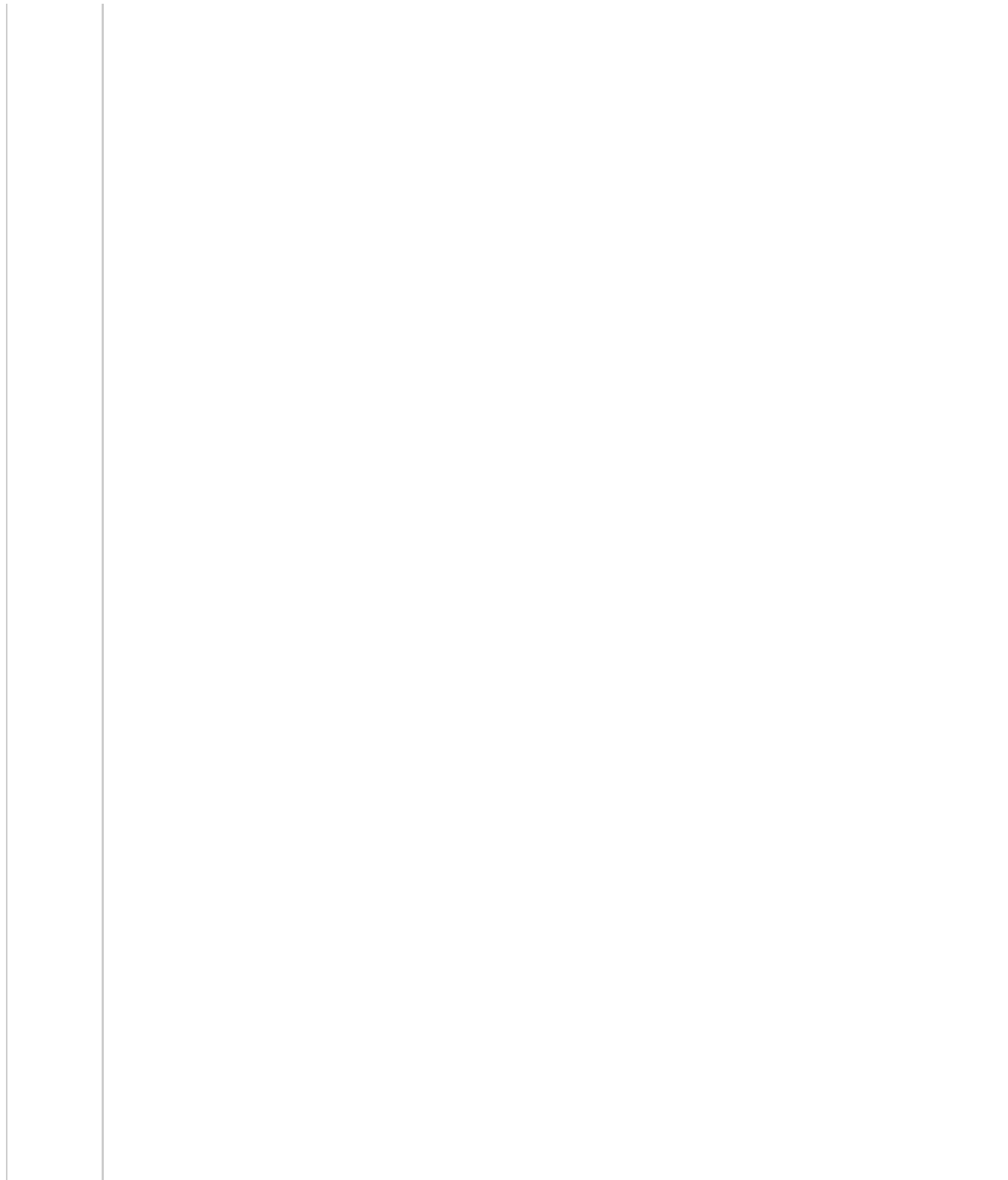
 [New Location](#)  [Import Location](#)

Location Display Name	Number of Queries (last 30 days)
Internet Search Results	0
Internet Search Suggestions	0
Local Search Results	0
Confluence	3

5. Enter the information for the federated location. Here are some guidelines on the mandatory fields:

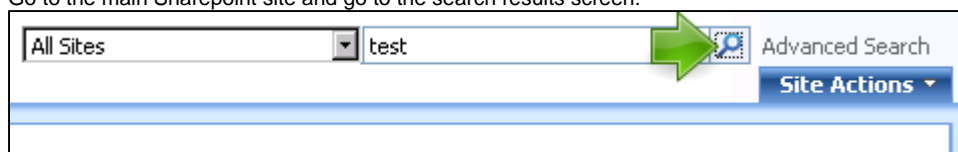
Field Name	Meaning
Location Name	The name of this location. We suggest 'Confluence'
Display Name	The name of the location which will be displayed to users
Description	A description of this location
Location Type	The type of search to perform. We need OpenSearch.
Query Template	This is the URL which will be used to perform the actual search. This URL depends on the authentication used by Confluence: * Standard (forms) authentication: <code>http://<CONFLUENCE_SERVER>/plugins/servlet/opensearch?query={searchTerms}&format=rss_1.0&os_a</code> * NTLM: <code>http://<CONFLUENCE_SERVER>/plugins/servlet/opensearch?query={searchTerms}&format=rss_1.</code>
"More Results" Link Template	The link which users will go to if they click the "More Results" link: <code>http://<CONFLUENCE_SERVER>/dosearchsite.action?queryString={userQuery}</code>
Specify Credentials	This specifies how Sharepoint will send the credentials for the searching user to Confluence. Make sure that you set the credentials in the 'Advanced' section, not the 'Common' section. The actual credentials depend on the authentication used by Confluence: * Standard (forms) authentication: choose "Basic Authentication" * NTLM: choose "NTLM Authentication" If you use Microsoft SSO, check "Use SSO" and select the Confluence SSO application, if you do not use Microsoft SSO then unchecked.
Federated Search Results	This specifies how to display the results. This can optionally be changed using the example XML to use Confluence icons for Confluence search results.

Display
Metadata:
XSL

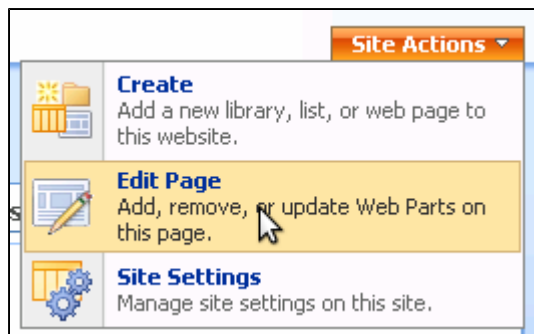


Step 2: Add Web Part to Search Results

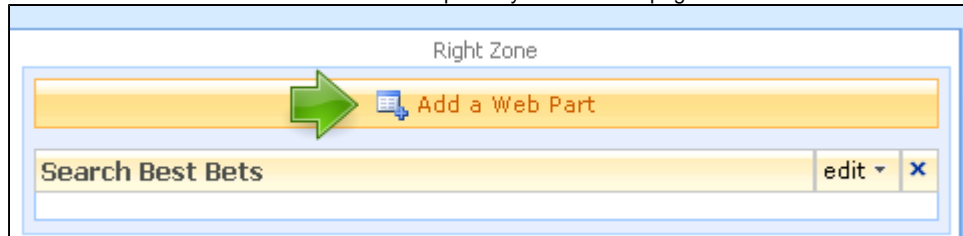
1. Go to the main Sharepoint site and go to the search results screen:



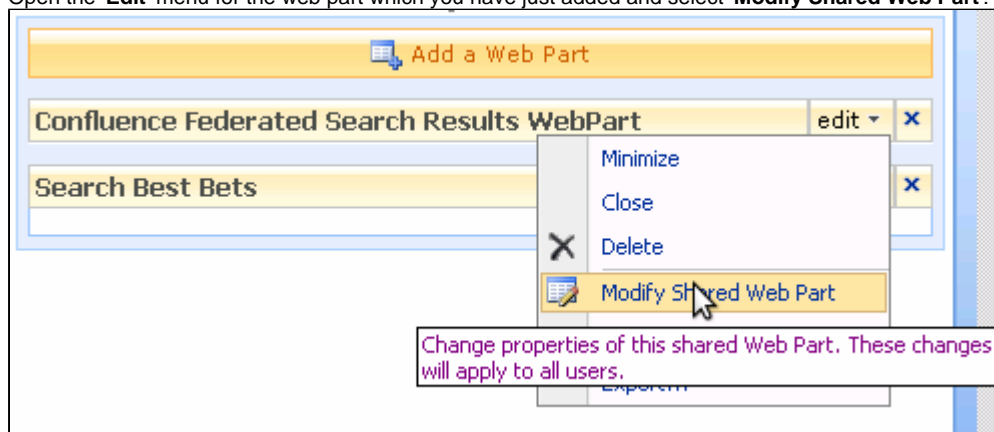
2. Click '**Site Actions**', then '**Edit Page**':



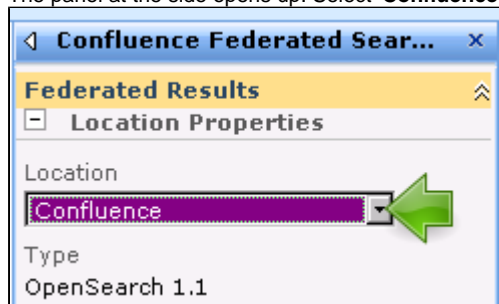
- Click 'Add a Web Part'. You can add the web part anywhere on the page. This is where the Confluence results will appear:



- The 'Add Web Parts' screen appears. Select the web part:
 - With SSO:** If you are using SSO and checked 'Use SSO' when setting up the federated location, then select '**Federated Results**'.
 - Without SSO:** If you are not using SSO and did not check 'Use SSO' when setting up the federated location, then select '**Confluence Federated Search Results WebPart**'.
- Click the 'Add' button.
- Open the 'Edit' menu for the web part which you have just added and select 'Modify Shared Web Part':



- The panel at the side opens up. Select 'Confluence' (or whatever you named the federated location) from the dropdown menu:



- Click 'OK', then 'Exit Edit Mode'. Setup is complete.

RELATED TOPICS

[Installing and Configuring the SharePoint Feature on SP 2007](#)
[Installing the SharePoint Connector](#)

Installing the SharePoint Connector on SP 2010

This page describes the requirements and procedures for installing the **SharePoint Connector 1.3** on **SharePoint 2010**.

Prerequisites and Planning your Configuration

1. Check the [system requirements and supported platforms](#).
2. Plan your configuration, using our [guidelines on selecting a supported authentication configuration](#).

Installation and Configuration

Install and configure the components in this order:

1. [Configure the access to SharePoint](#).
2. [Install and configure the plugins in Confluence](#).
3. [Configure the access to Confluence](#).
4. [Install and configure the feature in SharePoint](#).

Planning your Environment with SP 2010

This section provides guidelines on planning the infrastructure and configuration necessary to support your installation of the Confluence SharePoint Connector.

These instructions apply if you are using the connector with **SharePoint 2010**. If you have SharePoint 2007 WSS or MOSS, please refer to the [planning guide for SharePoint 2007](#).

On this page:

- [Prerequisites and Supported Platforms](#)
- [Supported Configurations](#)
 - [Configuring Access to SharePoint](#)
 - [Selecting your Configuration for Access to SharePoint](#)
 - [Configuring Access to Confluence](#)
 - [Selecting your Configuration for Access to Confluence](#)
- [Unsupported Configurations](#)
 - [Atlassian Crowd](#)
 - [SiteMinder and other Single Sign-On Management Solutions](#)
 - [SharePoint Forms-Based Authentication](#)
- [Next Step](#)

Prerequisites and Supported Platforms

Please ensure you read through and comply with the following requirements before installing the SharePoint Connector.

Windows

The Confluence SharePoint Connector supports the same Windows operating system requirements as those specified by Microsoft for SharePoint.

Confluence

You need **Confluence 2.10.0 or later**. You can download Confluence from the [Confluence download centre](#).



.NET Framework required on Windows

Note that if you are running Confluence on a Windows Server, you should ensure that the Microsoft .NET Framework 2.0 is installed. Microsoft .NET is required for Confluence in certain configurations (see the guide on [Configuring Access to SharePoint with SP 2010](#) for more information).

You can download the .NET Framework 2.0 [here](#) (for the 32-bit version) or [here](#) (for the 64-bit version).

SharePoint



These instructions apply if you are using the connector with **SharePoint 2010**. If you have SharePoint 2007 WSS or MOSS, please refer to the [planning guide for SharePoint 2007](#).

Versions 1.2 and later of the SharePoint Connector support Microsoft SharePoint 2010. This includes SharePoint Foundation 2010 and SharePoint Server 2010. For a quick guide to the different SharePoint versions available, see our [comparison of SharePoint versions and editions](#). Some features of the SharePoint Connector are only available when using SharePoint Server 2010, as described below.

1. You will need **SharePoint Foundation 2010** as a minimum requirement.
 - To check if SharePoint Foundation 2010 is installed, go to **Start -> All Programs -> Microsoft SharePoint 2010 Products -> SharePoint 2010 Central Administration**. If you can see 'SharePoint 2010 Central Administration', then SharePoint Foundation has already been installed.
2. (Optional) For added functionality, you need **Microsoft SharePoint Server 2010** (Standard or Enterprise)
 - SharePoint Server 2010 is **required** for the following features:
 - a. For the federated search feature. For more information, see our guide to [configuring the SharePoint federated](#)

[search](#).









- b. For Secure Store Service (single sign-on) functionality from SharePoint using Windows Integrated Authentication to Confluence. For more information, see the [Microsoft product information](#).
- For the Confluence SharePoint Connector, it makes no difference whether you have SharePoint Server 2010 Standard or SharePoint Server 2010 Enterprise edition.

Checking whether you have SharePoint Foundation 2010 or SharePoint Server 2010

To determine whether you have SharePoint Foundation 2010 or SharePoint Server 2010 installed, go to Windows **Start -> Control Panel -> Programs -> Programs and Features**.

- If you see 'Microsoft SharePoint Server 2010' in the list, then SharePoint Server 2010 has been installed.
- If you see only 'Microsoft SharePoint Foundation 2010' (and not 'Microsoft SharePoint Server 2010') then you only have SharePoint Foundation 2010 installed.

Table: SharePoint Connector feature compatibility matrix

Feature	Supported in SharePoint Foundation 2010	Supported in SharePoint Server 2010
Embed Confluence content in SharePoint (Web Parts)		
Embed SharePoint content in Confluence (Macros)		
Integration with Microsoft Secure Store Service		
Federated Search		



We recommend separate server machines for Confluence and SharePoint

Due to the substantial memory and CPU requirements of SharePoint, we recommend that you run Confluence and SharePoint on separate machines. For evaluation purposes, it is OK to run them both on the same machine.

Supported Configurations

Next, please decide which of the supported configurations is best suited to your environment. There are two areas to consider when setting up the SharePoint Connector and deciding which authentication methods to use:

- Configuring access to SharePoint
- Configuring access to Confluence

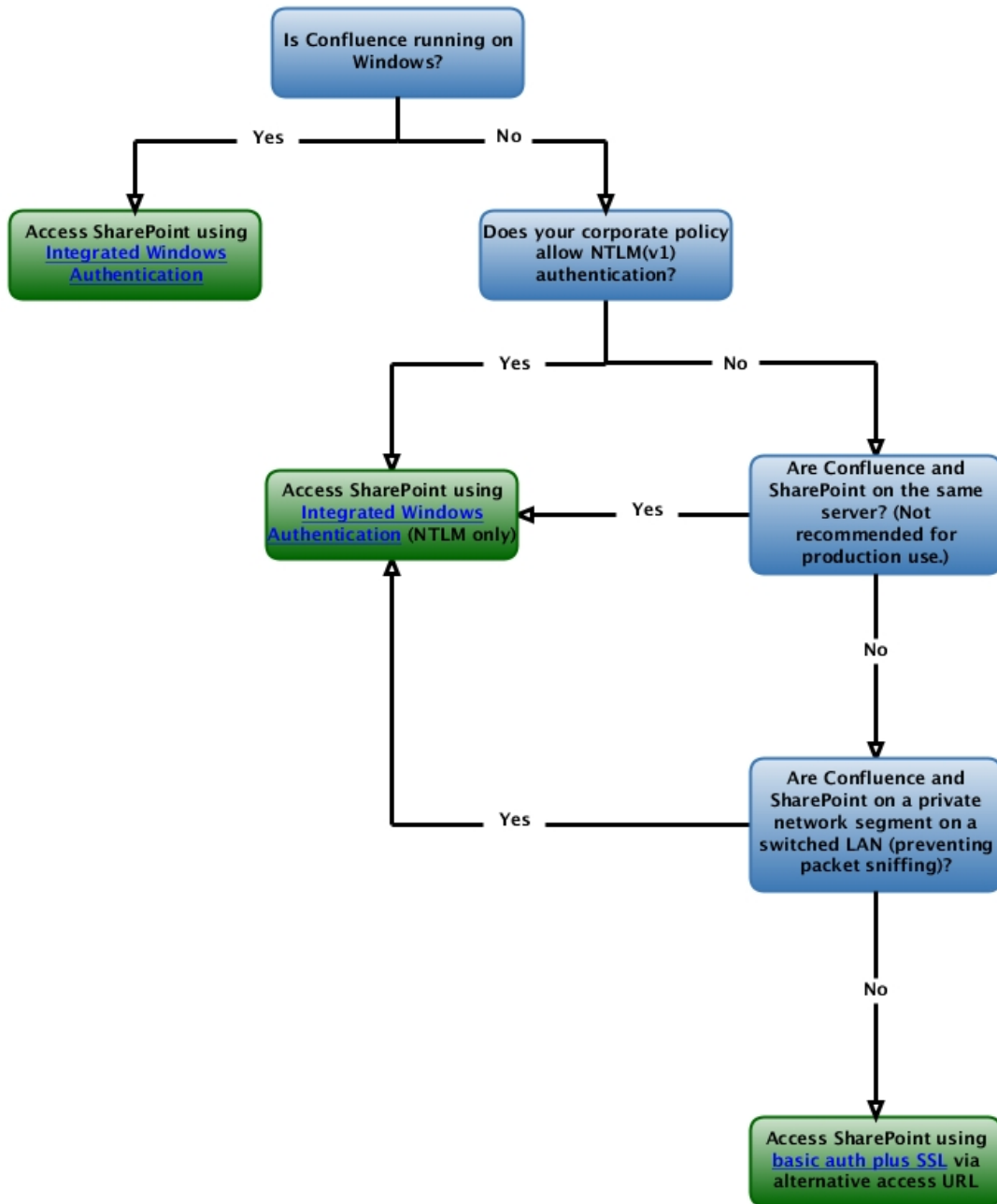
Configuring Access to SharePoint

These configurations control the authentication method used by the Confluence server and client browsers when requesting content from the SharePoint server.

- [Access SharePoint using Integrated Windows Authentication with SP 2010](#)
- [Access SharePoint using Integrated Windows Authentication \(NTLM Only\) with SP 2010](#)
- [Access SharePoint using Basic Authentication and SSL \(via Alternative Access URL\) with SP 2010](#)

Selecting your Configuration for Access to SharePoint

Configuring the Access to Microsoft SharePoint 2010 When Using the SharePoint Connector



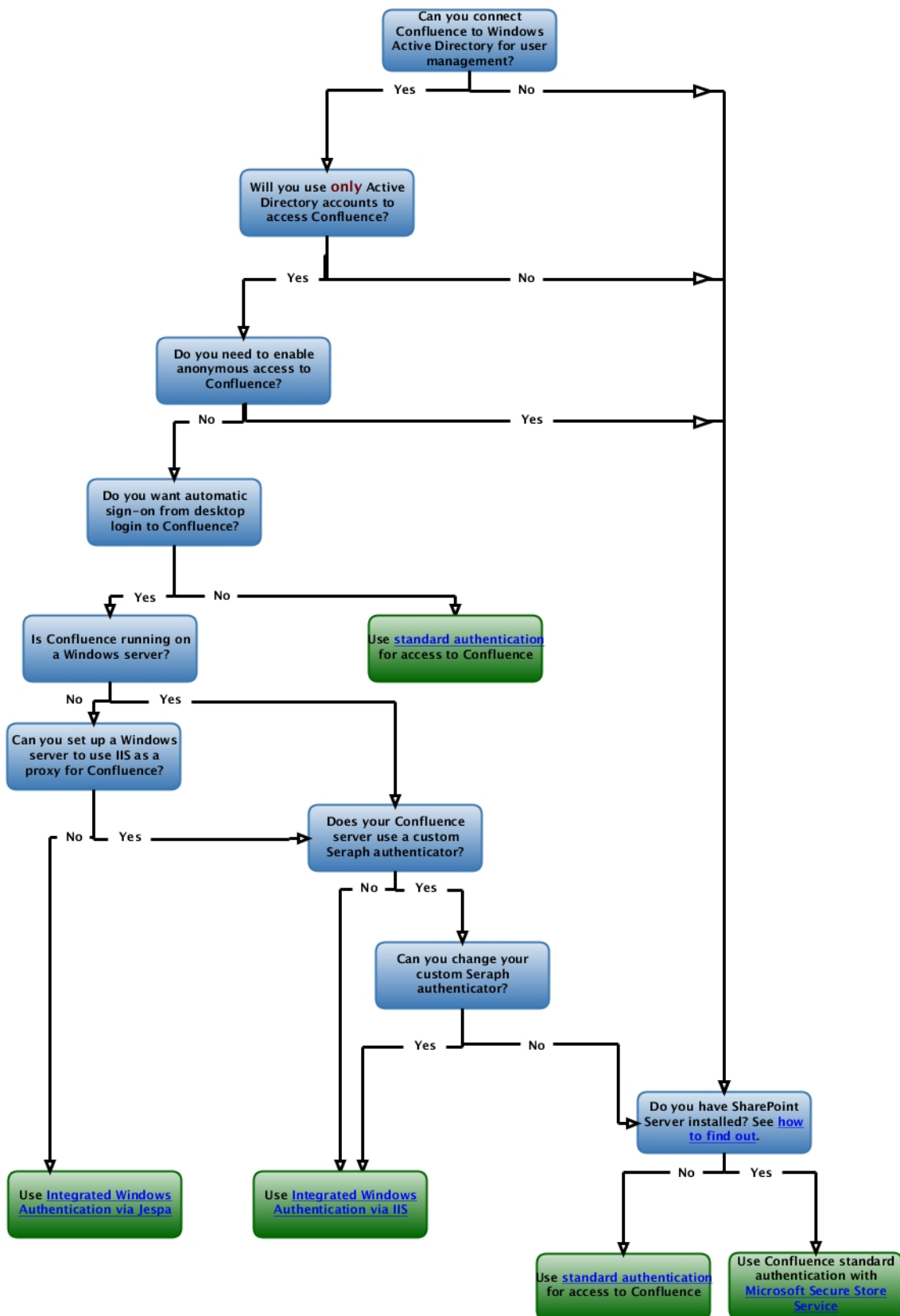
Configuring Access to Confluence

These configurations control the authentication method used by the SharePoint server and client browsers when requesting content from the Confluence server.

- Access Confluence using Integrated Windows Authentication via IIS with SP 2010
- Access Confluence using Integrated Windows Authentication via Jespa with SP 2010
- Access Confluence using Standard Authentication with SP 2010
- Access Confluence using Standard Authentication with Secure Store Service on SP 2010

Selecting your Configuration for Access to Confluence

Configuring the Access to Confluence When Using the SharePoint Connector with SP 2010



Unsupported Configurations

Atlassian support does not cover the configurations listed below.

Atlassian Crowd



Not supported:

Crowd is Atlassian's single sign-on (SSO) and user management solution. For the initial release of the SharePoint Connector, we made a decision to delay full support for Crowd in favour of Microsoft's Single Sign-On Service (Microsoft SSOSrv). At the time, we felt that Microsoft SSOSrv's tight integration with SharePoint was a more compelling feature for SharePoint customers.

As the SharePoint Connector matures, we are now looking at expanding our support to reach a broader customer base. We hope to support Crowd for SSO in the future.

If you are interested in this feature, we encourage you to vote for the feature request in our JIRA issue tracker: [CSI-588](#).

SiteMinder and other Single Sign-On Management Solutions



Microsoft SSO and Secure Store Service are supported:

We have tested the connector with the following single sign-on solutions from Microsoft:

- Single Sign-On Service, provided with MOSS 2007.
- Secure Store Service provided with SharePoint Server 2010 (available with version 1.2 and later of the SharePoint Connector).



Not supported:

We have not tested any other single sign-on products. If you are interested in support for other SSO solutions, we encourage you to vote for the relevant request if it already exists in our JIRA issue tracker or create a new request. When voting or adding a request, please describe your environment.

- Request for SiteMinder integration: [CSI-218](#)

SharePoint Forms-Based Authentication



Not supported:

The SharePoint Connector cannot connect to SharePoint sites that use an ASP.NET Forms authentication provider. We may add support for this configuration in the future. If you are interested in this feature, we encourage you to vote for the feature request in our JIRA issue tracker: [CSI-590](#).

Next Step

To continue with the installation of the SharePoint Connector, please [configure the access to SharePoint](#).

Configuring Access to SharePoint with SP 2010

This section describes the methods which may be used to **configure access to SharePoint** for the SharePoint Connector. You should complete one of the supported configuration guides before proceeding further with the SharePoint Connector installation. If you have not already seen our guide to [planning your environment](#), please refer to it now for information that will help you select the best configuration for your environment. These instructions apply to the connector for SharePoint 2010.

Please follow one of these configuration guides:

- [Access SharePoint using Integrated Windows Authentication with SP 2010](#)
- [Access SharePoint using Integrated Windows Authentication \(NTLM Only\) with SP 2010](#)
- [Access SharePoint using Basic Authentication and SSL \(via Alternative Access URL\) with SP 2010](#)

Next Step

To continue with the installation of the SharePoint Connector, please [install and configure the Confluence plugins](#).

Access SharePoint using Integrated Windows Authentication with SP 2010

This page is part of the installation guide for the **Confluence SharePoint Connector**. It tells you about accessing SharePoint via Integrated Windows Authentication. These instructions apply to SharePoint 2010.

On this page:

- [Overview](#)
- [Installation Instructions](#)
- [Next Step](#)

Overview

In this configuration, both Confluence and client browsers authenticate against SharePoint using Integrated Windows Authentication (IWA).

Use this Configuration when...

- Confluence is running on a Windows server.

If you have not already seen our guide to [planning your environment](#), you can refer to it for information that will help you select the best configuration for your environment.

Installation Instructions

IWA is the default configuration for your SharePoint server. No additional configuration to SharePoint is required.

However, you must ensure that Microsoft .NET Framework 2.0 is installed on your Confluence server. You can download the .NET Framework 2.0 [here](#) (for the 32-bit version) or [here](#) (for the 64-bit version).

Next Step

To continue with the installation of the SharePoint Connector, please [install and configure the Confluence plugins](#).

Access SharePoint using Integrated Windows Authentication (NTLM Only) with SP 2010

This page is part of the installation guide for the **Confluence SharePoint Connector**. It tells you how to configure access to SharePoint using Integrated Windows Authentication (NTLM only). These instructions apply to the connector for SharePoint 2010.

On this page:

- [Overview](#)
- [Caveats](#)
- [NTLM Only](#)
- [Additional Layers of Security](#)
- [Installation Instructions](#)
 - [Domain or Local?](#)
 - [Password Length](#)
 - [LAN Manager Authentication Level](#)
 - [Minimum Session Security for NTLM SSP-Based Servers](#)
 - ['Do Not Store LAN Manager Hash' Value](#)
 - [Reboot Your SharePoint Server](#)
- [Next Step](#)

Overview

In this configuration, both Confluence and client browsers authenticate against SharePoint using Integrated Windows Authentication (NTLM only).

Use this Configuration when...

- Confluence is **not** running on a Windows server. (If Confluence is running on Windows, you can use [full IWA](#).)
- There is minimal risk of eavesdropping on the network traffic from Confluence to SharePoint. Examples of scenarios involving minimal risk include:
 - The Confluence and SharePoint applications are on the same physical server. (For production use, we recommend that you run Confluence and SharePoint on separate machines, but you may choose to run them on the same server for evaluation purposes.)
 - The SharePoint site(s) are accessed using HTTP Secure (HTTPS).
 - The Confluence and SharePoint servers are on a private network segment.

If you have not already seen our guide to [planning your environment](#), you can refer to it for information that will help you select the best configuration for your environment.

Caveats

NTLM Only

When configuring authentication for a top-level SharePoint site, the **SharePoint Central Administration** application allows administrators to select Integrated Windows Authentication using NTLM or Kerberos (or both).

Due to the limited number of authentication methods supported by the SharePoint Connector's Java components (see the section on additional layers of security [below](#)), in order for a site collection to be accessible from Confluence, the NTLM authentication option **must** be selected.

Additional Layers of Security

If you are concerned about the possibility of password hashes sent from Confluence to SharePoint being captured and decoded by a third party, Atlassian recommends that you apply additional layers of security (such as HTTP Secure) if you use this configuration.

Because Confluence is written in Java, it has a dependency on the Sun Java Virtual Machine's (JVM's) internal NTLM implementation to decode NTLM challenge messages from the server and issue encoded NTLM responses. Our testing of the SharePoint Connector with recent versions of the Sun JVM (1.6.*) indicate that the JVM is only able to reliably work with the NTLM and LAN Manager (LM) Windows Authentication protocols. Newer (and more secure) protocols such as NTLMv2 and Kerberos are not supported in this configuration.

LM authentication and to a lesser extent, NTLM, are regarded as weak authentication mechanisms and there are widely accessible tools for deciphering passwords encrypted with LM and NTLM. Atlassian recommends that you apply additional layers of security (such as HTTP Secure) if you use this configuration.

Installation Instructions

Domain or Local?

If your Windows user accounts are stored in Active Directory, then the configuration steps listed here must be applied to all **Domain Controllers**. If your user accounts are local accounts on the SharePoint Server, then the configuration steps must be applied to your **SharePoint server**.

LAN Manager Authentication Level

The LAN Manager Authentication Level controls what network authentication methods are supported by Windows clients and servers. The authentication level is controlled via a registry entry (called **LMCompatibilityLevel**) or a group policy setting (called **Network Security: LAN Manager Authentication Level**).

In order for Confluence to successfully authenticate against the SharePoint server, the LAN Manager Authentication Level must be set to one of the following values:

Registry Key Value	Group Policy Value
0	Send LM & NTLM responses
1	Send LM & NTLM - use NTLMv2 session security if negotiated
2	Send NTLM response only
3	Send NTLMv2 response only
4	Send NTLMv2 response only. Refuse LM

For more information on how to alter this setting and greater detail on what the value of each setting entails, please consult this [Microsoft TechNet article](#).

Note that this registry value does not need to be modified on the Confluence server. Confluence uses a Java HTTP client that is unaware of the Windows configuration.

Symptoms of Unsupported LM Authentication Level

Using an unsupported LAN Manager Authentication Level will have the following results:

- SharePoint will return an error: `'HTTP 401.1 Unauthorised: Access is denied due to invalid credentials'`.
- The error message you may see in Confluence is: `'org.apache.cxf.Interceptor.Fault: Could not send Message'`.

Reboot Your SharePoint Server

We strongly recommend that you restart your SharePoint server after applying any of these configuration settings in order to ensure that they take effect.

Additionally, changes to your group policy may take a short while to propagate through your domain. Please keep this in mind when testing your configuration.

Next Step

To continue with the installation of the SharePoint Connector, please [install and configure the Confluence plugins](#).

Access SharePoint using Basic Authentication and SSL (via Alternative Access URL) with SP 2010

This page is part of the installation guide for the **Confluence SharePoint Connector**. It tells you how to configure access to SharePoint using basic authentication and SSL via an alternative access URL in SharePoint. These instructions apply to the connector for SharePoint 2010.

On this page:

- [Overview](#)
- [Caveats](#)
 - [Server Certificate](#)
- [Installation Instructions](#)
 - [Configuring SharePoint](#)
 - [Step 1: Extend the SharePoint Site to Another IIS Web Site](#)
 - [Step 2: Configure the IIS Authentication Providers](#)
 - [Step 3: Configure the Alternate Access Mappings](#)
 - [Step 4: Import the SSL Certificate into IIS](#)
 - [Step 5: Restrict the IIS Web Site to Confluence](#)
 - [Configuring Confluence](#)
 - [Step 1: Trust SharePoint's SSL Certificate](#)
 - [Step 2: Configure the Alternative URL in Confluence](#)

Overview

In this configuration, client browsers authenticate against SharePoint using Integrated Windows Authentication (NTLM or Kerberos). Confluence however, authenticates against SharePoint on a separate port that is configured to use basic authentication over Secure Sockets Layer (SSL). This is accomplished using SharePoint's capability to extend a site collection over multiple web applications. Using alternative access mappings in SharePoint, all hyperlinks in the SharePoint content direct users back to the primary SharePoint site.

This configuration method offers a greater level of security than the method that [accesses SharePoint using Integrated Windows Authentication \(NTLM Only\)](#). The configuration procedure is, however, more complex. You should review the security measures of your internal network before deciding which method is most appropriate for your environment.

Use this Configuration when...

- Confluence is **not** running on a Windows server.
- Your corporate security policy prohibits the use of NTLM(v1) authentication, which is necessary for the [NTLM](#) configuration.
- Your SharePoint site(s) is/are not configured to use Secure HTTP (HTTPS) and you are concerned about the possibility of packet sniffing or eavesdropping.

If you have not already seen our guide to [planning your environment](#), you can refer to it for information that will help you select the best configuration for your environment.

Caveats

Server Certificate

Enabling SSL requires the installation of a certificate on the SharePoint server. Depending on the way in which you source the certificate, this could involve either an additional financial cost or a number of additional configuration steps.

Installation Instructions

Configuring SharePoint



Use IE7+ when Configuring SharePoint

We recommend that you use Internet Explorer 7 or later to perform the configuration steps described on this page. You may experience unusual behaviour if you use FireFox or other browsers on some SharePoint administrative pages.

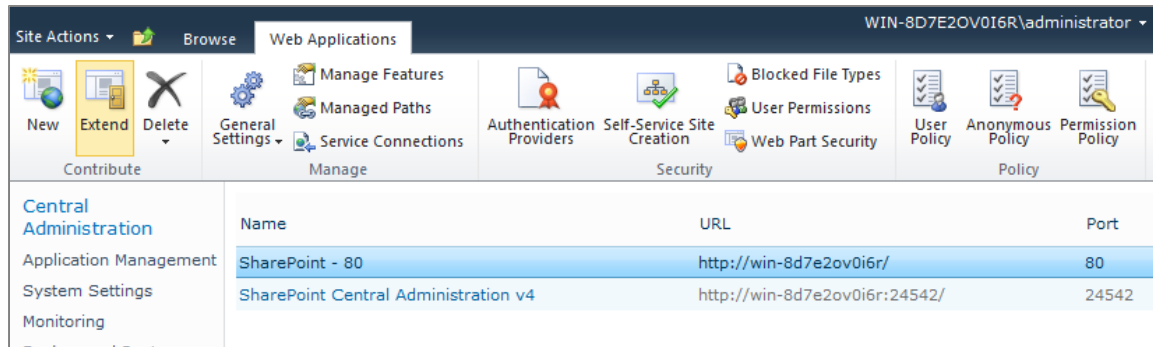


Configure all SharePoint Top-Level Sites used by Confluence

You will need to perform these configuration steps for each SharePoint top-level site that is exposed to Confluence.

Step 1: Extend the SharePoint Site to Another IIS Web Site

1. Log in to **SharePoint Central Administration** and select the '**Application Management**' portal.
2. In the '**Web Applications**' section, select '**Manage web applications**'.
3. Select the required SharePoint site and click '**Extend**'.
[*Screenshot: Selecting 'Extend' for a SharePoint site*](#)



4. The '**Extend Web Application to Another IIS Web Site**' screen appears. Select '**Create a new IIS web site**'
5. Fill out the details of the new site:
 - Add a meaningful name that describes the purpose of the site.
 - Ensure that the IIS web site is assigned a unique port that is not currently in use on your SharePoint server.
 - Ensure that '**Allow Anonymous**' is set to '**No**'.
 - Ensure that '**Use Secure Sockets Layer (SSL)**' is set to '**Yes**'.
 - Make a note of the '**Zone**' that is set for the '**Load Balanced URL**'. You will need to know this zone in step 2 below.
6. Click '**OK**'.

Screenshot: Extending the SharePoint site to another IIS web site

IIS Web Site

Choose between using an existing IIS web site or create a new one to serve the Microsoft SharePoint Foundation application.

If you select an existing IIS web site, that web site must exist on all servers in the farm and have the same name, or this action will not succeed.

If you opt to create a new IIS web site, it will be automatically created on all servers in the farm. If an IIS setting that you wish to change is not shown here, you can use this option to create the basic site, then update it using the standard IIS tools.

Security Configuration

Kerberos is the recommended security configuration to use with Integrated Windows authentication. Kerberos requires the application pool account to be Network Service or special configuration by the domain administrator. NTLM authentication will work with any application pool account and the default domain configuration.

If you choose to use Secure Sockets Layer (SSL), you must add the certificate on each server using the IIS administration tools. Until this is done, the web application will be inaccessible from this IIS web site.

Public URL

The public URL is the domain name for all sites that users will access in this SharePoint Web application. This URL domain will be used in all links shown on pages within the web application. By default, it is set to the current servername and port.
<http://go.microsoft.com/fwlink/?LinkId=114854>

Options:

- ☐ Use an existing IIS web site (Default Web Site)
- ☒ Create a new IIS web site
 - Name: My site - Confluence access - 9090
 - Port: 9090
 - Host Header:
 - Path: C:\inetpub\wwwroot\wss\VirtualDirector

Authentication provider:

- ☐ Negotiate (Kerberos)
- ☒ NTLM

Allow Anonymous: ☐ Yes ☒ No

Use Secure Sockets Layer (SSL): ☒ Yes ☐ No

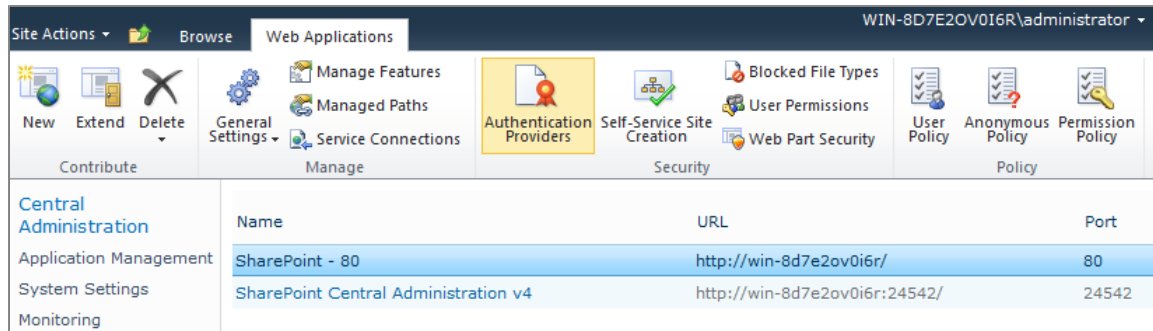
URL: https://WIN-8D7E2OV0I6R:9090

Zone: Internet

OK Cancel

Step 2: Configure the IIS Authentication Providers

1. Go back to SharePoint's '**Manage web applications**' section.
 2. Select the required SharePoint site and click '**Authentication Providers**'.
- Screenshot: Selecting 'Authentication Providers' for a SharePoint site*



3. The '**Authentication Providers**' screen appears. Click the name of the **Zone** (such as, 'Intranet' or 'Internet') that you used to extend the SharePoint site in step 1 [above](#).
4. The '**Edit Authentication**' screen appears. Ensure that '**Integrated Windows authentication**' is not selected and '**Basic authentication (password is sent in clear text)**' is selected.
5. Click '**Save**'.



SSL will secure the password information

Because this endpoint will be using Secure Sockets Layer (SSL), the password will not be sent in clear text even though basic authentication is used.

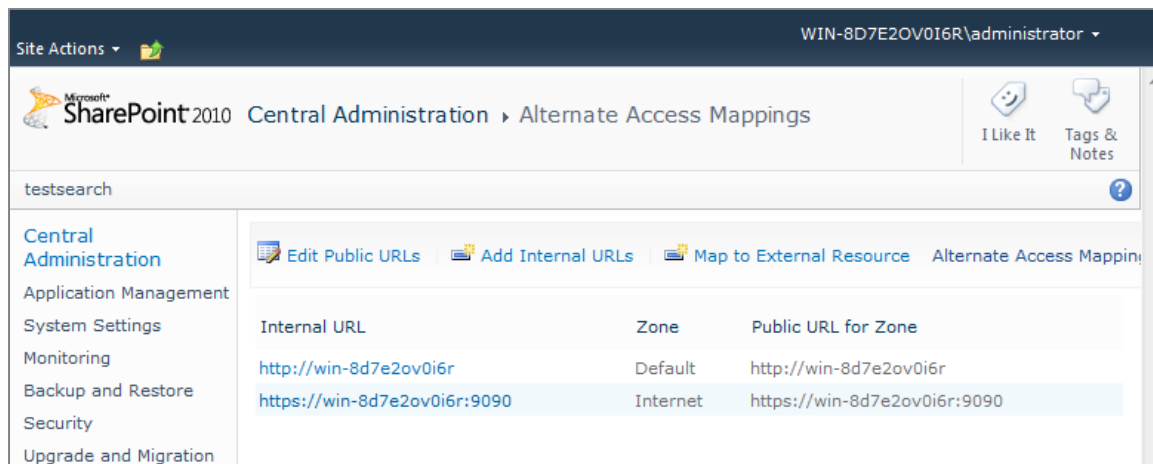
Screenshot: Editing the IIS authentication settings

Edit Authentication	
Zone These authentication settings are bound to the following zone.	Zone Internet
Authentication Type Choose the type of authentication you want to use for this zone. Learn about configuring authentication.	Authentication Type <input checked="" type="radio"/> Windows <input type="radio"/> Forms Click here for details on how to enable Forms Based Authentication in claims mode. <input type="radio"/> Web single sign on Click here for more details.
Anonymous Access You can enable anonymous access for sites on this server or disallow anonymous access for all sites. Enabling anonymous access allows site administrators to turn anonymous access on. Disabling anonymous access blocks anonymous users in the web.config file for this zone. Note: If anonymous access is turned off when using Forms authentication mode, Forms aware client applications may fail to authenticate correctly.	<input type="checkbox"/> Enable anonymous access
Client Object Model Permission Requirement You can require that the user must have the Use Remote Interfaces permission in order to use the Client Object Model to access the server. The Client Object Model is used by some parts of the UI. Enabling this prevents users from performing some tasks using the UI if they do not have the Use Remote Interfaces permission.	<input type="checkbox"/> Require Use Remote Interfaces permission
IIS Authentication Settings Kerberos is the recommended security configuration to use with Integrated Windows authentication. Kerberos requires the application pool account to be Network Service or special configuration by the domain administrator. NTLM authentication will work with any application pool account and the default domain configuration.	<input type="checkbox"/> Integrated Windows authentication <input type="radio"/> Negotiate (Kerberos) <input checked="" type="radio"/> NTLM <input checked="" type="checkbox"/> Basic authentication (password is sent in clear text)
Client Integration Disabling client integration will remove features which launch client applications. Some authentication mechanisms (such as Forms) don't work well with client applications. In this configuration, users will either have to use browser-based editors to edit their documents or work on them locally and upload changes. Note: If client integration is turned on in conjunction with Forms mode, anonymous access should also be turned on or Forms aware client applications may fail to authenticate correctly.	Enable Client Integration? <input checked="" type="radio"/> Yes <input type="radio"/> No
<div> <input type="button" value="Save"/> <input type="button" value="Cancel"/> </div>	

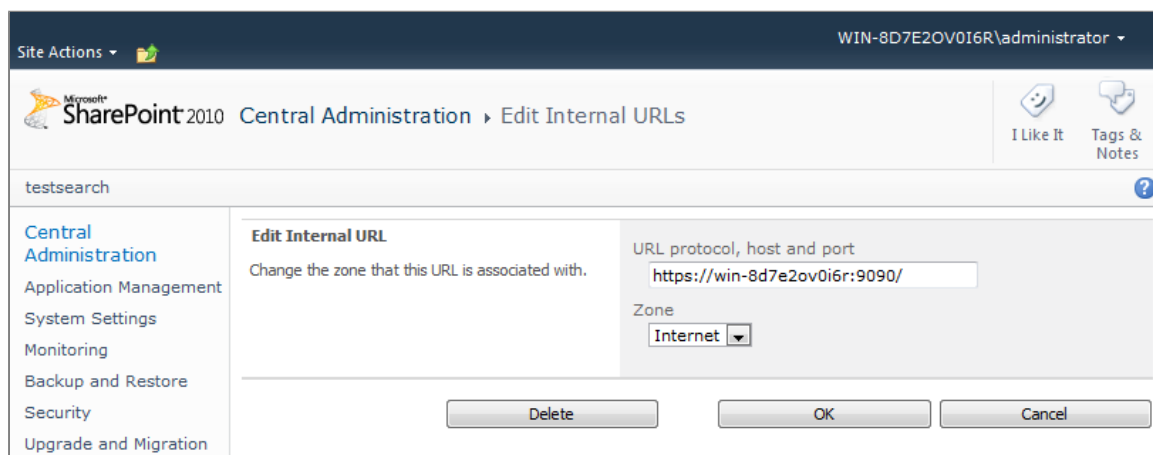
Step 3: Configure the Alternate Access Mappings

In this step you will remove the default public URL that SharePoint created during the previous step and replace it with an internal URL mapping.

1. Go back to **SharePoint Central Administration** and select the '**System Settings**' portal.
2. In the '**Farm Management**' section, select '**Configure alternate access mappings**'.
3. Click the link on the '**Internal URL**' that represents the newly-created IIS web site defined in step 1 above.
[Screenshot: Finding the newly-created alternate access mapping to delete](#)

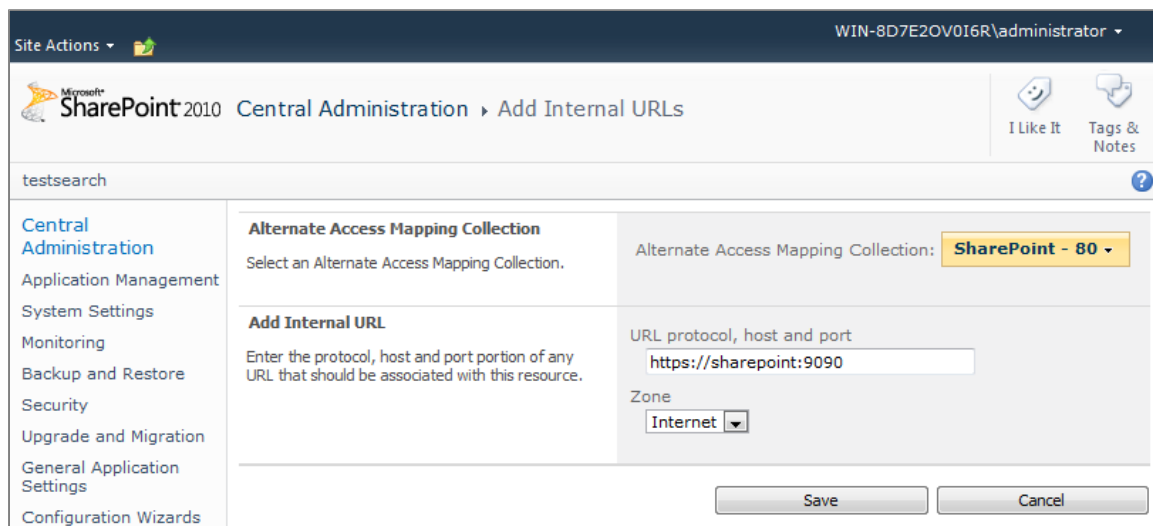


4. Click the **'Delete'** link to remove this mapping.
Screenshot: Deleting the alternate access mapping



5. Click **'Add Internal URLs'**.
6. Select the **'Alternate Access Mapping Collection'** that represents the root SharePoint site that you are extending.
7. Set the **'URL protocol, host and port'** to the URL that directs to the newly-created IIS web site defined in step 1 above.
8. Click **'Save'**.

Screenshot: Adding the alternate access mapping



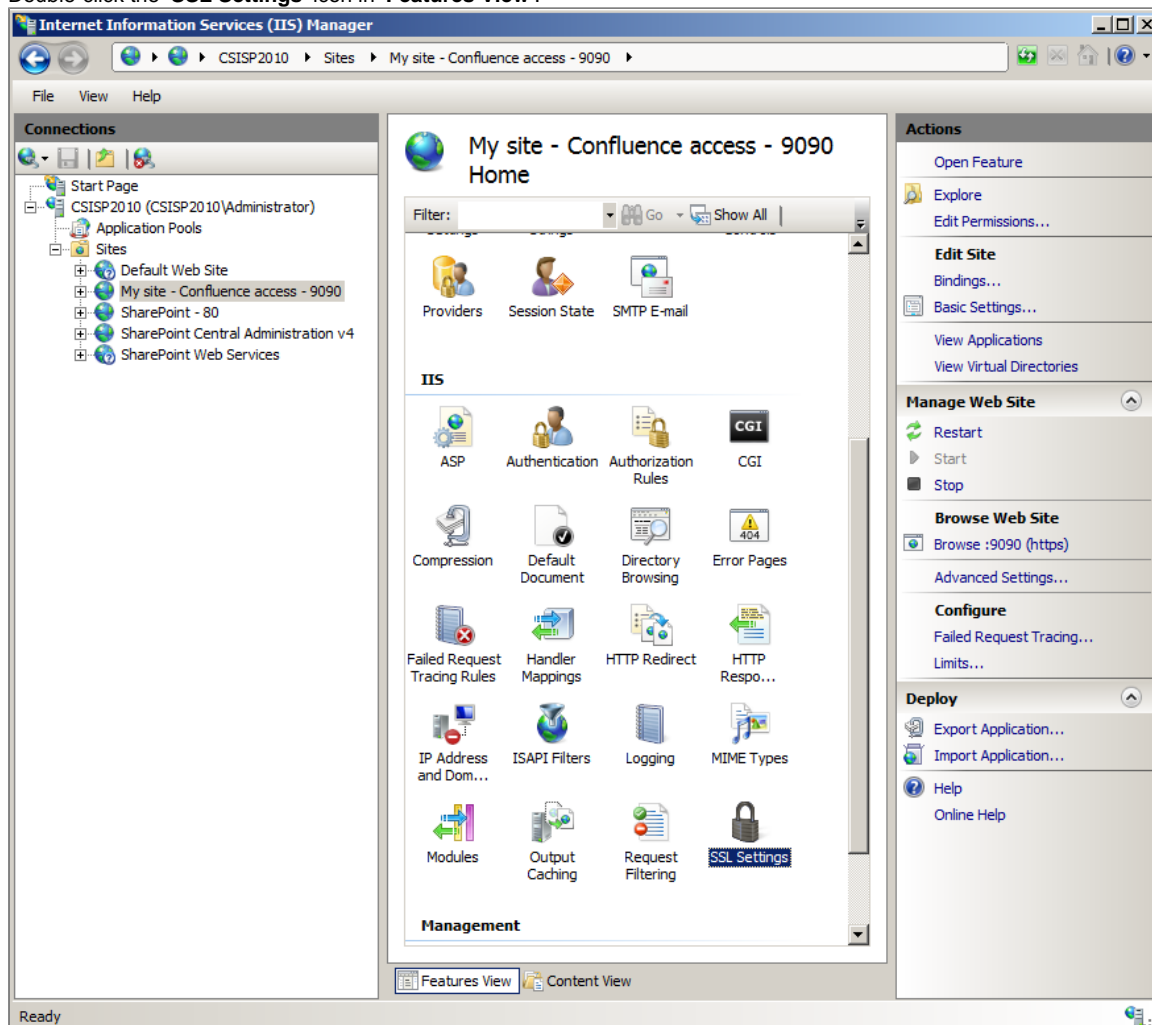
Step 4: Import the SSL Certificate into IIS

In this step you will ensure that your IIS web site is configured for SSL and import an SSL certificate into the IIS web site.

Step 4.1: Make Sure the IIS Web Site is Configured for SSL

1. Log in to your SharePoint server with a Windows account that has permission to administer IIS.
2. Run the **'Internet Information Services (IIS) Manager'**.

- In the **'Connections'** panel on the left, expand the **'Sites'** folder and click on the IIS web site that you created in step 1 [above](#). You can identify this web site by looking at the **'Description'** field.
- Double-click the **'SSL Settings'** icon in **'Features View'**.



- Ensure that the **'Require SSL'** option is selected.
- Click **'Apply'** in the **'Actions'** panel on the right.

Step 4.2: Obtain or Create a Certificate



SharePoint already accepting SSL?

If your SharePoint Server already accepts SSL traffic, then you already have a certificate installed on your SharePoint server. If this is the case, please skip ahead to step 4.3 [below](#).

You need an X.509 certificate that you can import into IIS. IIS will use the certificate to encrypt the SSL channel and prove the server's identity to clients. In the table below are the two ways of obtaining a certificate.



Disclaimer

Atlassian does not endorse or represent any of the example certificate issuers listed below.

Atlassian cannot accept responsibility for the veracity of any digital certificate issued by a third party. You should ensure that any certificate you use is from a provider that you trust.

Option	Example Provider	Benefit	Drawback
Obtain a certificate from a trusted certificate authority	Thawte Consulting Verisign	Most major certificate authorities are automatically trusted by most modern operating systems, so no configuration is required on the client to trust your certificate.	The certificate authority may charge a fee for issuing the certificate and/or an annual renewal fee.
Generate your own certificate	x509Builder Java keytool	Free	Client computers may require configuration to trust your certificate's authenticity.

Step 4.3: Import the Certificate into IIS

Once you have generated or obtained a certificate, you will usually receive:

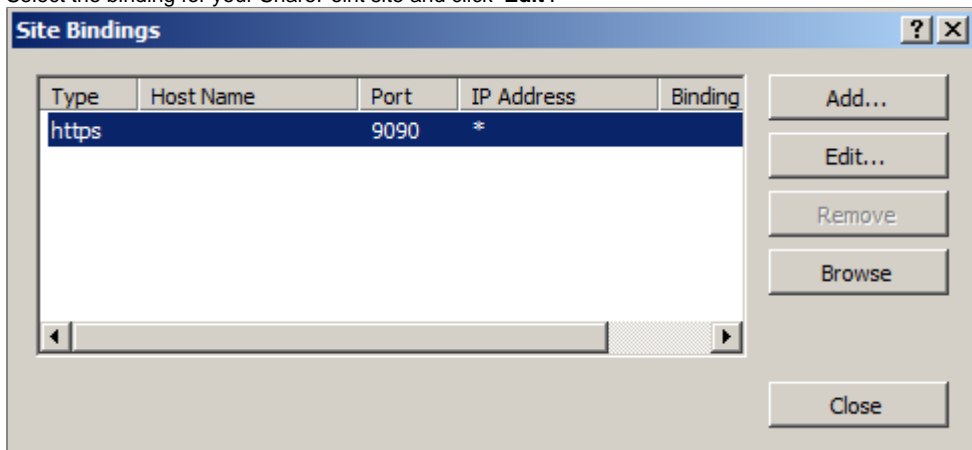
- The certificate stored in a file format such as `pfx`.
- A password that encrypts the file.

Follow these instructions to import the certificate into IIS:

1. Copy the certificate file to your SharePoint server.
2. Log in to your SharePoint server with a Windows account that has permission to administer IIS.
3. Run the **'Internet Information Services (IIS) Manager'**.
4. Select the local IIS Web Server in the **'Connections'** panel on the left.
5. Double-click the **'Server Certificates'** icon in the **'Features View'**.
6. Click the **'Import'** link in the Actions panel on the right.
7. Set the **'Certificate file (.pfx)'** field to the path to your certificate file on your SharePoint server.
8. Enter the **'Password'** for certificate.
9. Click **'OK'**.

Step 4.4: Configure SSL Binding

1. In the **'Connections'** panel on the left, expand the **'Sites'** folder and click on the IIS web site that you created in step 1 above. You can identify this web site by looking at the **'Description'** field.
2. In the **'Actions'** panel on the right, click **'Bindings'**.
3. Select the binding for your SharePoint site and click **'Edit'**.



4. In the **'SSL certificate:'** field, select the SSL Certificate that you imported into IIS in Step 4.3.
5. Click **'OK'**.
6. Click **'Close'**.

**Test your configuration**

Make sure that you test your SSL configuration by accessing the SharePoint site in a web browser, before proceeding any further.

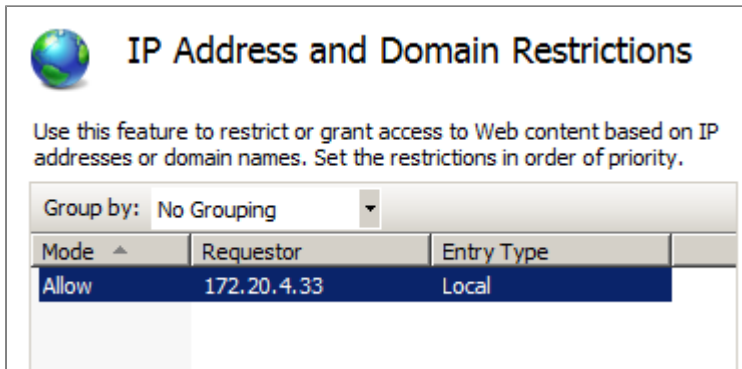
Step 5: Restrict the IIS Web Site to Confluence

As an additional layer of security, you should configure your SSL-secured web site to allow access from the Confluence server only.

**Confluence must have a static IP address or DHCP lease reservation**

You will only be able to perform this step if your Confluence server has a static IP address. If your Confluence server has a dynamic IP address, then speak to your network administrator about adding a static IP address or a DHCP lease reservation for the Confluence server.

1. Note the IP address of your Confluence server.
2. Log in to your SharePoint server with a Windows account that has permission to administer IIS.
3. Run the **'Internet Information Services (IIS) Manager'**.
4. In the **'Connections'** panel on the left, expand the **'Sites'** folder and click on the IIS web site that you created in step 1 above. You can identify this web site by looking at the **'Description'** field.
5. Double-click on **'IP Address and Domain Restrictions'** in the **'Features View'**.
6. Click **'Edit Feature Settings'** in the **'Actions'** panel on the right.
7. In the **'Edit IP and Domain Restrictions Settings'** popup, set the **'Access for unspecified clients:'** to **'Deny'**.
8. Click **'OK'**.
9. Click **'Add Allow Entry'** in the **'Actions'** panel on the right.
10. In the **'Specific IP address:'** field, enter the IP Address of your Confluence server.
11. Click **'OK'**.

Screenshot: IP restriction on IIS web site**Configuring Confluence****Step 1: Trust SharePoint's SSL Certificate****Skip all of step 1 if you obtained a certificate from a trusted CA**

If you purchased a certificate from a trusted certificate authority, then your certificate is already trusted by the Confluence server and you can skip this step. Go to step 2 [below](#). If you generated your own certificate or obtained one from a less well-known certificate authority, please follow the steps below.

To configure Confluence to trust the certificate on your SharePoint server, you must add the certificate's public key to the Java runtime's Certificate Authority keystore as described below.

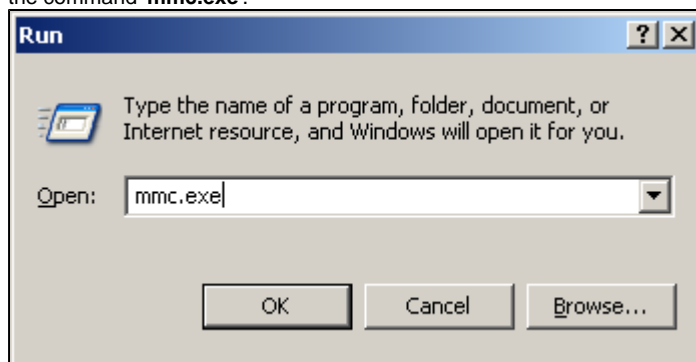
Step 1.1: Create a .cer File**Skip step 1.1 if you already have a .cer file**

The certificate's public key must be imported into the Java keystore as a certificate file in .cer file format. If you already have a .cer file you can skip this step and go to step 1.2 [below](#). If you only have a .pfx file and need to create the .cer file, read on!

A simple way to create the required file is to import and export the certificate in and out of the Windows certificate store. This works because the export operation allows you to choose the export format.

The first step is to import the certificate into Windows:

1. Using a Windows computer, open the Microsoft Management Console by clicking the 'Start' button, selecting 'Run' and then running the command 'mmc.exe'.



2. In the Microsoft Management Console, select 'Add/Remove Snap-in...' from the 'File' menu.
3. Click 'Add...'.
4. Highlight the 'Certificates' snap-in from the list and click 'Add'.
5. Ensure that 'My user account' is selected and then click 'Finish'.
6. Click 'Close'.
7. Click 'OK'.
8. Expand the tree from 'Console Root' to 'Certificates - Current User' to 'Personal'.
9. Right-click 'Personal' and select 'Import...' from the 'All Tasks' menu.
10. When the 'Certificate Import Wizard' is displayed, click 'Next'.

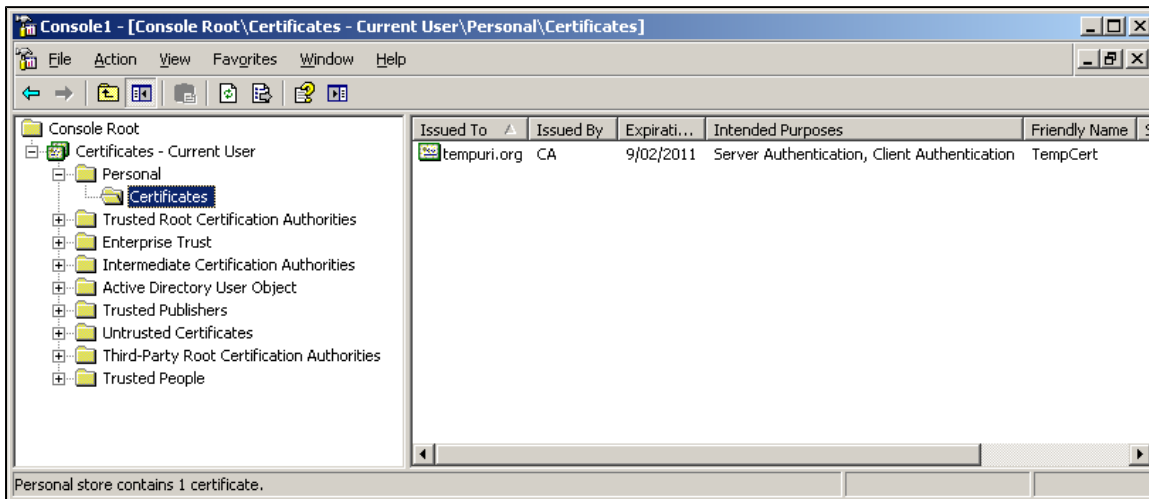
Screenshot: The certificate import wizard



11. Click '**Browse...**' and select the .pfx certificate file. (You may need to set the '**Files of type**' filter to '**Personal Information Exchange (.pfx, *.p12)***').
12. Click '**Next**'.
13. Enter the '**Password**' for the certificate.
14. Ensure that the '**Mark this key as exportable**' option is selected.
15. Click '**Next**'.
16. Click '**Next**'.
17. Click '**Finish**'.

At this point, your certificate should appear in the '**Personal**' folder of the 'Certificates' snap-in.

Screenshot: Personal certificates



Now you can export the certificate in the desired .cer format:

1. Right-click the certificate and select '**Export...**' from the '**All Tasks**' menu.
2. When the Certificate Export Wizard opens, click '**Next**'.
3. Ensure that the '**No, do not export the private key**' option is selected.
4. Click '**Next**'.
5. Ensure that the '**DER encoded binary X.509 (.CER)**' option is selected.
6. Click '**Next**'.
7. Enter a '**File name**' for the exported certificate (such as '{{}}C:\cert.cer').
8. Click '**Next**'.
9. Click '**Finish**'.

Step 1.2: Import the .cer File onto the Confluence Server

We have provided a batch script (see below) for Windows environments. If you are running Confluence on UNIX, please perform the import manually. The batch script uses the Java runtime's **keytool** command to import the certificate into the required location on the Confluence server. The script will add the certificate to the root Java Secure Sockets Extensions keystore, which is located in your Java Runtime Environment's (JRE's) `lib\security` directory with the name `jssecacerts`. This is the required location in order for the certificate to be trusted by Confluence.



Requirements

This script assumes the following about your environment:

- You are using a Confluence stand-alone installation running on the Sun JVM.
- Your `%JAVA_HOME%` environment variable has been set correctly.
- You have copied the `.cer` file created in step 1.1 [above](#) to the `C:` drive of your Confluence server.

Copy and execute this batch script (Windows) to add the certificate to the keystore:

.....

Step 2: Configure the Alternative URL in Confluence

The final step is to configure your Confluence server to communicate via the new URL you have set up.

- If you are installing the SharePoint Connector for the first time, please continue with the [next step of the installation procedure](#). In one of the later steps, you will configure the alternative URL in Confluence.
- If you have already installed and configured the Confluence plugins, please follow the instructions now to [configure the alternative URL in Confluence](#).

Installing and Configuring the Confluence Plugins for SP 2010

This page tells you how to install and configure the Confluence plugins that you need for the SharePoint Connector, to integrate with Microsoft SharePoint 2010.

On this page:

- [1. Install the Confluence Plugins](#)
- [2. Configure Confluence and the Plugins](#)
 - [Enabling Confluence Remote API](#)
 - [Configuring Confluence to Work with a SharePoint Site](#)
 - [Configuring an Alternative SharePoint URL for Confluence](#)
 - [Configuring Confluence to Share Search Results with SharePoint MOSS](#)
- [Editing an Existing SharePoint Site's Settings](#)
- [Next Step](#)

1. Install the Confluence Plugins

To install the plugins into Confluence:

Go to the Confluence '**Administration Console**'. To do this:

- Open the '**Browse**' menu and select '**Confluence Admin**'. The 'Administration Console' view will open.

Using Confluence earlier than 3.4

1. Click '**Plugin Repository**' in the 'Configuration' section of the left-hand navigation panel to open the 'Atlassian Plugin Repository' page.
 2. Scroll down to the row indicating '**The SharePoint Connector for Confluence**' and click '**Install**'. The Confluence plugin will be installed into Confluence.
 3. Scroll to the row indicating '**Permission Checker RPC Plugin**' and click '**Install**'. The Permission Checker RPC plugin will be installed into Confluence.
- This plugin is also known as the 'Confluence SOAP Permission Checker Plugin'.
4. Decide whether you will be able to use the SharePoint Connector's federated search feature. With the federated search, you can share search results between Confluence and SharePoint. It is available only if you have SharePoint MOSS 2007 or SharePoint Server 2010. If you want to use the federated search, you will need the Atlassian-supported OpenSearch plugin. Scroll to the row indicating '**OpenSearch Plugin**' and click '**Install**'. The OpenSearch plugin will be installed into Confluence.

Using Universal Plugin Manager, or using Confluence 3.4 or later

1. Click '**Plugins**' in the 'Configuration' section of the left-hand navigation panel to open the 'Universal Plugin Manager' page.
2. Click on the '**Install**' tab.
3. In the '**Search Plugin Exchange**' search box, enter 'Sharepoint Connector'.
4. Click on the search result to expand. Once expanded, click on '**Install Now**' button.
5. Repeat for '**Permission Checker RPC Plugin**'.
6. If you want to use the SharePoint Connector's federated search feature, you will need the Atlassian-supported OpenSearch plugin. Search for '**OpenSearch Plugin**' and repeat the procedure.

2. Configure Confluence and the Plugins

Once you have installed the required plugins into Confluence, you should then configure the plugins and your Confluence site to work and communicate successfully with a SharePoint site. Follow the instructions below.

Enabling Confluence Remote API

In order for your SharePoint site(s) to communicate with and retrieve content from Confluence, the **Remote API (XML-RPC & SOAP)** must be enabled in Confluence. Check whether the remote API is enabled and if not, enable it. See the instructions in the [Confluence administrator's guide](#).

Configuring Confluence to Work with a SharePoint Site

In this step, you will tell Confluence which SharePoint site(s) it can communicate with.

To configure Confluence to work with a SharePoint site:

1. Go to the Confluence '**Administration Console**'. To do this:
 - Open the '**Browse**' menu and select '**Confluence Admin**'. The 'Administration Console' view will open.
2. Click '**SharePoint Admin**' in the 'Administration' section of the left-hand navigation panel to open the 'SharePoint Integration Administration' screen. On this screen you can configure one or more SharePoint sites to work with your Confluence installation.

Screenshot: The site configuration section of the Confluence 'SharePoint Admin' page

SharePoint Integration Administration

Alias	SharePoint Site URL	Default Site	Login	
MySite	http://win-8d7e2ov0i6r/my		win-8d7e2ov0i6r\admin	- Edit -
QASP	http://win-8d7e2ov0i6r		win-8d7e2ov0i6r\admin	- Edit -

Please set these values correctly to provide access to your SharePoint site.

SharePoint Site Alias

SharePoint Site URL

Confluence Access URL Enabled ☒ No (Use Standard Access URL) ☐ Yes (Use Alternative Access URL)

User Name

Password:

☒ Make this SharePoint Site the default. This means its SharePoint Site Alias need not be specified when referencing SharePoint lists.

☐ Enable sp-list permission trimming - a user can only see a SharePoint list if they have permission to the list under the same username in SharePoint.

Confluence Permission Checker Plugin is installed.

Connection Test: **Success**

Examples: http://sharepoint-server or https://sharepoint-server:8080/sites/sitecollection1
[See documentation on SSL configuration.](#)

This option enables Confluence to access SharePoint using a different URL to users. This may be useful if SharePoint provides different authentication schemes at different URLs.

Example: ATlassian-SERV\Administrator (Note: Please be sure to use a backslash).

3. Enter the appropriate details into the following fields:


Table: SharePoint Site Configuration Fields


|| Field || Description ||

SharePoint Site Alias	Enter a simple name that identifies the SharePoint site easily in Confluence. SharePoint-related Confluence macros use this name as a parameter value to identify the SharePoint site on which to run their queries. Each SharePoint alias must be unique. However, do not modify this field when editing a pre-configured SharePoint site.
SharePoint Site URL	Enter the base URL of the SharePoint site, for example, [http://www.example-sharepoint-server.com]\\ \ \ \ .
Confluence Access URL Enabled	You can choose to configure an alternative SharePoint URL for Confluence to use when accessing SharePoint. See the details below.
User Name	The Windows user account that Confluence will use to access the SharePoint site. Note that this user must be a <i>SharePoint site collection administrator</i> . The user name <i>must</i> follow the syntax SERVERNAME\username, where: <ul style="list-style-type: none"> SERVERNAME is the name of the Windows domain on which the SharePoint site can be accessed. Otherwise, this is the name of the computer hosting SharePoint. username is the username of the Windows user account used to access the SharePoint site.
Password	The password associated with the Windows user account.
Make this SharePoint Site the default.	Selecting this option makes any Confluence SharePoint macros that do not reference a SharePoint Site Alias, query this SharePoint site. If this option is selected, a appears in the 'Default Site' field of the list of configured SharePoint sites (at the top of the SharePoint Admin page).

Enable sp-list permission trimming	Selecting this option filters the SharePoint List macro results to display only content that the user has permission to access in SharePoint.
------------------------------------	---

- Click the **'Test Connection'** button to test that the connection to the SharePoint site is correct.

If the connection was successful, you will see the message  **Connection Test: Success.**

If the connection was not successful, you will see the message  **Connection Test: Server unreachable.** If you see this message, please ensure that your SharePoint site settings are correct, as described in the table above.

- Click **'Update SharePoint Settings'** to save the configuration settings for your SharePoint site.

Configuring an Alternative SharePoint URL for Confluence

The **'Confluence Access URL Enabled'** option on the 'SharePoint Admin' screen allows you to set up a special URL for Confluence to use when accessing SharePoint. There are two choices:

- 'Use Standard Access URL'** – This is the default value. If you choose this option Confluence will query the SharePoint site via the 'SharePoint Site URL' configured above.
- 'Use Alternative Access URL'** – If you choose this option, the **'Confluence Access URL'** field appears on the screen. Enter an alternative URL. Confluence will query the SharePoint site via this URL instead of the 'SharePoint Site URL'.

The alternative access URL allows you to resolve problems where the SharePoint installation uses an authentication protocol not supported by Confluence, such as [NTLMv2](#) or [Kerberos](#). You can configure SharePoint to run on a separate port that bypasses the unsupported authentication protocol, and then allow Confluence to communicate with SharePoint via this alternative URL. See the [recommended configuration for securing Confluence access to SharePoint](#).

To configure Confluence to access SharePoint via an alternative URL:

- Set up an alternative URL in SharePoint. (See the [recommended configuration for securing Confluence access to SharePoint](#).)
- Select **'Use Alternative Access URL'** on the Confluence 'SharePoint Admin' screen shown above.



Which URL will the Confluence macros use?

Confluence's SharePoint macros will query the SharePoint site via the alternative access URL. However, any links returned by these macros that lead back to the SharePoint site will query the standard access URL.



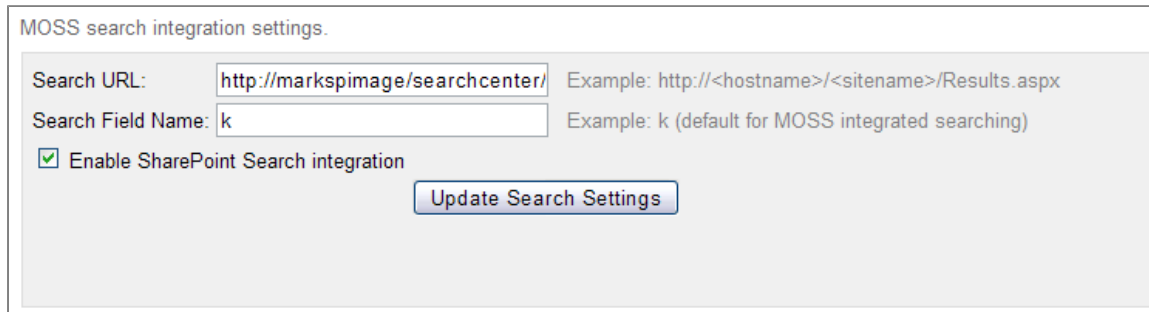
The alternative access URL must be configured externally, as a separate network configuration.

In practice, an alternative access URL would be used in situations where Confluence and SharePoint are hosted in the same private network, either behind a firewall or on the same VPN.

Configuring Confluence to Share Search Results with SharePoint MOSS


If you have a Microsoft Office SharePoint Server (MOSS) instead of just SharePoint WSS, you can configure Confluence to share search results with the MOSS server. This will allow users to search content in both Confluence and SharePoint from Confluence's search features.

Screenshot: The MOSS search integration section of the Confluence 'SharePoint Admin' page

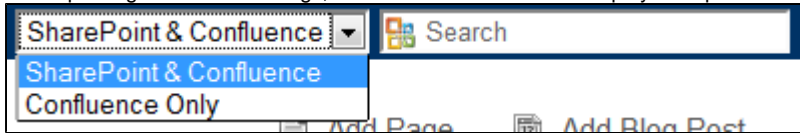


To configure Confluence to share search results with a MOSS server:

- Enter the MOSS server's Search URL into the **'Search URL'** field. This usually has the format `[http://www.example-sharepoint-server.com/searchcenter/Pages/Results.aspx]`.
- Enter the MOSS Search URL's search parameter into the **'Search Field Name'**. This is usually the letter `k` only.
- Click the **'Update Search Settings'** button.

 You will also need to configure the SharePoint side of things. You will come to this step later, as described in [Configuring the SharePoint Federated Search on SP 2007](#).

After updating the search settings, the Confluence theme will display a drop-down menu next to the Confluence search box, looking like this:



The drop-down menu offers two options:

- 'SharePoint & Confluence' – If you select this option when searching for content via the Confluence search, the search results page will open in SharePoint and will show results from both SharePoint and Confluence.
- 'Confluence Only' – If you select this option when searching for content via the Confluence search, the search results page will open in Confluence and will show results from Confluence only.

Editing an Existing SharePoint Site's Settings

This section describes how to edit the settings for a SharePoint site that has already been configured in Confluence.

To edit the existing configuration settings of a SharePoint site in Confluence:


1. Go to the Confluence '**Administration Console**'. To do this:
 - Open the '**Browse**' menu and select '**Confluence Admin**'. The 'Administration Console' view will open.
2. Click '**SharePoint Admin**' in the 'Administration' section of the left-hand navigation panel.
3. In the top list of already-configured SharePoint sites, click the '**- Edit -**' link next to the SharePoint site that you want to update. The fields below the list will be populated with the current settings for that SharePoint site.
4. Edit the field details according to the table above, to the updated settings.
5. If necessary, update the additional options as described above.
6. Test that the connection to the SharePoint site is correct by clicking the '**Test Connection**' button. A message will be displayed, indicating whether or not the connection was successful.
7. Click '**Update SharePoint Settings**' to save the updated configuration settings for your SharePoint site.



Do not change the SharePoint site alias

If you only intend to edit an existing SharePoint site's configuration, do not change the 'SharePoint Site Alias' field. If you do change this value, Confluence adds these settings as a new entry in the list of configured SharePoint sites.

Screenshot: Example List of Configured SharePoint Sites

Alias	SharePoint Site URL	Default Site	Login	
Another	http://another-server		ANOTHER\Administrator	- Edit -
SharePoint	http://sharepoint-server		SHAREPOINTSERV\Administrator	- Edit -

Next Step

To continue with the installation of the SharePoint Connector, please [configure the access to Confluence](#).

Configuring Access to Confluence for SP 2010

This section describes the methods which may be used to **configure access to Confluence** for the SharePoint Connector, when using SharePoint 2010. You should complete one of the supported configuration guides before proceeding further with the SharePoint Connector installation. If you have not already seen our guide to [planning your environment](#), please refer to it now for information that will help you select the best configuration for your environment.

Please follow one of these configuration guides:

- [Access Confluence using Integrated Windows Authentication via IIS with SP 2010](#)
- [Access Confluence using Integrated Windows Authentication via Jespa with SP 2010](#)
- [Access Confluence using Standard Authentication with SP 2010](#)
- [Access Confluence using Standard Authentication with Secure Store Service on SP 2010](#)

Next Step

To continue with the installation of the SharePoint Connector, please [install and configure the SharePoint feature](#).

Access Confluence using Integrated Windows Authentication via IIS with SP 2010

This page is part of the installation guide for the **Confluence SharePoint Connector**. It tells you how to configure access to Confluence using Integrated Windows Authentication via IIS with SharePoint 2010.

On this page:

- [Overview](#)
- [Caveats](#)
 - [Supported Platforms](#)
 - [Additional Dependencies](#)
 - [Custom Seraph Authenticator](#)
 - [Custom ISAPI Filter](#)
 - [Anonymous Access Disabled](#)
 - [Known issues](#)
- [Installation Instructions](#)
 - [Step 1. Configure Confluence for LDAP User Management](#)
 - [Step 2. Configure IIS](#)
 - [Step 3. Configure Confluence for Integrated Windows Authentication](#)
 - [Step 3.1: Set Confluence Path](#)
 - [Step 3.2: Add AJP Connector](#)
 - [Step 3.3: Add Custom Authenticator](#)
 - [Step 3.4: Modify Base URL](#)
 - [Step 4. Set Client Browser Options](#)
- [Next Step](#)

Overview

In this configuration, both SharePoint and client browsers are authenticated against Confluence using Windows authentication provided by a Microsoft Internet Information Services (IIS) server. IIS proxies the pre-authenticated requests through to Confluence and then returns the content to the requester. Confluence and IIS communicate using Apache JServ Protocol (AJP).

Use this Configuration when...

- You want to enable 'pass-through authentication' for your users logged in to a Windows domain.
- All users who access Confluence are members of an Active Directory domain.
- Confluence is running on Windows Server, or you are able to set up Windows Server to act as a proxy for Confluence.

If you have not already seen our guide to [planning your environment](#), you can refer to it for information that will help you select the best configuration for your environment.

Caveats

Supported Platforms

Due to the complex nature of this configuration, Atlassian is only able to provide support if your configuration satisfies these additional conditions:

- Confluence must be installed as a stand-alone Tomcat application server.
- IIS and Confluence must be hosted on the same logical server (unless Confluence is running on a non-Windows system).
- The only supported operating systems for this configuration are Windows Server 2003 and Windows Server 2008.
- The server must be a member of the same Active Directory domain that contains the user records that will be authenticated.
- Confluence must be configured to use LDAP integration to Active Directory for user management.

Additional Dependencies

Using this configuration adds a number of additional dependencies to Confluence, which you should review.

Custom Seraph Authenticator

This configuration requires the use of a specialised Seraph authenticator for Confluence. If you are already using a different custom Seraph authenticator, you may not be able to use this configuration. In this situation, you must either choose a different configuration for the SharePoint Connector or consider developing a new custom Seraph authenticator that aggregates the functionality of both.



No support for custom authenticators

Please note that we are unable to provide support for any custom authenticators not written or explicitly supported by Atlassian.

Custom ISAPI Filter

This configuration requires the use of a custom ISAPI filter for IIS that can communicate using AJP. Atlassian will only support the use of the open source Tomcat Connector provided by the [Apache Tomcat project](#).

**Limited support for third-party software**

Please note that Atlassian is unable to provide in-depth support for problems encountered with the Tomcat Connector, as this software is written and maintained by the [Apache Software Foundation](#). Atlassian will assist with ensuring the correct configuration values are applied and capturing diagnostic information, but any issues encountered with the Tomcat Connector must be raised through the appropriate channels with the [Apache Tomcat project](#) or with another organisation that provides commercial support for Tomcat.

Anonymous Access Disabled

Due to limitations with the custom Seraph authenticator that Confluence requires for this configuration, it is not possible to set up anonymous access for Confluence when using this configuration.

Atlassian is currently reviewing the suitability of using the third-party [NTLM Authenticator for Confluence](#) instead.

Known issues

These are some reported problems with this configuration:

- The user is not able to explicitly log out. Even when they select the logout action, they remain logged-in.
- If you log in using NTLM authentication as a user that does not exist in the AD repository, you will not see the personal menu in Confluence's top navigation bar.
- You cannot fall back to using forms-based authentication or anonymous authentication.

Installation Instructions**Step 1. Configure Confluence for LDAP User Management**

If you have already configured Confluence to connect to your Active Directory domain, then skip ahead to the next step.

Set up your Confluence server to synchronise its user repository with your Windows Active Directory domain. See the Confluence documentation on [LDAP user management](#).

Step 2. Configure IIS

This and following steps guide you through the configuration required to use IIS as an NTLM authenticator for Confluence. NTLM is an authentication format developed by Microsoft. While some third-party implementations are available, IIS provides the most robust and full-featured NTLM authentication support.

Summary of this configuration:

- It places the Tomcat application server running Confluence behind an IIS website configured for Integrated Windows Authentication.
- IIS is then configured with a custom ISAPI handler that communicates directly with the Tomcat server using Apache JServ Protocol to serve the Confluence content back to the user.

Please follow the guide below that matches the version of your Windows Server:

- Windows Server 2003: [Configuring Tomcat-Connector for IIS 6.0 \(Windows Server 2003\)](#)
- Windows Server 2008: [Configuring Tomcat-Connector for IIS 7.0 \(Windows Server 2008\)](#)

Step 3. Configure Confluence for Integrated Windows Authentication

This section of the guide describes the steps necessary to configure Confluence to co-operate with the IIS Web Server.

Throughout this section, '%confluence_install%' refers to your [Confluence installation directory](#).

Step 3.1: Set Confluence Path

This step is only necessary if your IIS instance is already hosting other websites and you want to host Confluence underneath an existing site (for example, if your corporate intranet is hosted at <http://intranet.company.com> and you want to host Confluence at <http://intranet.company.com/confluence>).

1. Edit the %confluence_install%\conf\server.xml file.
2. Find the **Context** element in the file, and then change the **path** value to '/confluence'.
The line should look something like this:
.....
3. Save your changes and close the file.
4. Restart Confluence and verify that it is now accessible from the new path, such as <http://localhost:8080/confluence>.

Step 3.2: Add AJP Connector

Now you will change Tomcat's configuration, replacing the standard Coyote HTTP connector (which allows Tomcat to send and receive HTTP traffic) with a custom AJP connector (which allows Tomcat to communicate using Apache JServ Protocol).

1. Edit the `%confluence_install%\conf\server.xml` file.
2. Locate the **Connector** element and comment it out entirely.
3. Add a new **Connector** element that looks like the one below. The values that must match exactly are **address**, **protocol** and **tomcatAuthentication**:



If IIS is **not** located on the same server as Confluence, then you should not enter the **address** value at all.

4. Ensure that your `server.xml` file now contains only a single Connector definition.
5. Save your changes and close the file.
6. Restart Confluence and ensure that the server initialises successfully.

Step 3.3: Add Custom Authenticator

By default, Confluence will not understand the pre-authenticated requests that come through via the IIS Web Site. In order to allow this authentication information to pass through, you must modify the authenticator module used by Confluence.

1. Download the [customauth-0.4.jar](#) file attached to this page and place it in your `%confluence_install%\confluence\WEB-INF\lib` directory.
2. Edit the `%confluence_install%\WEB-INF\classes\seraph-config.xml` file.
3. Locate the **authenticator** element and comment it out entirely.
4. Add a new **authenticator** element that looks like this:

5. Save your changes and close the file.
6. Restart Confluence and ensure that the server initialises successfully.

Step 3.4: Modify Base URL

The final step in configuring Confluence is to modify the Server Base URL to point to the IIS web site, rather than directly to Confluence. This ensures that any hyperlinks generated within Confluence pages will direct users through the IIS website. For example, if your Tomcat server runs Confluence on <http://intranet.company.com:8080/confluence> and the IIS web site runs on <http://intranet.company.com>, then the Confluence Base URL needs to be changed to <http://intranet.company.com/confluence>.

See the [Confluence documentation](#) for instructions on modifying the Base URL.

Step 4. Set Client Browser Options

In order for users to be automatically logged in to Confluence without being prompted for their username and password, the browser must be correctly configured for pass-through authentication.

Please instruct all users to ensure that the [recommended browser settings](#) are applied.

Next Step

To continue with the installation of the SharePoint Connector, please [install and configure the SharePoint feature](#).

Access Confluence using Integrated Windows Authentication via Jespa with SP 2010

This page is part of the installation guide for the **Confluence SharePoint Connector**. It tells you how to configure access to Confluence using Integrated Windows Authentication via Jespa, with SharePoint 2010.

On this page:

- [Overview](#)
- [Caveats](#)
 - [Supported Platforms](#)
 - [Anonymous Access](#)
 - [Additional Dependencies](#)
- [About Jespa](#)
 - [Authentication Methods](#)
 - [Cost](#)
- [Installation Instructions](#)
- [Next Step](#)

Overview

In this configuration both SharePoint and client browsers are authenticated against Confluence using Windows authentication provided by [Jespa](#), a third-party implementation written in Java.

Use this Configuration when...

- Your users are logged in to a Windows domain and access Confluence using a web browser that supports automatic pass through of

- Windows credentials. (See the [recommended browser settings](#).)
- You want your users to experience a seamless single sign-on experience when accessing Confluence.
- Your Confluence installation is not running on a Windows server and you do not want to provision a new Windows server to provide an IIS proxy for Confluence (see [Integrated Windows Authentication via IIS](#)).

If you have not already seen our guide to [planning your environment](#), you can refer to it for information that will help you select the best configuration for your environment.

Caveats

Supported Platforms

Due to the complex nature of this configuration and its reliance on third-party products, Atlassian is only able to offer support if your configuration matches these specifications:

- Confluence is installed as a stand-alone Tomcat application server.
- Confluence is configured to use LDAP integration to Active Directory for user management.

Anonymous Access



Anonymous access is not supported

You will not be able to get anonymous access for Confluence working when using this configuration.

When configuring Confluence with Jespa (as described in our [guide](#)) you will not be able to set up a satisfactory anonymous access mechanism, due to the requirements of the custom authenticator and the Confluence Base URL.

Atlassian is currently reviewing the suitability of using the third-party [NTLM Authenticator for Confluence](#) instead.

Additional Dependencies

Please consider the following additional dependencies:

- The configuration requires a custom Seraph authenticator for Confluence. If you are already using a custom Seraph authenticator, you may not be able to use this configuration.
- The configuration requires a third-party library that implements the Windows authentication protocols. See the section on Jespa below for details of this dependency.

About Jespa

Jespa is a Java software library that provides advanced integration between Microsoft Active Directory and Java applications such as Confluence. For more information, visit the [Jespa website](#).

Authentication Methods

Jespa supports the following Windows authentication methods:

- LM
- NTLMv1
- NTLM2 Session Security
- LMv2
- NTLMv2

Cost

Jespa is a commercial software package that has a licensing cost associated with its use. Atlassian does not have a redistribution agreement with IOPlax, the suppliers of Jespa. If you wish to use Jespa, you must arrange a purchase agreement with IOPlax directly.

Purchasing information can be found on the [IOPlax website](#).

Installation Instructions

Follow the instructions on [configuring Confluence to use Jespa for NTLM authentication](#).

Next Step

To continue with the installation of the SharePoint Connector, please [install and configure the SharePoint feature](#).

Access Confluence using Standard Authentication with SP 2010

This page is part of the installation guide for the **Confluence SharePoint Connector**. It tells you how to configure access to Confluence using standard Confluence authentication. These instructions apply to the connector for SharePoint 2010.

On this page:

- [Overview](#)

- [Caveats](#)
 - [User Credentials Must Match](#)
- [Installation Instructions](#)
- [Next Step](#)

Overview

In this configuration, both SharePoint and all client browsers are authenticated using Confluence's built in authentication module, which is a style of forms-based authentication.

Use this configuration when...

- You have no specific authentication requirements for your environment.
- You do not need your users to have pass-through authentication to Confluence via their desktop logins.

If you have not already seen our guide to [planning your environment](#), you can refer to it for information that will help you select the best configuration for your environment.

Caveats

User Credentials Must Match

In order for the SharePoint Connector to seamlessly extract content from Confluence to SharePoint (and vice versa), Confluence's user repository must contain **usernames and passwords that exactly match** the usernames and passwords being used for SharePoint Authentication.

For small installations, you may be happy to maintain the standard Confluence user repository manually.

For larger installations, and if your SharePoint server authenticates users with Active Directory, you may consider synchronising the Confluence user repository with Active Directory.

Installation Instructions

No additional installation steps are necessary beyond following the standard installation guide for Confluence and the SharePoint Connector.

If you wish to synchronise the Confluence user repository with Active Directory, then read the Confluence documentation on [LDAP user management](#).

Next Step

To continue with the installation of the SharePoint Connector, please [install and configure the SharePoint feature](#).

Access Confluence using Standard Authentication with Secure Store Service on SP 2010

This page is part of the installation guide for the **Confluence SharePoint Connector**. It tells you how to configure access to Confluence using the standard Confluence authentication with Microsoft Secure Store Service. These instructions apply to the connector for SharePoint 2010.

On this page:

- [Overview](#)
- [Caveats](#)
 - [Caching of Username and Password](#)
 - [Hardening the Secure Store Service](#)
- [Installation Instructions](#)
 - [Step 1. Ensure that the Secure Store Service is running](#)
 - [Step 1.1. Start a New Instance of the Secure Store Service](#)
 - [Step 2. Configure a Secure Store Application for Confluence](#)
 - [Step 2.1. Generate New Key](#)
 - [Step 2.2 Create New Application](#)
- [Next Step](#)

Overview

In this configuration, SharePoint and all client browsers are authenticated using Confluence's built-in authentication module, which is a style of Forms-based Authentication. The Microsoft Secure Store Service acts as a 'man-in-the-middle', performing mappings between Confluence and SharePoint user accounts.

Use this Configuration when...

- You have no specific authentication requirements for your environment. You do not need your users to have pass-through authentication to Confluence via their desktop logins.
- The usernames and passwords in your Confluence user repository do not exactly match the usernames and passwords in your SharePoint user repository (such as Active Directory).
- You are not able to configure Confluence to synchronise its user repository with Active Directory (see [Confluence LDAP user management](#)).

If you have not already seen our guide to [planning your environment](#), you can refer to it for information that will help you select the best

configuration for your environment.

Caveats

Caching of Username and Password

The Microsoft Secure Store Service caches users' credentials for external applications such as Confluence. The first time a user accesses Confluence, they will be prompted to enter their username and password. Subsequent logins to Confluence will use the cached credentials.

Hardening the Secure Store Service

The Microsoft TechNet article on [Planning the Secure Store Service](#) has a number of guidelines on how to run the service in a manner that is as secure as possible. You should read through these guidelines and apply them to your environment, where practical.


Installation Instructions

After installing the SharePoint Connector, follow the instructions below to configure the Secure Store Service to work with Confluence.

Step 1. Ensure that the Secure Store Service is running

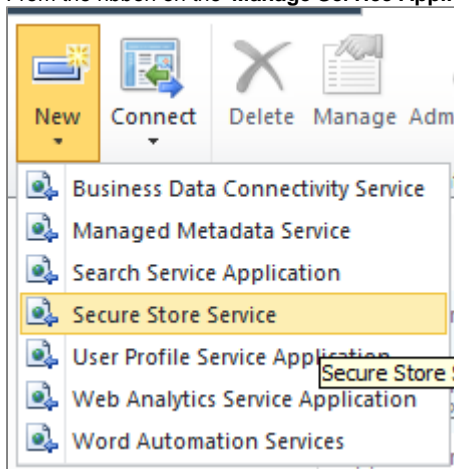
By default, the Secure Store Service is already set up and started on new installations of SharePoint Server 2010. This step of the guide just ensures that the Secure Store Service is running in your environment.

1. Log in to your **SharePoint Central Administration** site with a user account that has farm administration privileges.
2. Click **'Manage Service Applications'**.
3. In the table of service applications, locate the **'Secure Store Service Application'**.
4. Ensure that the **'Status'** of the service application is set to **'Started'**.

 If the Secure Store Service is not started, or is not listed in the table, then follow the instructions below to configure a new instance of the Secure Store Service. Otherwise, skip to [step 2](#).

Step 1.1. Start a New Instance of the Secure Store Service

1. From the ribbon on the **'Manage Service Applications'** page, click **'New'** and select **'Secure Store Service'**.



2. The **'Create New Service Store Service Application'** popup window appears. Enter the details of the new service application. The settings should satisfy the recommended guidelines for the Secure Store Service (see the corresponding [TechNet article](#)).
3. Click **'OK'**.
4. Once the new Secure Store Service Application has been created successfully, click **'OK'** again.

Step 2. Configure a Secure Store Application for Confluence

The next step involves creating a new target 'application' in the Secure Store database that will hold the credentials for your Confluence server.

1. Click the name of the Secure Store Service Application (see step 1 [above](#)) in the **'Manage Service Applications'** table.

Step 2.1. Generate New Key



You only need to perform this step if, upon loading the Secure Store Service Application page, you receive the following error:



Before creating a new Secure Store Target Application, you must first generate a new key for this Secure Store Service Application from the ribbon.

1. In the ribbon at the top of the page, click '**Generate New Key**'.
2. The '**Generate New Key**' popup window appears. Enter a new passphrase for encrypting the credentials in the Secure Store Service.
3. Click '**OK**'.

Step 2.2 Create New Application

1. In the ribbon at the top of the page, click '**New**'.
2. Set the '**Target Application ID**' to 'Confluence'.
3. Enter a '**Display Name**' and '**Contact E-mail**' for the application.
4. Set the '**Target Application Type**' to 'Individual'.
5. Ensure that the '**Use default page**' option under '**Target Application Page URL**' is selected.
6. Set the '**Ticket Timeout**' to 2 (minutes).
7. Click '**Next**'.
8. Create two fields for the application, matching the example shown below:

Field Name	Field Type	Masked	Delete
Confluence User Name	User Name	<input type="checkbox"/>	X
Confluence Password	Password	<input checked="" type="checkbox"/>	X

Important: The field names and field types cannot be edited later.

9. Click '**Next**'.
10. Add the current user to the '**Target Application Administrators**' group.
11. Click '**OK**'.

Next Step

To continue with the installation of the SharePoint Connector, please [install and configure the SharePoint feature](#). When [configuring the SharePoint web part](#) make sure that you select 'Access Confluence with the Secure Store Service' as your authentication method.

Installing and Configuring the SharePoint Feature on SP 2010

This page tells you how to install and configure the SharePoint feature, that is, the SharePoint component of the Confluence SharePoint Connector. This component provides the Confluence web parts on the computer running SharePoint. These instructions are for SharePoint 2010.

On this page:

- [1. Install the SharePoint Component](#)
- [2. Configure the Confluence Settings for the SharePoint Sites](#)

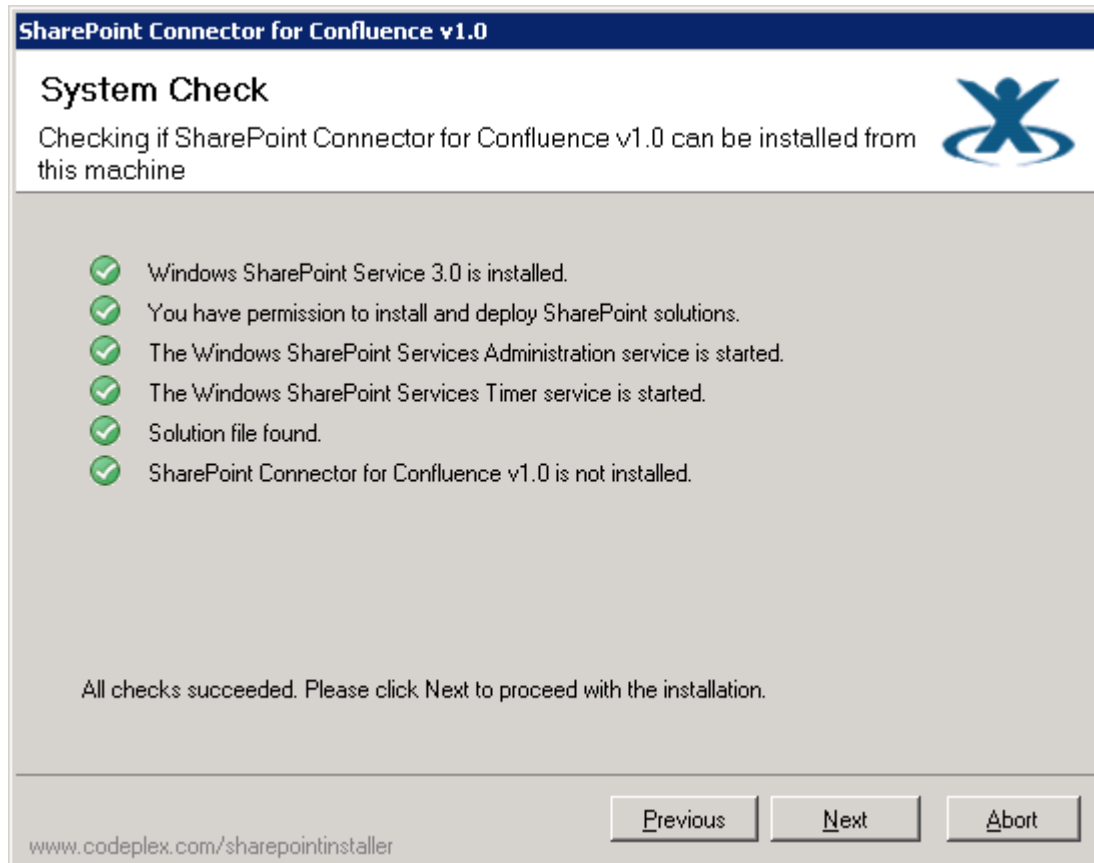
1. Install the SharePoint Component

To install the SharePoint component:


1. Download the SharePoint component from the [SharePoint Connector download centre](#).
2. Extract the contents of the downloaded SharePointConnector zip file and open the 'SharePoint Installer' directory.
3. Run the file in this directory named Setup_WebParts.exe. This starts the installation wizard for the SharePoint web parts.

All files in the 'SharePoint Installer' directory must remain intact for the installation of the SharePoint web parts to succeed.
4. After the welcome page loads, click the '**Next**' button to start the installation process.
5. The SharePoint web part installer performs a 'System Check' to ensure that all pre-installation and configuration requirements have been met.

[Screenshot: SharePoint Web Part Installer - 'System Check' Step](#)




Click **'Next'** to proceed with the installation wizard. If, however, one or more of the requirements checks fails, you must address those requirements before proceeding.

 The 'Windows SharePoint Services Administration' service in Windows may be stopped by default and if so, the third item in this check list will fail.

To resolve this issue:

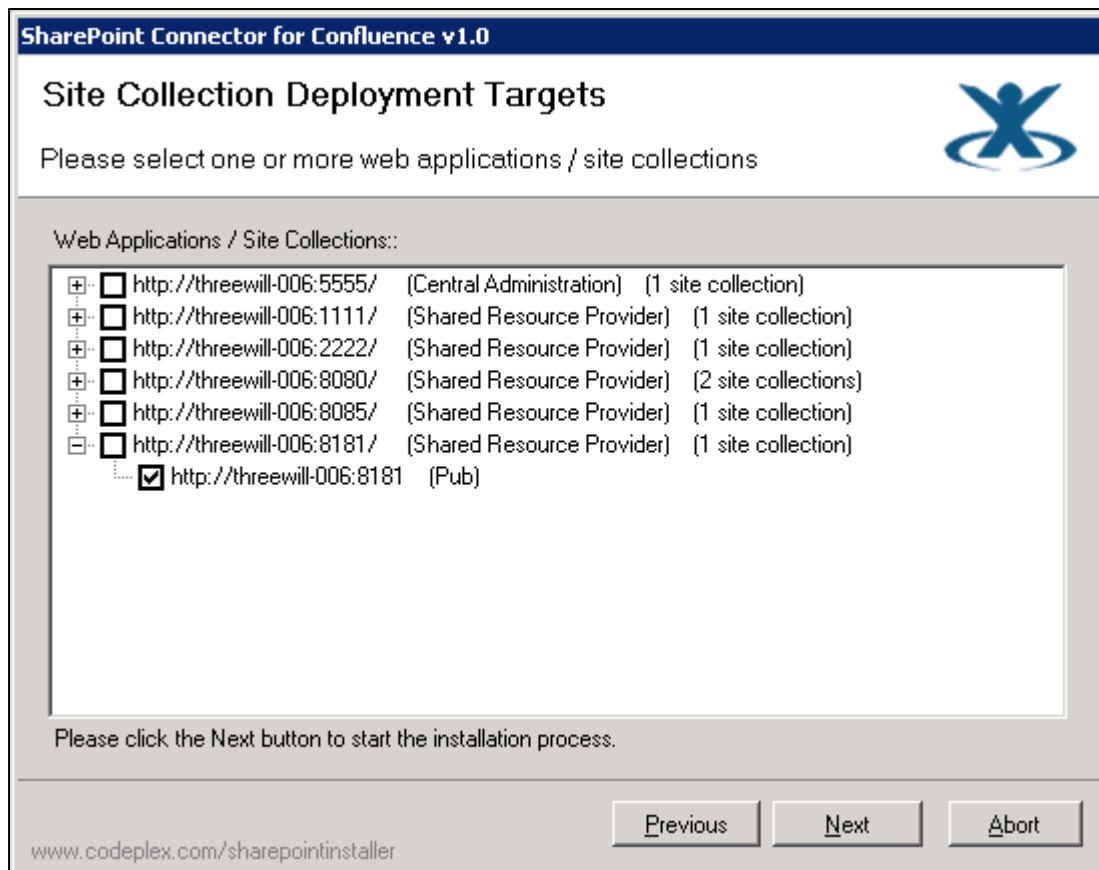
- In Windows, go to **Start -> All Programs -> Administrative Tools** and select **'Component Services (or Services)'**.
- In the Component Services console, select **'Services (Local)'** then scroll down to the **'Windows SharePoint Services Administration'** option and select it.
- Right-click this option and select **'Start'** from the popup menu.
- Stop and restart the SharePoint web part installation from step 2 above.

- The Atlassian End User license agreement is displayed. If you choose to continue, you must accept the license agreement by selecting the check box, then click the **'Next'** button to continue.
- In the 'Site Collection Deployment Targets' step, select the SharePoint site collections within your SharePoint installation, to deploy the Confluence SharePoint web part. This web part permits Confluence integration with the selected SharePoint site collections.

 Typically, the Confluence SharePoint web part is deployed to one or more SharePoint site collections within a SharePoint installation. The Confluence SharePoint web part is usually not deployed to the 'Central Administration' or 'Shared Resource Providers'/'Shared Service Providers'.

 All selected site collections in your SharePoint installation must be online before proceeding.

Screenshot: SharePoint Web Part Installer - 'Choose SharePoint Site Collections' Step



After selecting one or more Sharepoint site collections / web applications, click the **'Next'** button.

8. The installation process starts, deploying the Confluence SharePoint web part to the chosen SharePoint site collections.

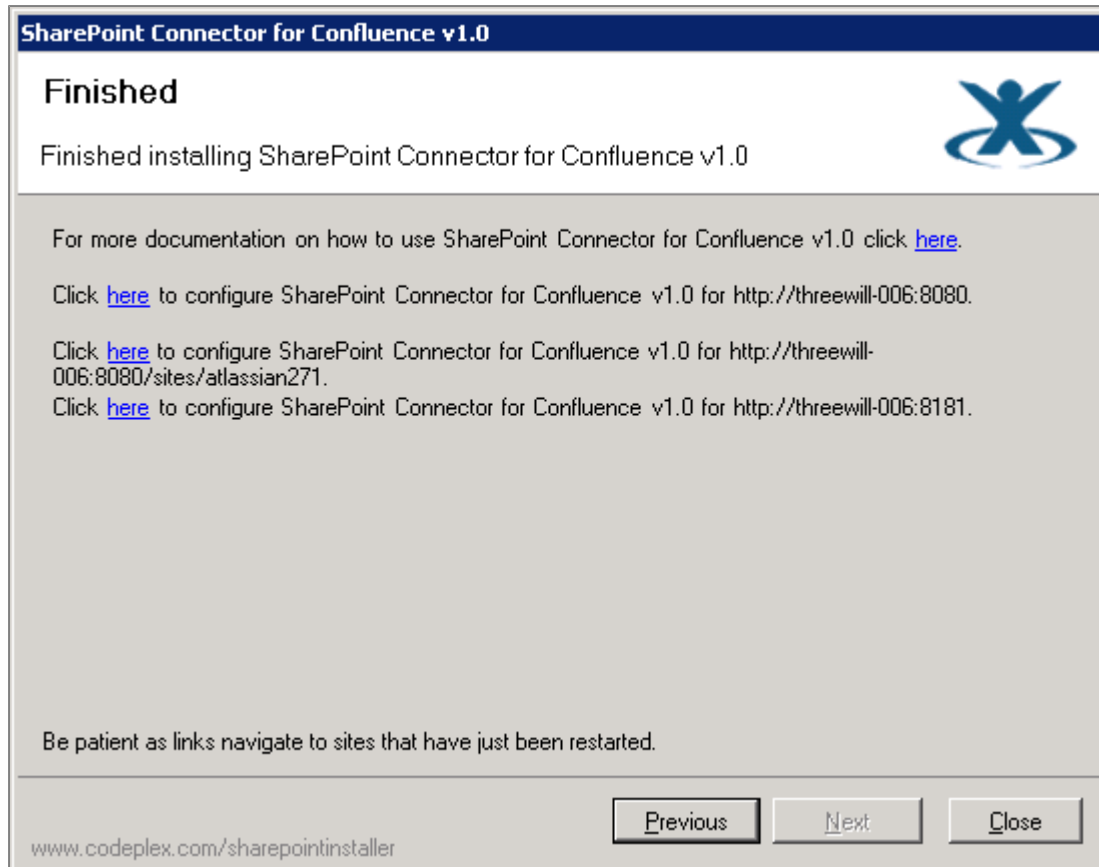
After the installation process is complete, click the **'Next'** button.

9. The **'Installation Successfully Completed'** step of the installation wizard is displayed. This window shows the SharePoint site collections that now have the Confluence SharePoint web parts. Click **'Next'** to continue.
10. The **'Finished'** step of the installation wizard is displayed. This window provides one or more configuration links. Each link points to the Confluence settings page of a SharePoint site with its newly installed Confluence SharePoint web part. Click each of these configuration links in turn to define how the SharePoint sites will connect to Confluence. See [Configuring the SharePoint Web Part on SP 2010](#).



When you click the links in this window, it may take some time for the configuration screens to appear because the SharePoint sites may require time to restart.

Screenshot: SharePoint Web Part Installer - 'Finished' Step



2. Configure the Confluence Settings for the SharePoint Sites

1. Configure the Confluence settings for each SharePoint site collection to which the SharePoint web part was deployed. You can do this by clicking the links on the 'Finished' screen of the installation wizard, as described above, or by navigating to the settings page yourself. See [Configuring the SharePoint Web Part on SP 2010](#) for full details.
2. Configure the SharePoint Federated Search, if required. See [Configuring the SharePoint Federated Search on SP 2010](#).


Configuring the SharePoint Web Part on SP 2010

This page tells you how to configure the Confluence settings for a SharePoint site, in SharePoint. These instructions apply to the connector for SharePoint 2010.

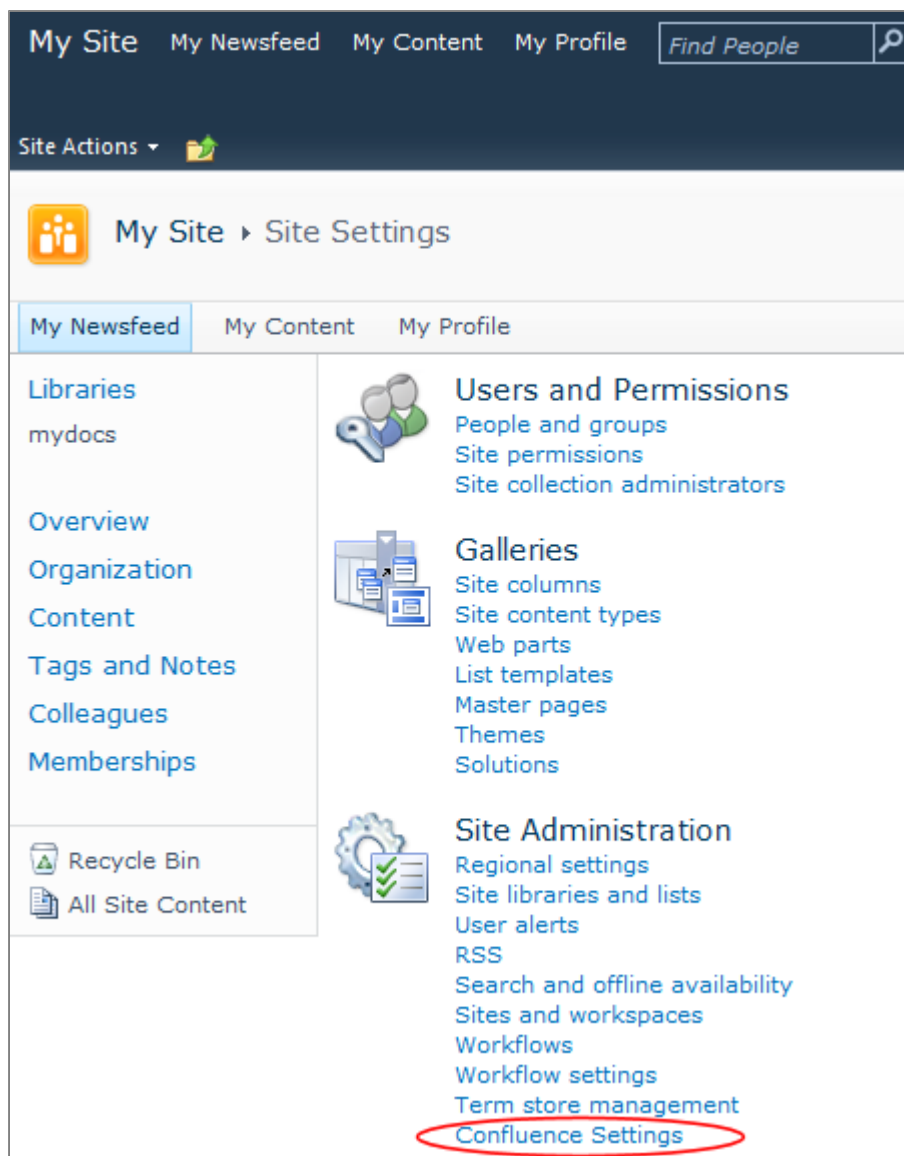
On this page:

- [Configuring the Confluence Administrative Settings for a SharePoint Site.](#)

Configuring the Confluence Administrative Settings for a SharePoint Site.

1. Open your web browser and use one of the following methods to open the Confluence settings page of the appropriate SharePoint site collection:
 - Navigate to the top level site within the site collection, select '**Site Actions**' (at the top left) -> '**Site Settings**' -> '**Confluence Settings**'.
-  The 'Confluence Settings' option is available only if the Confluence SharePoint web part was deployed to that SharePoint site.

Screenshot: SharePoint Site Settings, including 'Confluence Settings' option



- Or enter the URL for this page directly, using the format:
http://<sharepoint-site-collection>/_layouts/Atlassian/ConfluenceSettings.aspx
- Or use the final step of the web part installer wizard which provides direct links to these pages. For more information, please refer to the instructions on installing the SharePoint feature.

2. The Confluence administration screen appears:

Screenshot: Confluence Administrative Settings in SharePoint

3. Enter the base URL of the Confluence site in the '**Confluence Site**' field.
4. Under '**Authentication Selection**', choose the method by which SharePoint will access the Confluence site. See our [planning guide](#) for help with the authentication options.
 - If you choose '**Access Confluence with a single master account**':
 - Specify the Confluence **username** that SharePoint will use to access Confluence and enter the password recognised by Confluence for that username. This username must have full *Confluence site administration permissions*.
 - Optionally, you can also choose to customise the format of the username used to authenticate against Confluence. Select '**Customise the permission checking format**'. The '**User Name Format**' field will appear. Enter a format, such as this:


```
{domain} \ {username}
```

This example will pass the domain as well as the username when authenticating a user to Confluence. This is useful if you have configured Confluence to connect to multiple Active Directory domains and you therefore need to distinguish between two users with the same username in different domains.
 - Optionally, you can also choose to set the format of the username used to authenticate against Confluence to be the SharePoint user's configured Active Directory email address. To do this, select the '**Authenticate with Confluence using email**' field. This is useful if your users log in to Confluence with their email address, rather than their Active Directory username.
 - If you choose '**Access Confluence with the Microsoft Single Sign-On (SSO) Service**':
 - Select the Confluence SSO application in the dropdown box. This is the application that you have already set up when configuring [access to Confluence via the Microsoft SSO service](#).
5. If your Confluence site is especially large, and your users report problems while waiting for the Confluence web parts to load, you can optionally choose to increase the timeout value for retrieving content from Confluence. The default is 100 seconds, but you can increase this to a longer timeout if desired. To do this, enter a new numerical value in the '**Web Service Timeout**' field.
6. Click the '**Test Confluence Configuration**' button to test your configuration settings.
7. Click '**OK**' to save your changes.

**Settings are inherited by child SharePoint sites**

The Confluence settings are automatically inherited by any SharePoint sub-sites. If no Confluence settings have been configured for a SharePoint sub-site, the parent SharePoint site's Confluence settings apply. However, any Confluence settings configured for a sub-site will override the parent site's Confluence settings.

Configuring the SharePoint Federated Search on SP 2010

The Confluence SharePoint Connector provides a federated search, allowing SharePoint to issue search requests to Confluence and display the results it gets back from Confluence. Federated searches use Confluence's own search engine to retrieve up-to-date and relevant results. This guide is for SharePoint 2010

On this page:

- [Requirements](#)
- [SharePoint Configuration](#)
 - [Step 1. Configure the Federated Search Location](#)
 - [Step 2. Add Web Part to Search Results](#)
- [Troubleshooting](#)

Requirements

- **SharePoint Server 2010:** Only SharePoint Server 2010 (Standard or Enterprise) supports federated search locations. This functionality is not included in SharePoint Foundation 2010.
- **The Confluence OpenSearch plugin and SharePoint search configuration:** Your Confluence installation must include the OpenSearch plugin and must be configured to share search results with SharePoint. Optionally, you can also configure Confluence to use the SharePoint Decorators theme. See the [guide to installing the Confluence SharePoint plugins](#).

SharePoint Configuration

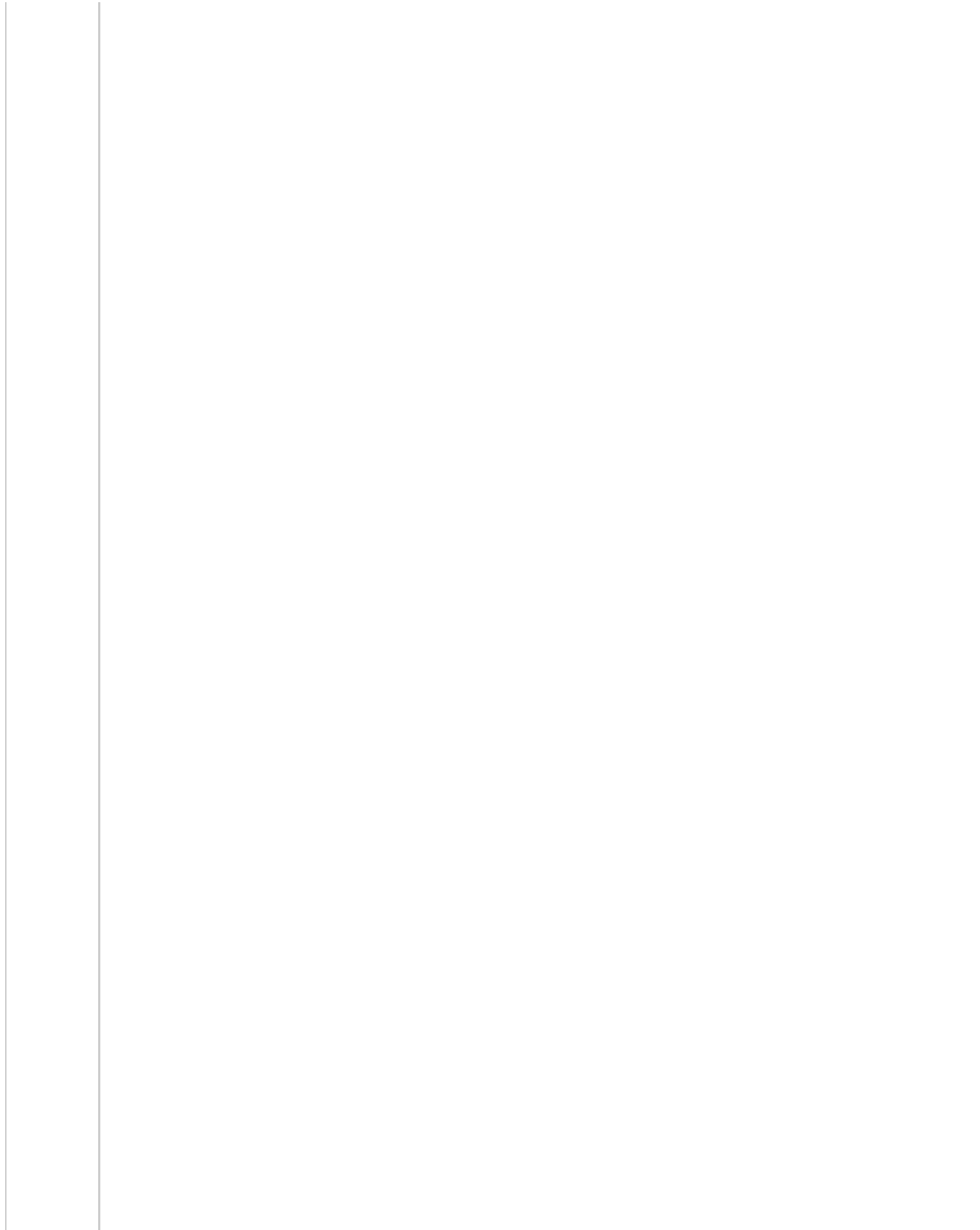
Step 1. Configure the Federated Search Location

1. Log in to your **SharePoint Central Administration** site as a SharePoint farm administrator.
2. Click **'Manage service applications'** under the **'Application Management'** heading.
3. Click **'Search Service Application'**.
4. Click **'Federated Locations'** under the **'Queries and Results'** heading in the left-hand navigation panel.
5. Click **'New Location'**.
6. Fill in the information for the new federated location, and then click **'OK'**. Here are some guidelines on the mandatory fields:

Field Name	Meaning
Location Name	The name of this location. We suggest 'Confluence'.
Display Name	The name of the location which will be displayed to users.
Description	A description of this location.
Location Type	The type of search to perform. We need OpenSearch.
Query Template	This is the URL which will be used to perform the actual search. This URL depends on the authentication used by Confluence: * Standard (forms) authentication: <code>http://<CONFLUENCE_SERVER>/plugins/servlet/opensearch?query={searchTerms}&format=rss_1.0&os_a</code> * NTLM: <code>http://<CONFLUENCE_SERVER>/plugins/servlet/opensearch?query={searchTerms}&format=rss_1.</code>
"More Results" Link Template	The link which users will go to if they click the "More Results" link: <code>http://<CONFLUENCE_SERVER>/dosearchsite.action?queryString={userQuery}</code>
Specify Credentials	This specifies how Sharepoint will send the credentials for the searching user to Confluence. Make sure that you set the credentials in the 'Advanced' section, not the 'Common' section. The actual credentials depend on the authentication used by Confluence: * Standard (forms) authentication: choose "Basic Authentication" * NTLM: choose "NTLM Authentication" If you use the Secure Store Service (see the corresponding configuration guide), select the Use SSS option and enter the name of the Confluence application in the Target Application ID field. If you do not use the Secure Store Service, then leave the Use SSS option unselected.

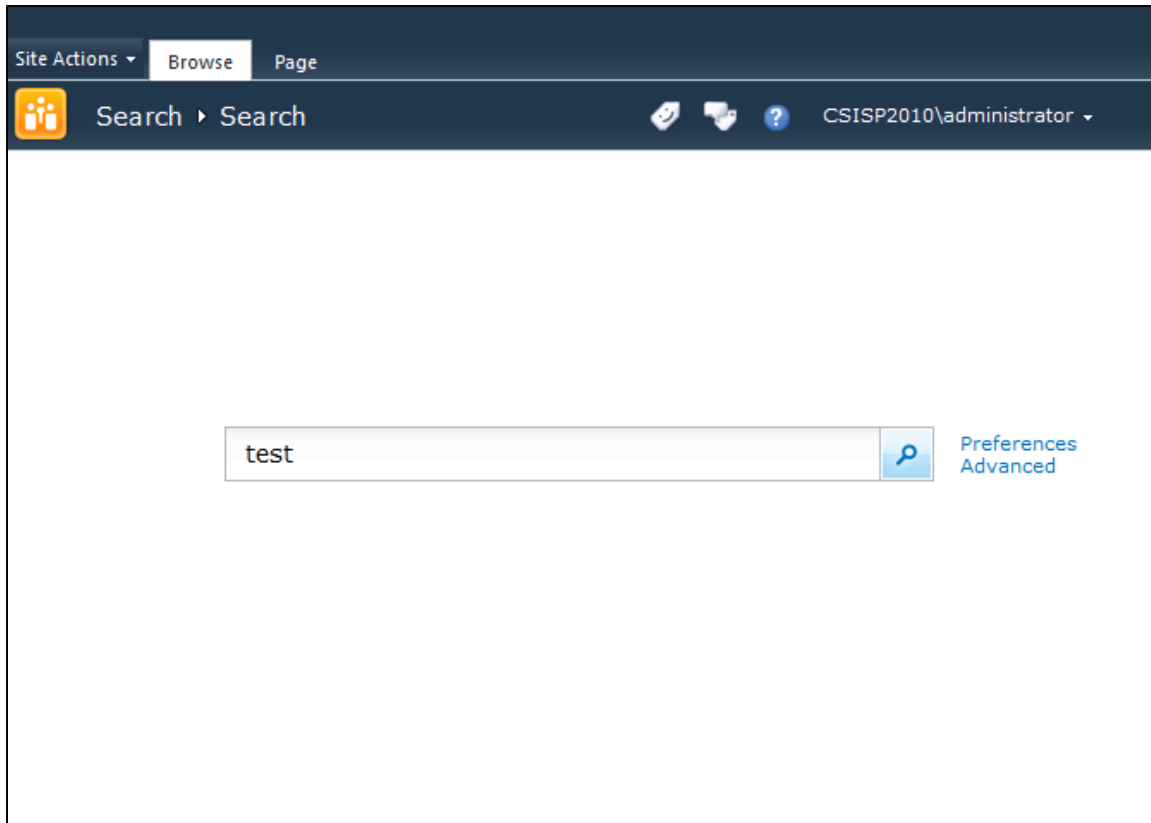
Federated
Search
Results
Display
Metadata:
XSL

This specifies how to display the results. This can optionally be changed using the example XML to use Confluence icons for C search results.

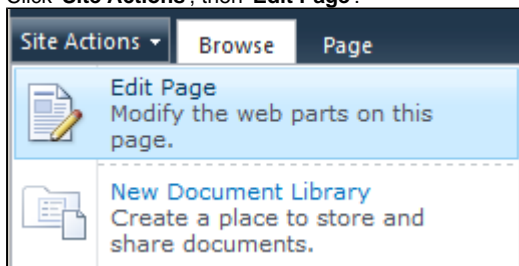


Step 2. Add Web Part to Search Results

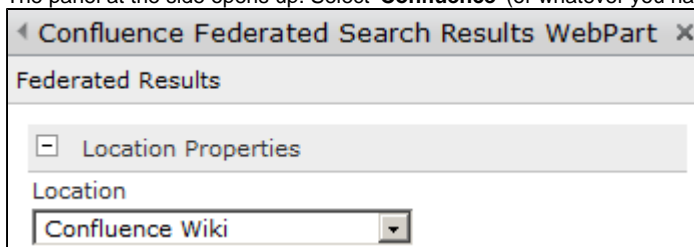
1. Go to your SharePoint Search Site and execute a search, which will take you to the search results screen.



2. Click **'Site Actions'**, then **'Edit Page'**:



3. Click **'Add a Web Part'**. You can add the web part anywhere on the page. This is where the Confluence results will appear:
4. The **'Add Web Parts'** screen appears. Select the web part:
 - **With SSS:** If you are using the Secure Store Service and selected **'Use SSS'** when setting up the federated location, then select **'Federated Results'**.
 - **Without SSS:** If you are not using the Secure Store Service and did not select **'Use SSS'** when setting up the federated location, then select **'Confluence Federated Search Results WebPart'**.
5. Click the **'Add'** button.
6. Open the **'Edit'** menu for the web part which you have just added and select **'Edit Web Part'**.
7. The panel at the side opens up. Select **'Confluence'** (or whatever you named the federated location) from the dropdown menu:



8. Click **'OK'**, then **'Stop Editing'**. Setup is complete.

Troubleshooting

Please refer to our [knowledge base](#), in particular the following:

- [SharePoint Formats the Confluence Search Results Badly](#)

RELATED TOPICS

[Installing and Configuring the SharePoint Feature on SP 2010](#)
[Installing the SharePoint Connector](#)

Upgrading the SharePoint Connector

This page tells you how to upgrade an existing installation of the Confluence SharePoint Connector to the latest version of the connector, **SharePoint Connector 1.3**.

There are two upgrade procedures to choose from:

- **Option 1: Upgrade your SharePoint Connector on SharePoint 2010.** This procedure assumes that you have upgraded your SharePoint server to Microsoft SharePoint 2010. To upgrade the connector, you will install the latest version of the SharePoint Connector plugin in Confluence and upgrade the SharePoint feature in Microsoft SharePoint 2010. See the [instructions](#).
- **Option 2: Upgrade your SharePoint Connector on SharePoint 2007.** This procedure assumes that you are running the SharePoint Connector on Microsoft SharePoint 2007. To upgrade the connector, you will install the latest version of the SharePoint Connector plugin in Confluence and upgrade the SharePoint feature in Microsoft SharePoint 2007. See the [instructions](#).

Upgrading the SharePoint Connector on SharePoint 2007

This page tells you how to upgrade an existing installation of the Confluence SharePoint Connector to the latest version of the connector, assuming you are using **Microsoft SharePoint 2007**. To upgrade the connector, you will install the latest version of the SharePoint Connector plugin in Confluence and upgrade the SharePoint feature in Microsoft SharePoint 2007.



Please check that this is the right guide for you.

Instructions in this guide assume the following:

- You are **upgrading an existing installation** of the SharePoint Connector. (If you have not previously installed the connector, please follow the [installation guide](#) instead.)
- You are upgrading the SharePoint Connector on **Microsoft SharePoint 2007**. (If you are using SharePoint 2010, please follow the guide to [upgrading the connector on SharePoint 2010](#).)
- You are upgrading from **SharePoint Connector 1.1.1**. (If you are upgrading from an earlier version of the connector, your experience may be slightly different. Please contact [Atlassian support](#) for assistance if you need it.)

On this page:

- [Step 1: Read the Release Notes and Upgrade Notes](#)
- [Step 2: Check the SharePoint Updates and Upgrade SharePoint if Necessary](#)
- [Step 3: Upgrade the SharePoint Connector Plugin in Confluence](#)
- [Step 4: Upgrade the SharePoint Connector Feature in SharePoint](#)

Step 1: Read the Release Notes and Upgrade Notes

Please read the [release notes and accompanying upgrade notes](#) for any versions you are skipping as well as the version you are upgrading to. Pay particular attention to the upgrade notes and make a note to perform any of the additional steps described there:

- [SharePoint Connector 1.3 Release Notes](#)
 - [SharePoint Connector 1.3 Upgrade Notes](#)
- [SharePoint Connector 1.2.1 Release Notes](#)
- [SharePoint Connector 1.2 Release Notes](#)
 - [SharePoint Connector 1.2 Upgrade Notes](#)
- [SharePoint Connector 1.1.1 Release Notes](#)
- [SharePoint Connector 1.1 Release Notes](#)
 - [SharePoint Connector 1.1 Upgrade Notes](#)
- [SharePoint Connector 1.0 Release Notes](#)
 - [SharePoint Connector 1.0 Changelog](#)



For example, if you are upgrading from version 1.0 to version 1.2 of the connector, skipping version 1.1, then you will need to perform the steps described in the [SharePoint Connector 1.1 Upgrade Notes](#).

Step 2: Check the SharePoint Updates and Upgrade SharePoint if Necessary

The SharePoint Connector's federated search feature relies on new functionality in SharePoint. At least one of the following updates to SharePoint must be installed on your MOSS Server(s):

- Search Server 2008 Infrastructure Update (<http://blogs.msdn.com/sharepoint/archive/2008/07/15/announcing-availability-of-infrastructure-updates.aspx>).
- Service Pack 1 (<http://blogs.msdn.com/sharepoint/archive/2007/12/11/announcing-the-release-of-wss-3-0-sp1-and-office-sharepoint-server-2007-sp1>).
- Service Pack 2 (<http://blogs.msdn.com/sharepoint/archive/2009/04/28/announcing-service-pack-2-for-office-sharepoint-server-2007-and-windows-sha>).


We recommend **Service Pack 2**, which is the most recent update. If you need to install one of these updates, you should schedule this

upgrade of SharePoint **before** proceeding with the SharePoint Connector 1.1 installation.

Step 3: Upgrade the SharePoint Connector Plugin in Confluence

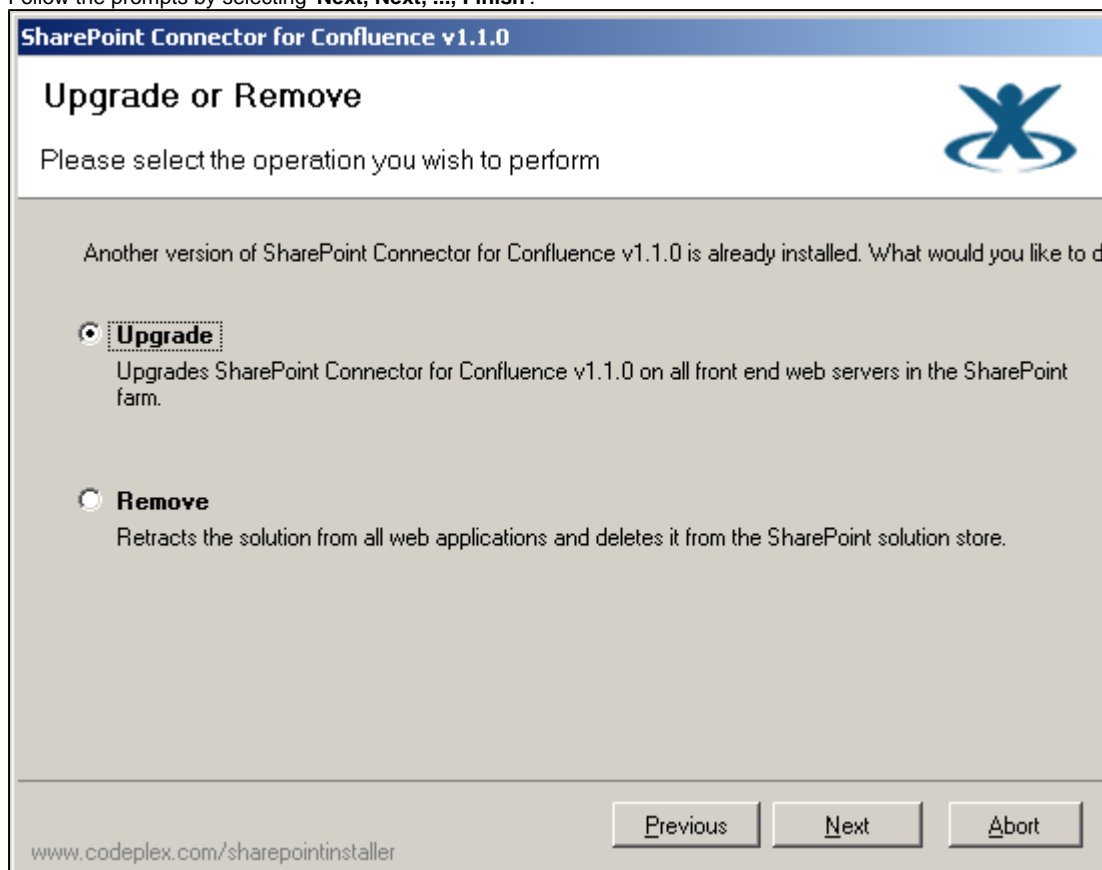
1. Upgrade the SharePoint Connector plugin via the Confluence Plugin Repository:
 - Go to the Confluence '**Administration Console**'. To do this:
 - Open the '**Browse**' menu and select '**Confluence Admin**'. The 'Administration Console' view will open.
 - Click '**Plugin Repository**' in the 'Configuration' section of the left-hand navigation panel to open the 'Atlassian Plugin Repository' page.
 - Scroll down to the row showing the '**SharePoint Plugin**' and click '**Upgrade**'.
2. You may need to restart Confluence after upgrading the Confluence SharePoint Connector plugin.

If you do not see the 'Upgrade' option, please follow these steps instead:

1. Click '**Plugins**' in the 'Configuration' section of the left-hand navigation panel (not 'Plugin Repository').
 2. Select the '**SharePoint Connector for Confluence**' plugin.
 3. Click '**Uninstall**' to remove the plugin from your Confluence site.
 4. Click '**Plugin Repository**' in the 'Configuration' section of the left-hand navigation panel to open the 'Atlassian Plugin Repository' page.
 5. Scroll down to the row for the '**SharePoint Plugin**' and click '**Install**'.
-  Provided you do not restart Confluence after uninstalling the old version of the plugin, you will not lose your configuration settings and SharePoint Connector license details.

Step 4: Upgrade the SharePoint Connector Feature in SharePoint

1. Download the SharePoint component from the [SharePoint Connector download centre](#).
2. Extract the contents of the downloaded SharePointConnector zip file and open the SharePoint Installer directory.
3. Upgrade the SharePoint features by running **Setup_WebParts.exe**. Select the option to '**Upgrade**' the SharePoint Connector. Follow the prompts by selecting '**Next, Next, ..., Finish**'.



4. You may need to restart IIS after upgrading the Sharepoint Connector feature.



Need help?

If you encounter a problem during the upgrade, please create a [support ticket](#) and one of our support engineers will assist you through the process.

RELATED TOPICS

- [Release Notes](#)
- [Installing the SharePoint Connector](#)
- [Upgrading the SharePoint Connector](#)
- [Applying Specific Confluence Configurations](#)
- [Deploying the SharePoint Connector to More SharePoint Sites](#)

Upgrading the SharePoint Connector on SharePoint 2010

This page tells you how to upgrade an existing installation of the Confluence SharePoint Connector to the latest version of the connector, assuming you are using **Microsoft SharePoint 2010**.



Please check that this is the right guide for you.

Instructions in this guide assume the following:

- You are **upgrading an existing installation** of the SharePoint Connector. (If you have not previously installed the connector, please follow the [installation guide](#) instead.)
- You are upgrading the SharePoint Connector on **Microsoft SharePoint 2010**. (If you are using SharePoint 2007, please follow the guide to [upgrading the connector on SharePoint 2007](#).)
- You are upgrading from **SharePoint Connector 1.1.1**. (If you are upgrading from an earlier version of the connector, your experience may be slightly different. Please contact [Atlassian support](#) for assistance if you need it.)

On this page:

- [Step 1: Plan your Upgrade of Microsoft SharePoint](#)
- [Step 2: Read the SharePoint Connector Release Notes and Upgrade Notes](#)
- [Step 3: Run the SharePoint Pre-Upgrade Checks](#)
- [Step 4: Upgrade the SharePoint Connector Plugin in Confluence](#)
- [Step 5: Upgrade your SharePoint Server to SharePoint 2010](#)
- [Step 6: Upgrade the SharePoint Connector Feature in SharePoint](#)
- [Step 7: Re-Apply the Confluence Settings in SharePoint](#)
- [Step 8: Run the SharePoint Visual Upgrade](#)

Step 1: Plan your Upgrade of Microsoft SharePoint

Read the [Microsoft TechNet guide on upgrading to SharePoint Server 2010](#) and plan your approach to upgrading from Microsoft Office SharePoint Server 2007 to Microsoft SharePoint Server 2010.

Step 2: Read the SharePoint Connector Release Notes and Upgrade Notes

Please read the SharePoint Connector [release notes and accompanying upgrade notes](#) for any versions you are skipping as well as the version you are upgrading to. Pay particular attention to the upgrade notes and make a note to perform any of the additional steps described there:

- [SharePoint Connector 1.3 Release Notes](#)
 - [SharePoint Connector 1.3 Upgrade Notes](#)
- [SharePoint Connector 1.2.1 Release Notes](#)
- [SharePoint Connector 1.2 Release Notes](#)
 - [SharePoint Connector 1.2 Upgrade Notes](#)
- [SharePoint Connector 1.1.1 Release Notes](#)
- [SharePoint Connector 1.1 Release Notes](#)
 - [SharePoint Connector 1.1 Upgrade Notes](#)
- [SharePoint Connector 1.0 Release Notes](#)
 - [SharePoint Connector 1.0 Changelog](#)



For example, if you are upgrading from version 1.0 to version 1.2 of the connector, skipping version 1.1, then you will need to perform the steps described in the [SharePoint Connector 1.1 Upgrade Notes](#).

Step 3: Run the SharePoint Pre-Upgrade Checks

Follow the [Microsoft TechNet guide](#) to perform the required pre-upgrade steps.

Step 4: Upgrade the SharePoint Connector Plugin in Confluence


1. Upgrade the SharePoint Connector plugin via the Confluence Plugin Repository:

- Go to the Confluence '**Administration Console**'. To do this:
 - Open the '**Browse**' menu and select '**Confluence Admin**'. The 'Administration Console' view will open.
- Click '**Plugin Repository**' in the 'Configuration' section of the left-hand navigation panel to open the 'Atlassian Plugin Repository' page.
- Scroll down to the row showing the '**SharePoint Plugin**' and click '**Upgrade**'.

2. You may need to restart Confluence after upgrading the Confluence SharePoint Connector plugin.

If you do not see the 'Upgrade' option, please follow these steps instead:

1. Click **'Plugins'** in the 'Configuration' section of the left-hand navigation panel (not 'Plugin Repository').
2. Select the **'SharePoint Connector for Confluence'** plugin.
3. Click **'Uninstall'** to remove the plugin from your Confluence site.
4. Click **'Plugin Repository'** in the 'Configuration' section of the left-hand navigation panel to open the 'Atlassian Plugin Repository' page.
5. Scroll down to the row for the **'SharePoint Plugin'** and click **'Install'**.

 Provided you do not restart Confluence after uninstalling the old version of the plugin, you will not lose your configuration settings and SharePoint Connector license details.

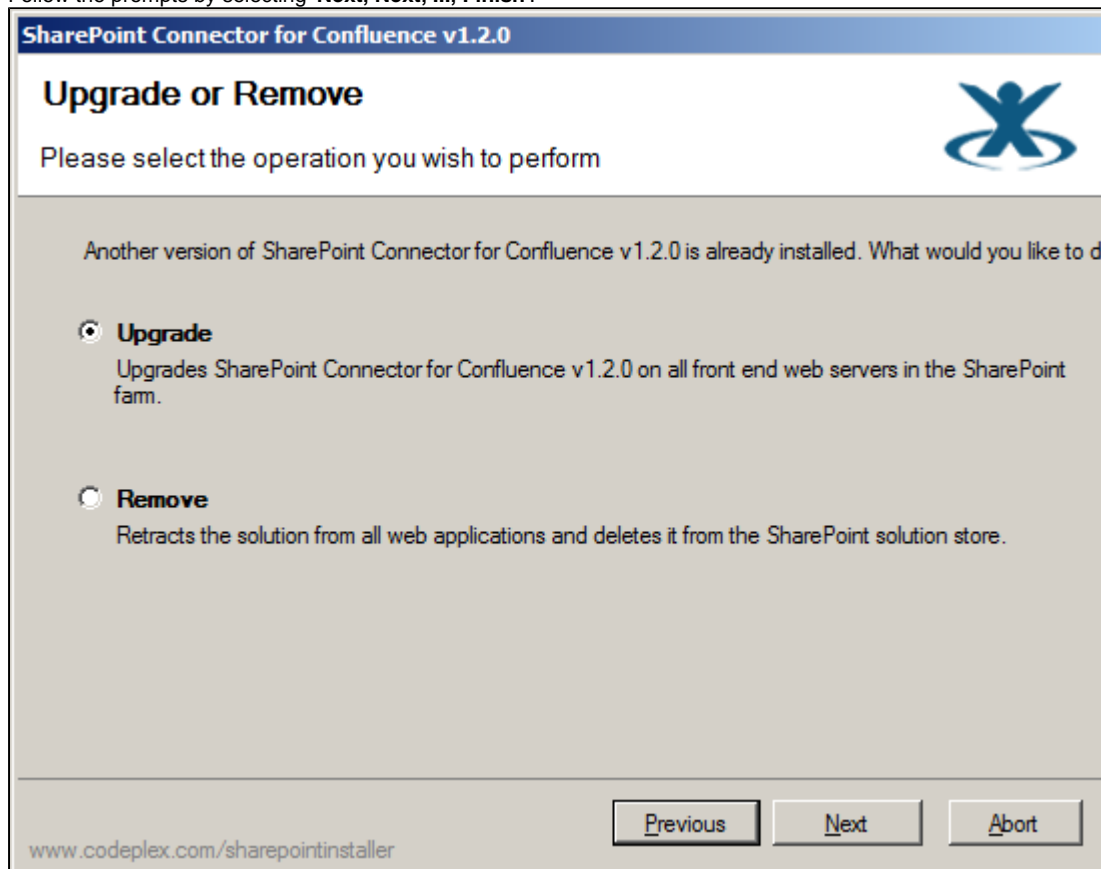
Step 5. Upgrade your SharePoint Server to SharePoint 2010

Upgrade your SharePoint farm to SharePoint 2010 by following one of the upgrade methods supported by Microsoft. You will find a full list of supported upgrade methods in the [TechNet article on determining your upgrade approach](#).

Step 6: Upgrade the SharePoint Connector Feature in SharePoint

After you have completed the SharePoint 2010 upgrade and run the **SharePoint 2010 Products Configuration Wizard**, you should proceed with upgrading the Confluence components to the SharePoint 2010 compatible version.

1. Download the SharePoint component from the [SharePoint Connector download centre](#).
2. Extract the contents of the downloaded `SharePointConnector` zip file and open the `SharePoint Installer` directory.
3. Upgrade the SharePoint features by running **Setup_WebParts.exe**. Select the option to **'Upgrade'** the SharePoint Connector. Follow the prompts by selecting **'Next, Next, ..., Finish'**.



4. You may need to restart IIS after upgrading the Sharepoint Connector feature.

Step 7. Re-Apply the Confluence Settings in SharePoint



New hardware?

This step is necessary if you have moved your SharePoint server to new hardware, that is, if you performed a 'database attach upgrade' of your SharePoint server as described in the [TechNet article](#). The encryption of the Confluence password is based on the SharePoint machine key. You will need to re-apply the settings to re-encrypt the password.

Follow the instructions to [configure the Confluence administrative settings in SharePoint](#).

Step 8. Run the SharePoint Visual Upgrade

Run the SharePoint Visual Upgrade feature as described in the [Microsoft TechNet article](#) to upgrade to the new user interface.



Need help?

If you encounter a problem during the upgrade, please create a [support ticket](#) and one of our support engineers will assist you through the process.

RELATED TOPICS

- [Release Notes](#)
- [Installing the SharePoint Connector](#)
- [Upgrading the SharePoint Connector](#)
- [Applying Specific Confluence Configurations](#)
- [Deploying the SharePoint Connector to More SharePoint Sites](#)

Applying Specific Confluence Configurations

This section is part of the SharePoint Connector installation and configuration guide. It contains specific configurations that you may need to apply to your Confluence installation.

Before applying any of these configurations, please read our guide to [planning your environment with SharePoint 2007](#) or [planning your environment with SharePoint 2010](#).

- [Configuring Tomcat-Connector for IIS 6.0 \(Windows Server 2003\)](#)
- [Configuring Tomcat-Connector for IIS 7.0 \(Windows Server 2008\)](#)
- [Configuring Confluence to use Jespa for NTLM Authentication](#)
- [Configuring Confluence to use JCIFS for NTLM Authentication](#)

Configuring Tomcat-Connector for IIS 6.0 (Windows Server 2003)

This page is part of the installation guide for the **Confluence SharePoint Connector**. It tells you how to configure access to Confluence using Integrated Windows Authentication via IIS.

This section of the guide describes the steps necessary to set up an IIS 6.0 website that will perform authentication using NTLM or Kerberos, and then forward the authenticated requests to the Confluence instance. This is achieved by installing a custom ISAPI filter in IIS that understands how to use the AJP protocol to communicate with Confluence.

On this page:

- [Installation](#)
 - [Step 1. Install and Configure AJP Connector](#)
 - [Step 2. Add ISAPI Filter](#)
 - [Step 3. Add Virtual Directory](#)
 - [Step 4. Enable Integrated Windows Authentication](#)
 - [Step 5. Add Web Service Extension](#)
- [Troubleshooting](#)

Installation

Step 1. Install and Configure AJP Connector



Connector is currently attached to this page

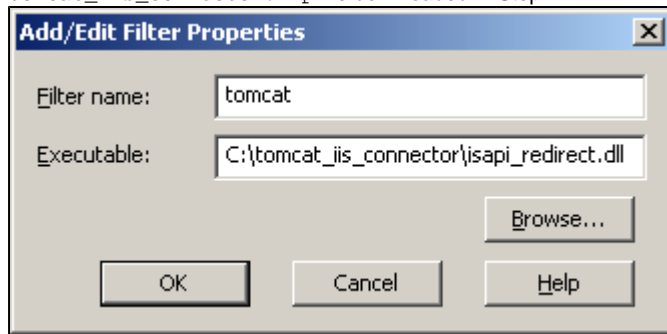
Currently, the Tomcat AJP Connector for IIS is attached to this page as a zip file. We are working on moving the connector to a central, managed location.

1. Download the [tomcat_iis_connector.zip](#) file attached to this page and extract it somewhere convenient on the server. The default location is `C:\tomcat_iis_connector`.
2. If you extracted the AJP Connector to a directory other than the default (`C:\tomcat_iis_connector`), then edit the `isapi_redirect.properties` file and ensure that the `log_file`, `worker_file`, `worker_mount_file` and `rewrite_rule_file` properties point to the correct locations.
3. If your Confluence server is not running on the same server as IIS (for example, if Confluence is running on non-Windows server) then edit the `workers.properties.minimal` file in the `conf` directory so that the `worker.worker1.host` property points to the IP Address or hostname of your Confluence server.
4. The default port used in this guide for Confluence's AJP Connector is **8009**. If you wish to use a different port, then edit the `workers.properties.minimal` file in the `conf` directory so that the `worker.worker1.port` property specifies the desired port number.

Step 2. Add ISAPI Filter

1. Open the **Internet Information Services (IIS) Manager**.
2. Right-click on the website that will be used to proxy Confluence requests and click **'Properties'**.
3. Select the **'ISAPI Filters'** tab and click **'Add'**.

4. Enter a '**Filter name**' of 'tomcat' and then set the '**Executable**' to the `isapi_redirect.dll` that you extracted from the `tomcat_iis_connector.zip` file downloaded in Step 1.



5. Click '**OK**'.
6. The filter should now be listed in the ISAPI Filters list for the website:

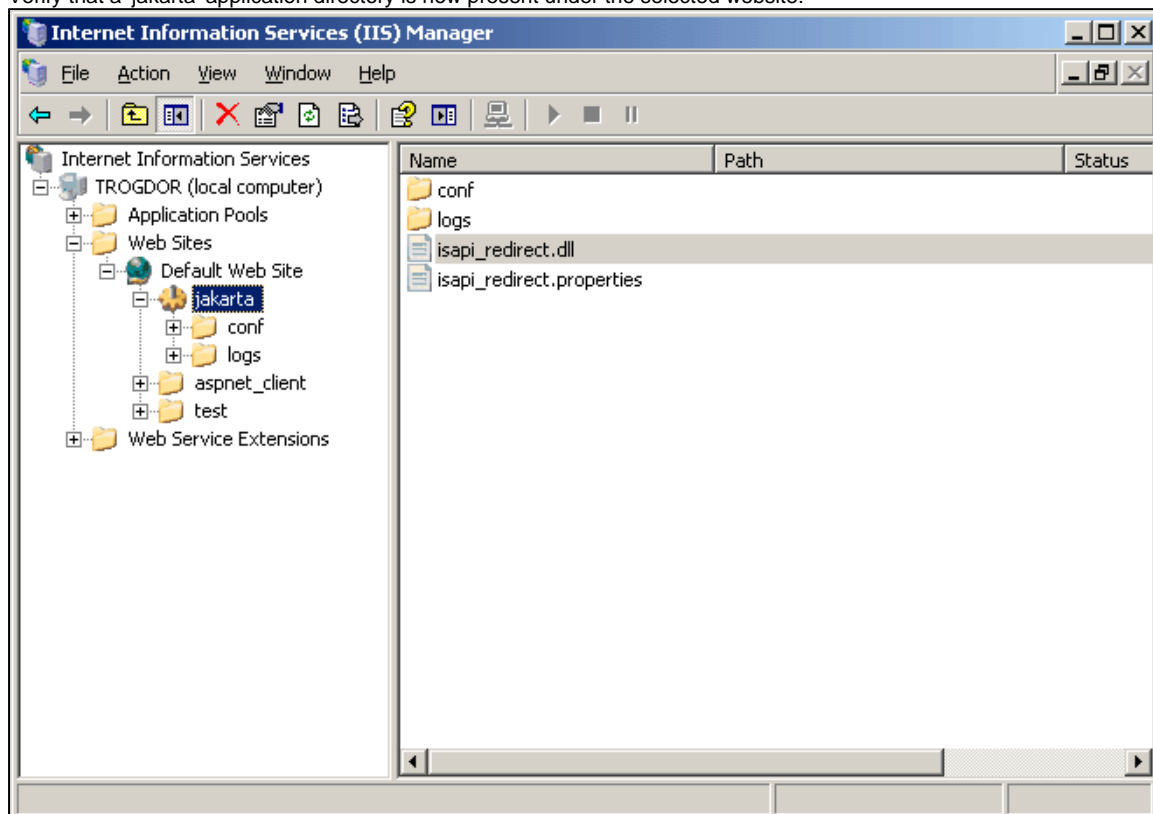
Status	Filter Name	Priority
	tomcat	* Unknown *

7. Click '**OK**'.

Step 3. Add Virtual Directory

Now you will add a virtual directory in the IIS website to host the ISAPI Filter.

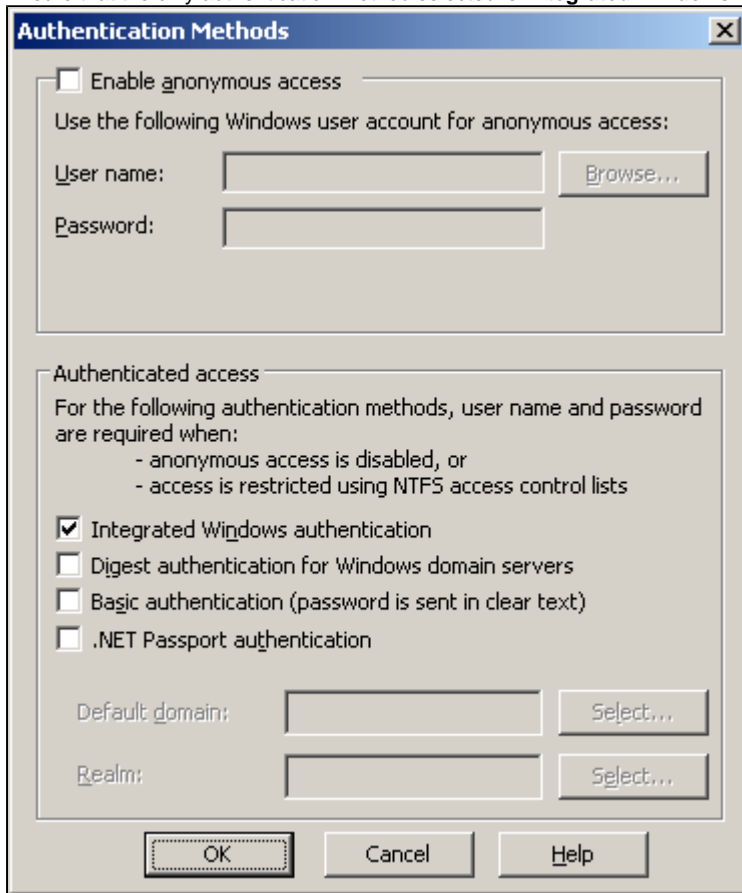
1. Right-click on the website that will be used to proxy Confluence requests and select '**New**', '**Virtual Directory**'.
2. Click '**Next**'.
3. Enter an '**Alias**' of 'jakarta' for the virtual directory.
4. Click '**Next**'.
5. Set the '**Path**' to be the directory where you extracted the `iis_tomcat_connector.zip` file in Step 1 (such as, `C:\tomcat_iis_connector`).
6. Click '**Next**'.
7. Allow the following permissions: **Read, Execute (such as ISAPI applications or CGI)**.
8. Click '**Next**'.
9. Click '**Finish**'.
10. Verify that a 'jakarta' application directory is now present under the selected website:



Step 4. Enable Integrated Windows Authentication

This step involves modifying the directory security of the website to use NTLM or Kerberos authentication.

1. Right-click the website that will be used to proxy Confluence requests and select '**Properties**'.
2. Select the '**Directory Security**' tab.
3. In the '**Authentication and access control**' section, select '**Edit**'.
4. Ensure that the only authentication method selected is '**Integrated Windows Authentication**'.

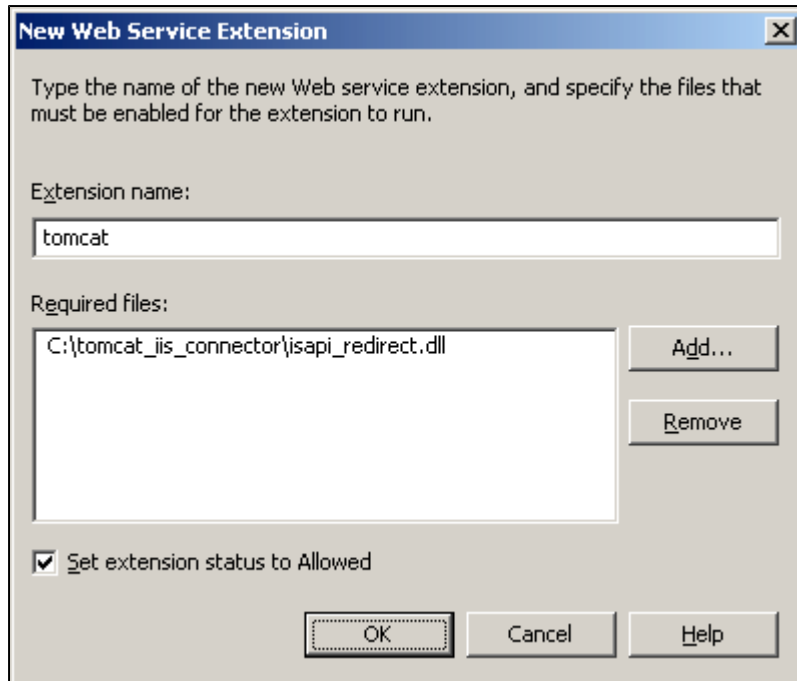


5. Click '**OK**'.
6. Click '**OK**'.

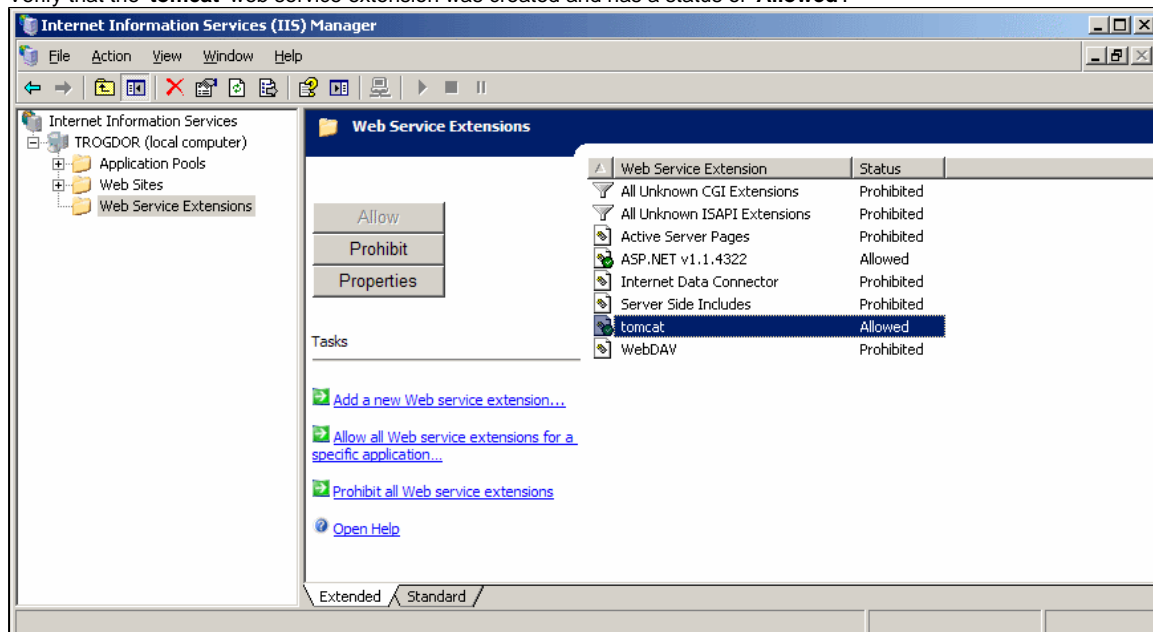
Step 5. Add Web Service Extension

The final step in configuring IIS is to register the custom ISAPI filter as a Web Service Extension.

1. In the **Internet Information Services (IIS) Manager**, right-click the '**Web Service Extensions**' folder and select '**Add a new Web service extension**'.
2. Set the '**Extension name**' to 'tomcat'.
3. Click '**Add**'.
4. Set the '**Path to file**' to the location of the `isapi_redirect.dll` extracted from the `tomcat_iis_connector.zip` file downloaded in Step 1.
5. Click '**OK**'.
6. Select the '**Set extension status to Allowed**' option:




7. Click 'OK'.
8. Verify that the 'tomcat' web service extension was created and has a status of 'Allowed'.



Troubleshooting

Could not load all ISAPI filters for site/service

If the Tomcat filter is listed in the 'ISAPI Filters' tab for your website with a bright red arrow after attempting to test the filter, this means that the filter has been disabled because IIS was unable to load it.

Status	Filter Name	Priority
	tomcat	* Unknown *

You should ensure that the identity of the application pool running the Web Service Extension has read permissions to the folder where you installed the connector and write permissions to the log file location specified in the **worker.properties.minimal** file.

RELATED TOPICS

- [Release Notes](#)
- [Installing the SharePoint Connector](#)
- [Upgrading the SharePoint Connector](#)
- [Applying Specific Confluence Configurations](#)
- [Deploying the SharePoint Connector to More SharePoint Sites](#)

Configuring Tomcat-Connector for IIS 7.0 (Windows Server 2008)

This page is part of the installation guide for the **Confluence SharePoint Connector**. It tells you how to configure access to Confluence using Integrated Windows Authentication via IIS.

This section of the guide describes the steps necessary to set up an IIS website that will perform authentication using NTLM or Kerberos, and then forward the authenticated requests to the Confluence instance. You will do this by installing a custom ISAPI filter in IIS that understands how to use the AJP protocol (Apache JServ Protocol) to communicate with Confluence.

On this page:

- [Installation](#)
 - [Step 1. Install and Configure the AJP Connector](#)
 - [Step 2. Add ISAPI Filter](#)
 - [Step 3. Add Virtual Directory](#)
 - [Step 4. Enable Integrated Windows Authentication](#)
 - [Step 5. Register the ISAPI Extension](#)
 - [Step 6. Allow Double Escaping](#)

Installation

Step 1. Install and Configure the AJP Connector

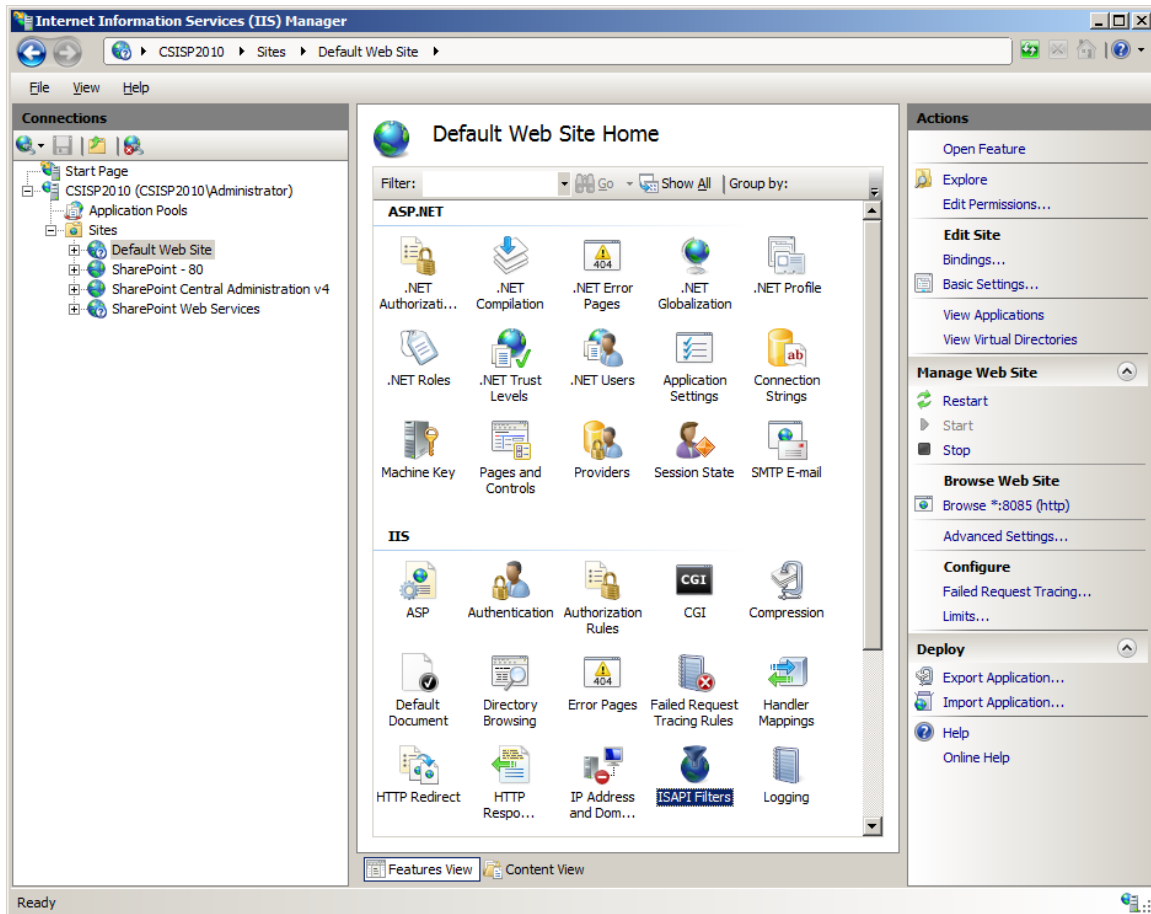
1. Download the latest Tomcat Connector ISAPI Filter binaries from the download page on apache.org, ensuring that you select the version that is appropriate for your operating system and CPU architecture. At the time this installation guide was written, the latest version was jk-1.2.30. Use the table below to help identify the correct download version for your server.

Operating System	CPU Architecture	Download Link
Windows Server 2008 x86 (32-bit)	Any	win32
Windows Server 2008 x64 (64-bit)	Intel 64 or AMD64 (x86-64)	win64-amd64
Windows Server 2008 x64 (64-bit)	Intel Itanium (IA-64)	win64-ia64

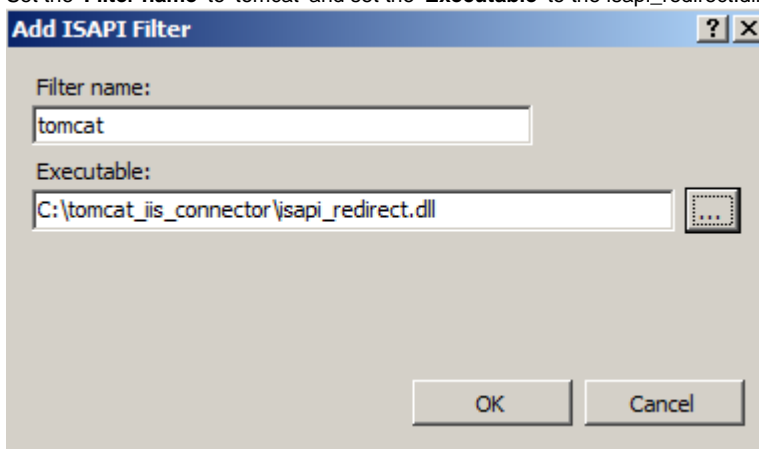
2. Download the [tomcat_iis_connector.zip](#) file attached to this page. It contains the configuration files necessary for the ISAPI filter to run and communicate with your Confluence server.
3. Extract the downloaded zip file and place the contents in a folder alongside the downloaded binary file in a convenient location on your server. The default location is `C:\tomcat_iis_connector`.
4. Rename the downloaded binary file to **isapi_redirect.dll** (that is, remove the version number from the file name).
5. If you extracted the AJP Connector to a directory other than the default (`C:\tomcat_iis_connector`), then edit the **isapi_redirect.properties** file and ensure that the **log_file**, **worker_file**, **worker_mount_file** and **rewrite_rule_file** properties point to the correct locations.
6. If your Confluence server is not running on the same server as IIS (for example, if Confluence is running on a non-Windows server), then edit the **worker.properties.minimal** file in the **conf** directory so that the **worker.worker1.host** property points to the IP address or host name of your Confluence server.
7. If you wish to change the default port for Confluence's AJP Connector, then edit the **worker.properties.minimal** file in the **conf** directory and change the **worker.worker1.port** property to specify the required port number. The default port used in this guide for Confluence's AJP Connector is **8009**.

Step 2. Add ISAPI Filter

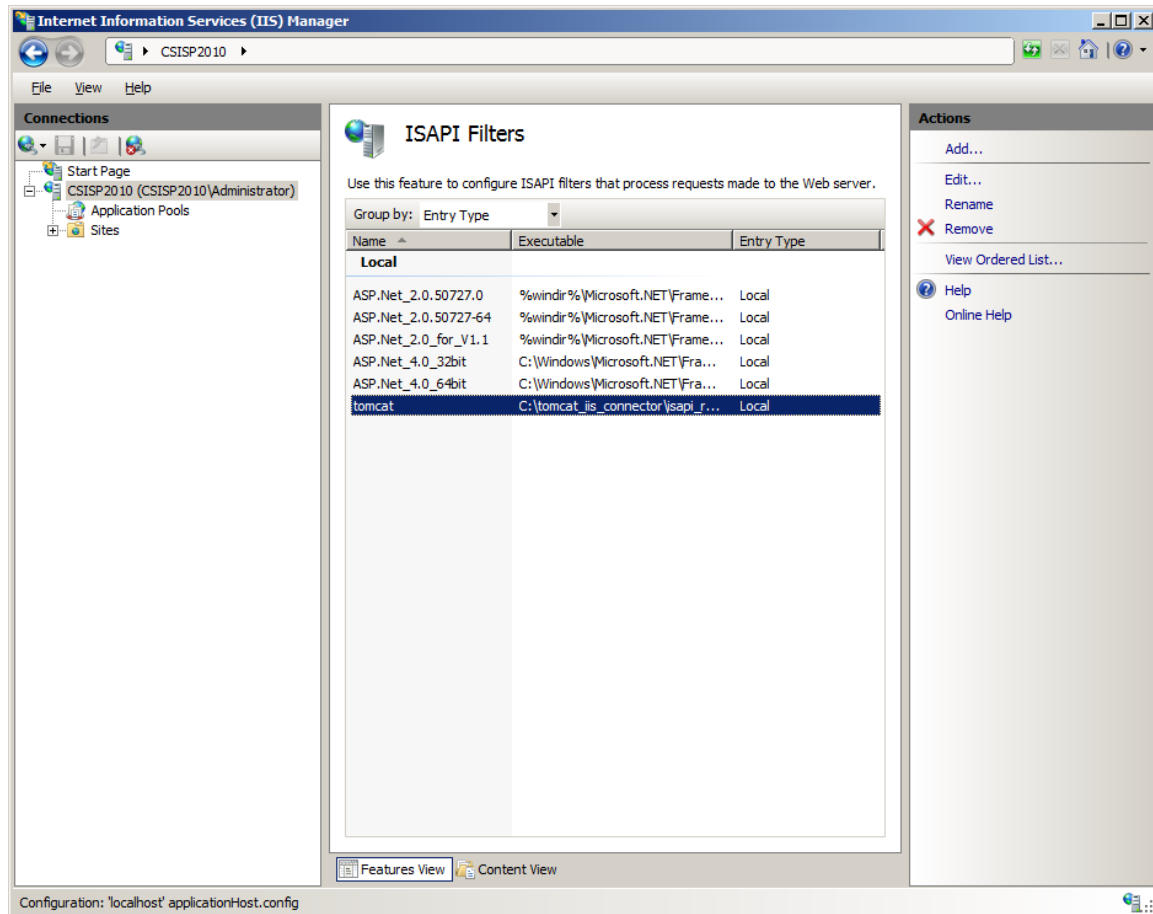
1. Open the **Internet Information Services (IIS) Manager**.
2. In the **'Connections'** panel, ensure that the IIS Web Site that will be used to proxy Confluence requests is selected.
3. Double-click the **'ISAPI Filters'** icon in **'Features View'**.



4. In the **'Actions'** panel on the right, select **'Add'**.
5. Set the **'Filter name'** to 'tomcat' and set the **'Executable'** to the isapi_redirect.dll that you downloaded in step 1.



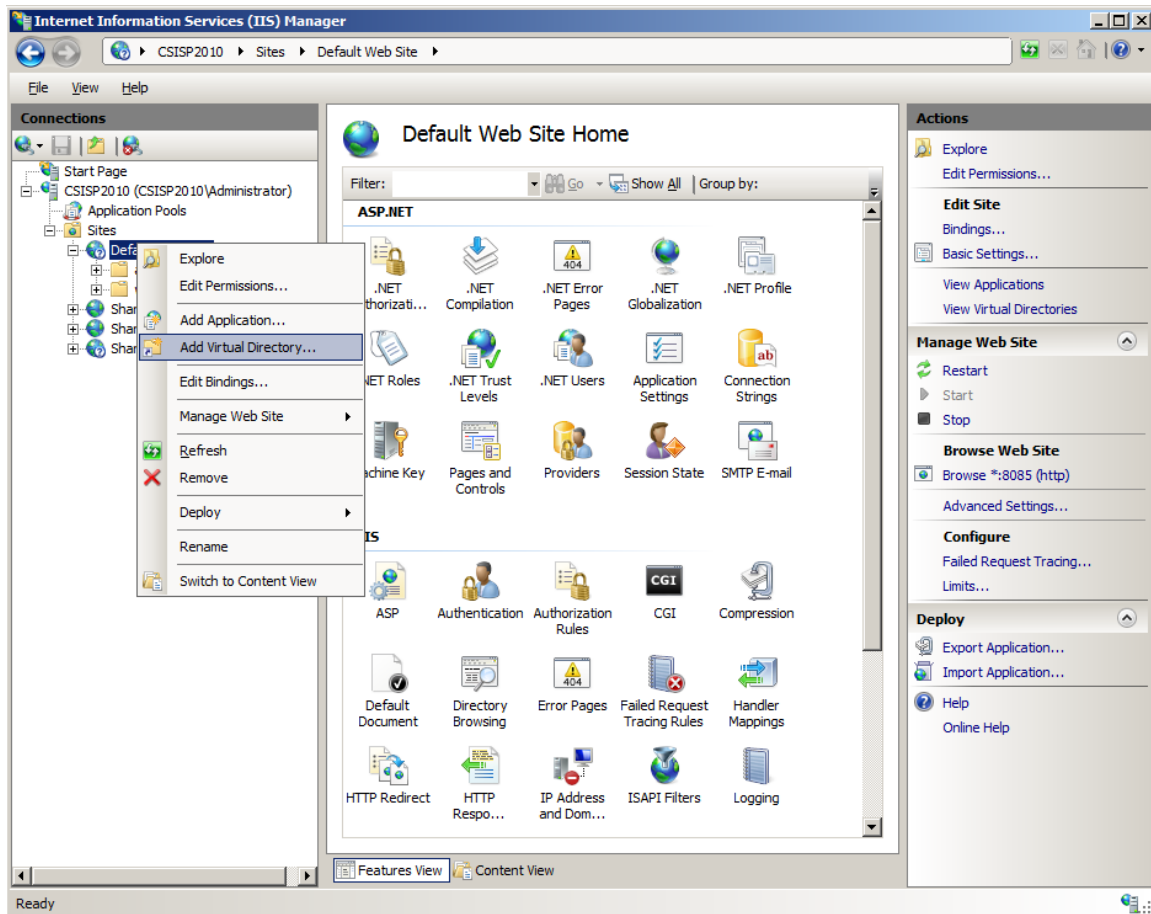
6. Click **'OK'**.
7. The new filter should now be listed in the ISAPI Filters list for the website.



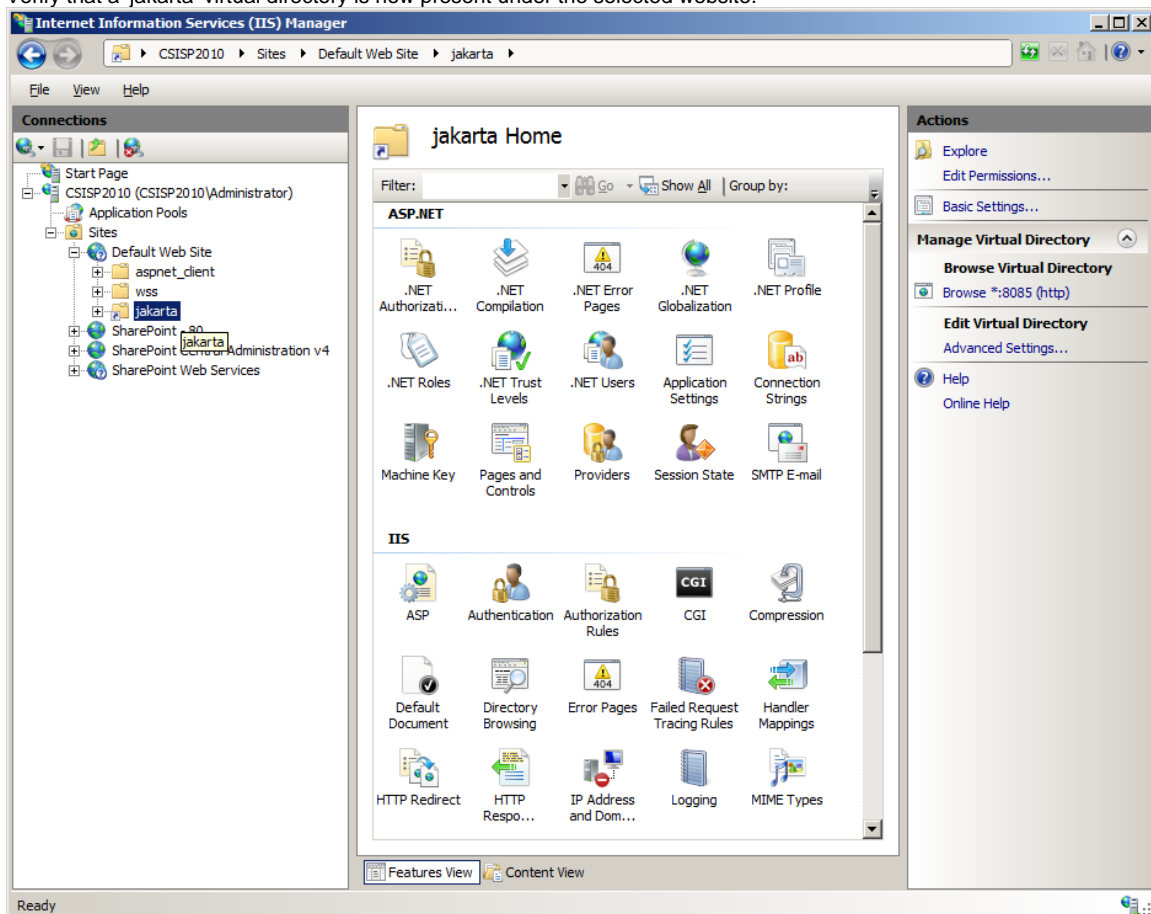
Step 3. Add Virtual Directory

Now you will add a virtual directory in the IIS website to host the ISAPI Filter.

1. In the **'Connections'** panel, ensure that the correct IIS Web Site is selected.
2. Right-click the IIS Web Site and select **'Add Virtual Directory'**.

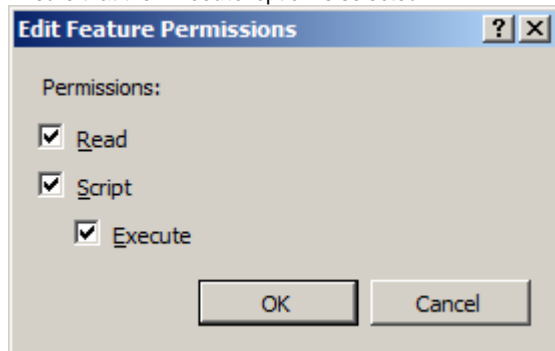


3. Set the '**Alias**' to 'jakarta'.
4. Set the '**Physical Path**' to the directory where you extracted the ISAPI Filter in step 1 (such as, C:\tomcat_iis_connector).
5. Click '**OK**'.
6. Verify that a 'jakarta' virtual directory is now present under the selected website.



7. Next, select the '**jakarta**' virtual directory in the '**Connections**' panel.

8. Double-click the **'Handler Mappings'** icon in **'Features View'**.
9. Click the **'Edit Feature Permissions'** link in the **'Actions'** panel.
10. Ensure that the **'Execute'** option is selected.

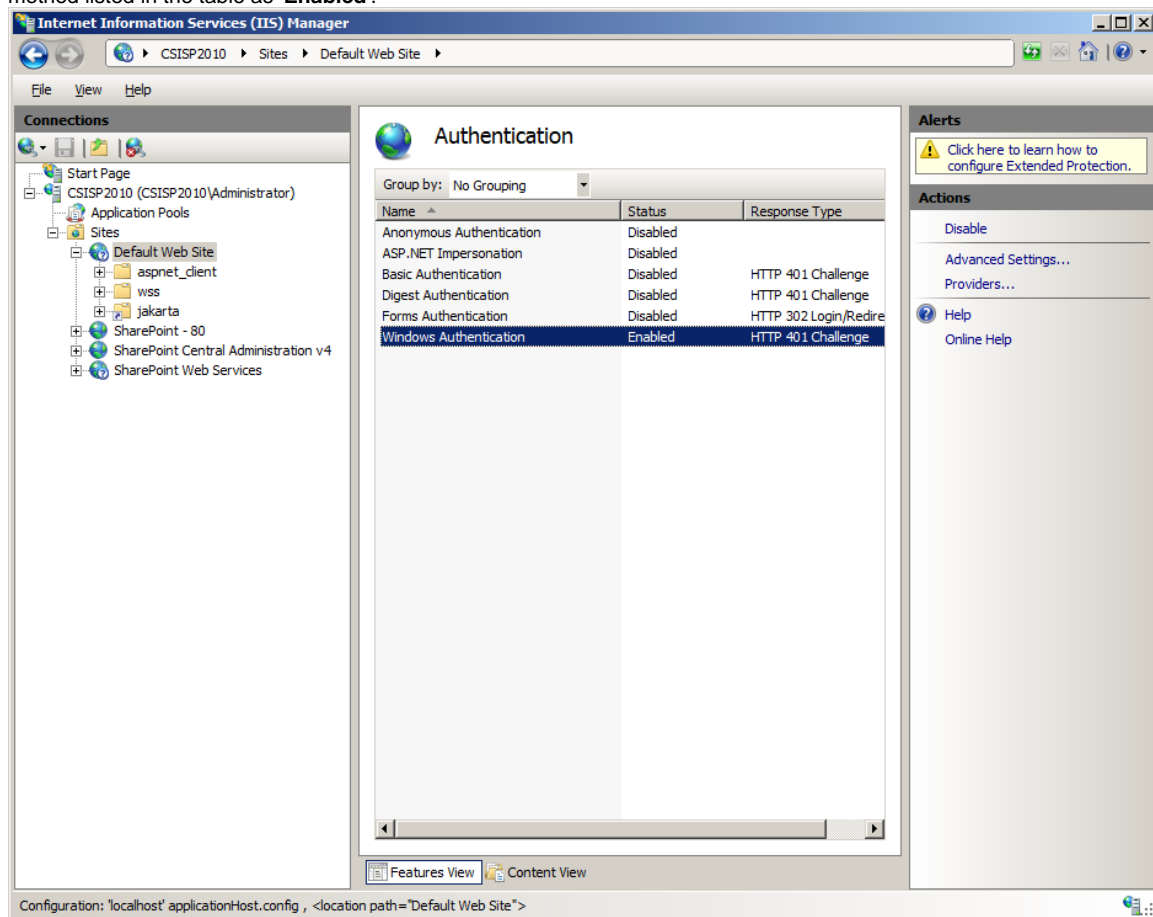


11. Click **'OK'**.

Step 4. Enable Integrated Windows Authentication

This step involves modifying the security of the IIS Web Site to use NTLM or Kerberos authentication.

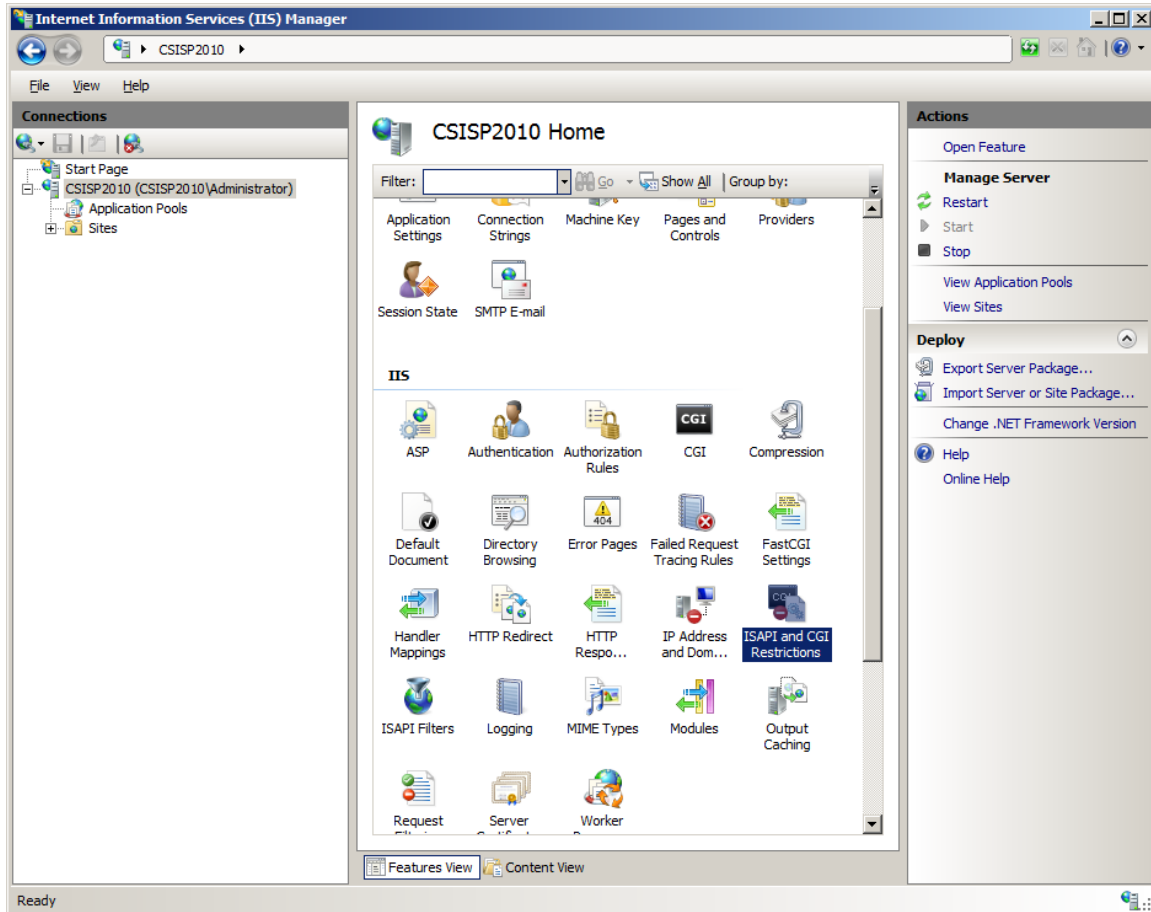
1. Select the IIS Web Site modified in step 3 and double-click the **'Authentication'** icon in **'Features View'**.
2. Use the **'Disable'** and **'Enable'** items in the **'Actions'** panel to ensure that **'Windows Authentication'** is the only authentication method listed in the table as **'Enabled'**.



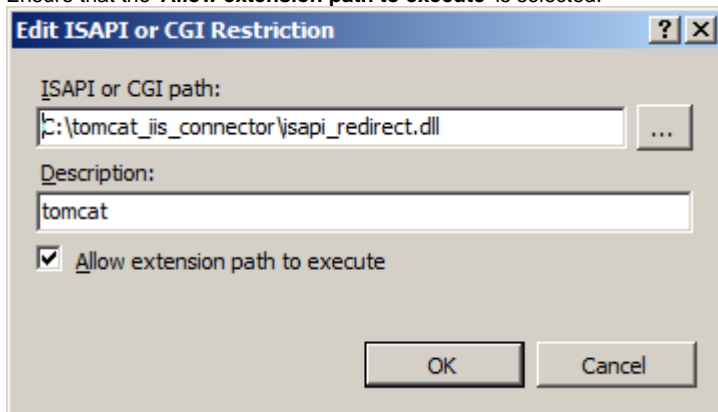
Step 5. Register the ISAPI Extension

Now you will register the `isapi_redirect.dll` as an authorised ISAPI Extension.

1. In the **'Connections'** panel, ensure that the local IIS Server is selected.
2. Double-click the **'ISAPI and CGI Restrictions'** icon in **'Features View'**.



3. Click **Add** in the **Actions** panel.
4. Set the **ISAPI or CGI path** to the `isapi_redirect.dll` you downloaded in step 1.
5. Set the **Description** to `tomcat`.
6. Ensure that the **Allow extension path to execute** is selected.

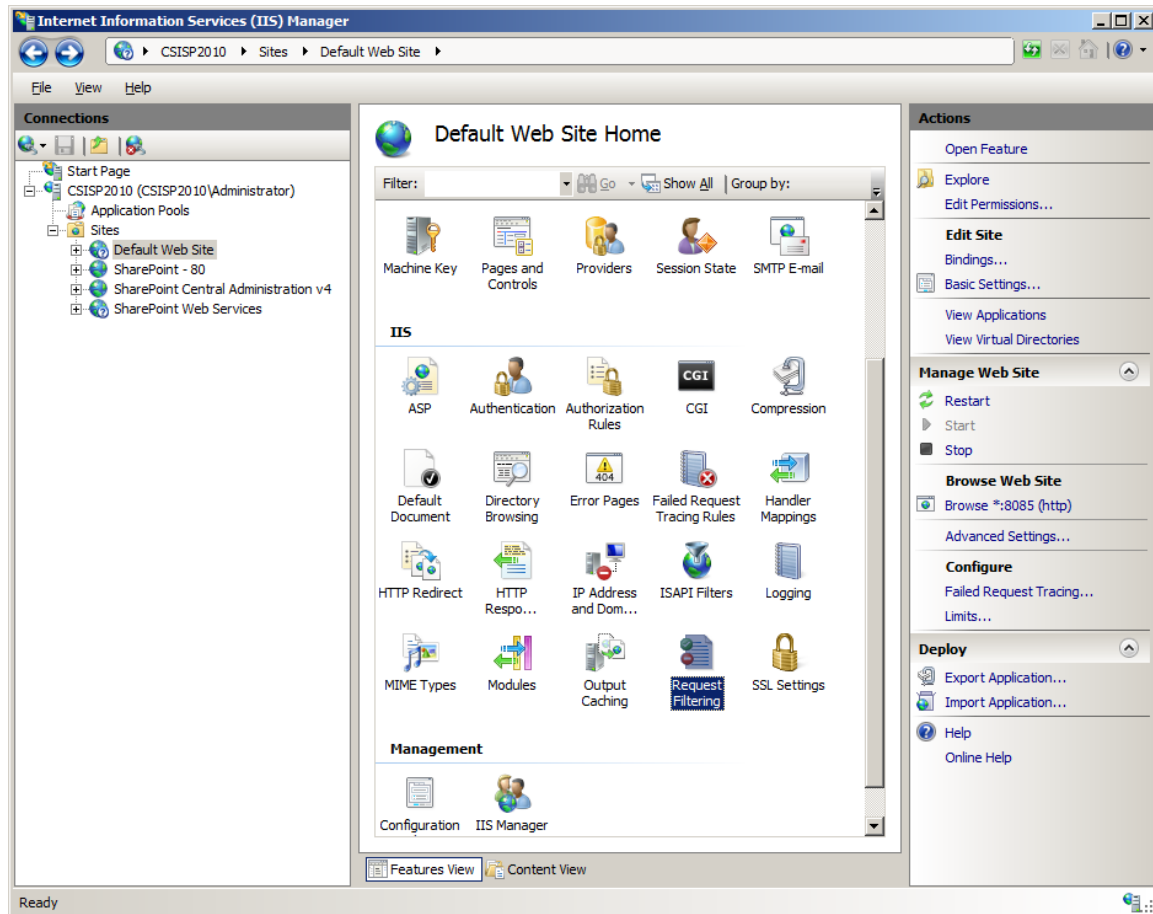


7. Click **OK**.
8. Verify that the new ISAPI restriction is listed in the table with a restriction of **Allowed**.

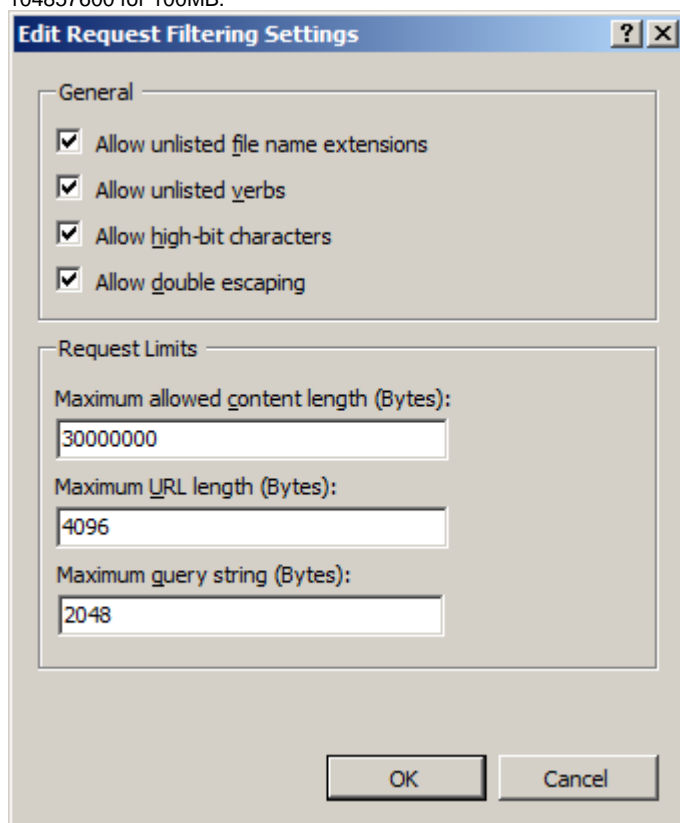
Step 6. Allow Double Escaping

By default, IIS 7 prohibits any URL that contains a " character in the URL from being served. This is referred to as 'double escaping'. In Confluence, any page with a space in the title will be served from a URL with spaces replaced by the "+" sign (such as, 'http://confluence/display/spacekey/This+Page+Has+Spaces+In+The+Title'). You will need to disable this security feature in IIS 7 in order for the ISAPI filter to correctly process any Confluence page URLs.

1. In the **Connections** panel, ensure that the IIS Web Site that will be used to proxy Confluence requests is selected.
2. Double-click the **Request Filtering** icon in **Features View** (If the **Request Filtering** icon is not displayed, you may need to download the IIS [Administration Pack](#) first).



3. Click the **'Edit Feature Settings'** link in the **'Actions'** panel.
4. Ensure that the **'Allow double escaping'** option is selected.
5. Modify "Maximum allowed content length (bytes)" to the maximum size of attachments you want that your installation allows. ie 104857600 for 100MB.



6. Click **'OK'**.

RELATED TOPICS

- [Release Notes](#)

- [Installing the SharePoint Connector](#)
- [Upgrading the SharePoint Connector](#)
- [Applying Specific Confluence Configurations](#)
- [Deploying the SharePoint Connector to More SharePoint Sites](#)

Configuring Confluence to use Jespa for NTLM Authentication

This page is part of the installation guide for the **Confluence SharePoint Connector**. It tells you how to configure access to Confluence using Integrated Windows Authentication via a third-party software package called **Jespa**.



Supportability

This document applies for Sharepoint Connector license holders only. For any Jespa specific issues and support please contact [IOPLEX](#)

On this page:

- [Installation](#)
 - [Step 1. Hook Confluence up to Active Directory](#)
 - [Step 2. Download and Install Jespa](#)
 - [Step 3. Configure Confluence](#)
 - [Step 4. Add Custom Authenticator](#)
 - [Step 5. Set Client Browser Options](#)

Installation

Step 1. Hook Confluence up to Active Directory

Configure Confluence to synchronise its user repository with the Active Directory domain. See the Confluence documentation on [LDAP user management](#).

Step 2. Download and Install Jespa

1. Download the Jespa package from the [IOPlex website](#).
2. Follow the **Installation** instructions in the [Jespa technical documentation](#) to install Jespa into your Confluence web app. Note that you need to follow the full installation guide for Jespa, which includes:
 - a. Creating a computer account in the target Active Directory domain for Jespa to authenticate with.
 - b. Testing your Jespa configuration with the Jespa example application provided.

Step 3. Configure Confluence

1. Copy the Jespa and JCIFS libraries from the Jespa example application into your `$confluence.home/confluence/WEB-INF/lib` directory.
2. Open the `$confluence.home/confluence/WEB-INF/web.xml` file in a text editor, and make the following modifications to the file:
 - a. Locate the section of the file that contains a `<filter>` with a `<filter-name>` set to 'login'. Immediately after this login filter, add a new `<filter>` for Jespa. You should copy the contents of the Jespa `<filter>` in the example application used in step 2, once the example application is able to authenticate correctly. The changed `web.xml` file should look like this:

web.xml	
	<pre> <filter-name>login</filter-name> <filter-class>com.atlassian.seraph.filter.LoginFilter</filter-class> <filter> <filter-name>jespa</filter-name> <filter-class>jespa.http.HttpSecurityFilter</filter-class> <init-param> <param-name>jespa.log.path</param-name> <!-- Enter the path to where you would like the Jespa log to be stored --> <param-value>C:\confluence-data\logs\jespa.log</param-value> </init-param> <init-param> <param-name>jespa.log.level</param-name> <param-value>2</param-value> </init-param> <init-param> <param-name>jespa.bindstr</param-name> <!-- Enter the fully-qualified name of your Active Directory domain --> <param-value>atlassian.com</param-value> </init-param> <init-param> <param-name>jespa.service.acctname</param-name> <!-- Enter the name of the computer account created in Step 2, followed by the '\$' sign, followed by the fully-qualified name of your Active Directory domain --> <param-value>CONFLUENCE\$@atlassian.com</param-value> </init-param> <init-param> <param-name>jespa.service.password</param-name> <!-- Enter the password for the Jespa service account, which was set in Step 2. --> <param-value>JCnckGJHDSd28c7Nc</param-value> </init-param> <!-- Note: also copy over all other default Jespa parameter values from the example web.xml --> </filter>]]> </pre>

- b. Locate the section of the file that contains a **<filter-mapping>** with a **<filter-name>** set to 'login'. Immediately *before* this filter mapping, add a new **<filter-mapping>** for Jespa. The changed web.xml file should look like this:

web.xml	
	<pre> <filter-name>jespa</filter-name> <url-pattern>/*</url-pattern> <filter-mapping> <filter-name>login</filter-name> <url-pattern>/*</url-pattern> </filter-mapping>]]> </pre>

Step 4. Add Custom Authenticator

By default, Confluence will not understand the pre-authenticated requests that come through via the Jespa filter. In order to allow this authentication information to pass through, you must modify the authenticator module used by Confluence.

1. Download the [customauth-0.4.jar](#) file attached to this page and place it in your

2. Edit the %confluence_install%\confluence\WEB-INF\lib directory.
3. Edit the %confluence_install%\WEB-INF\classes\seraph.xml file.
4. Locate the **Authenticator** element and comment it out entirely.
5. Add a new **Authenticator** element that looks like this:

```
<auth>
```

6. Save your changes and close the file.
7. Restart Confluence and ensure that the server initialises successfully.

Step 5. Set Client Browser Options

In order for users to be automatically logged in to Confluence without being prompted for their username and password, the browser must be correctly configured for pass-through authentication.

Please instruct all users to ensure that the [recommended browser settings](#) are applied.

RELATED TOPICS

- [Release Notes](#)
- [Installing the SharePoint Connector](#)
- [Upgrading the SharePoint Connector](#)
- [Applying Specific Confluence Configurations](#)
- [Deploying the SharePoint Connector to More SharePoint Sites](#)

Configuring Confluence to use JCIFS for NTLM Authentication

This page is an addendum to the installation guide for the **Confluence SharePoint Connector**. It has notes on configuring access to Confluence using Integrated Windows Authentication via JCIFS.



JCIFS is not supported. Please use Jespa instead.

This configuration is not supported. We are supplying the instructions because some people are using this configuration, but please note that the JCIFS documentation itself deprecates the configuration. We recommend the use of Jespa instead. See our guide to [configuring Confluence to use Jespa for NTLM authentication](#).

On this page:

- [Overview](#)
 - [About JCIFS](#)
 - [Authentication Methods](#)
 - [Feature Deprecation](#)
- [Installation Notes](#)

Overview

In this configuration both SharePoint and client browsers are authenticated against Confluence using Windows authentication provided by JCIFS, a third-party implementation written in Java.

If you have not already seen our guide to [planning your environment](#), you can refer to it for information that will help you select the best configuration for your environment.

About JCIFS

JCIFS is an Open Source client library that implements the CIFS/SMB networking protocol in 100% Java. CIFS is the standard file-sharing protocol on the Microsoft Windows platform. The JCIFS library also includes a Servlet Filter that allows support for NTLM authentication over HTTP. For more information, visit the [JCIFS website](#).

Authentication Methods

JCIFS supports the following Windows authentication methods:

- LM
- NTLMv1
- NTLM2 Session Security (Maybe?)
- LMv2

Feature Deprecation

This text is taken from the [JCIFS website](#):

IMPORTANT: All HTTP related code and corresponding documentation in JCIFS is not supported, no longer maintained and will be removed because it is broken and obsolete (and because HTTP has nothing to do with CIFS). This page remains only for informational purposes and for legacy users.

The HTTP "filter" in particular uses a "man in the middle" technique that cannot support NTLMv2. Since late 2008, users have started to report that client security policy is requiring NTLMv2 and that this solution no longer works.

For this reason and others described in [this post](#), this feature will be removed from the JCIFS package. Currently we recommend using [Jespa](#) which properly implements NTLMv2 server side authentication and includes an advanced NTLMv2 HTTP SSO Servlet Filter.

Installation Notes

We have tested JCIFS 1.3.14.

1. Download latest jar from <http://jcifs.samba.org/src/> and place in Confluence (`\confluence\WEB-INF\lib`)
2. Add the attached file named "[customauth-0.4.jar](#)" to Confluence (`\confluence\WEB-INF\lib`)



The customauth-0.4.jar is heavily based on the code for the "[Apache custom Seraph authenticator for Confluence](#)"

The configuration for the customauth-0.4.jar is also based on the information related to the "[NTLM Authenticator for Confluence](#)" (particularly the reference to LDAP User Management).

3. Configure Confluence with [LDAP User Management](#)

See the attached "atlassian-user.xml" for an example integration with Active Directory.



[Customising atlassian-user.xml](#) also contains excellent information to help understand how to edit this file.

4. Test access to Confluence using current "Login" page with both Active Directory accounts and non-Active Directory accounts



You will need to configure the Active Directory accounts to have appropriate permissions in Confluence (i.e.: adding to the confluence-users group)

5. Update `\confluence\web-inf\web.xml` to contain additional filter settings to support JCIFS

See [JCIFS NTLM HTTP Authentication](#) for more filter examples.

5a. Add the following filter as the last filter before `<filter-mapping>`

You will need to change the values to match your specific environment.

Filter

```

<filter-name>NtlmHttpFilter</filter-name>
<filter-class>jcifs.http.NtlmHttpFilter</filter-class>

<init-param>
<param-name>jcifs.http.domainController</param-name>
<param-value>PLACE DOMAIN CONTROLLER IP ADDRESS HERE</param-value>
</init-param>

<!--
always needed for preauthentication / SMB signatures
-->
<init-param>
<param-name>jcifs.smb.client.domain</param-name>
<param-value>PLACE DOMAIN NAME HERE (e.g., mydomain.local)</param-value>
</init-param>
<init-param>
<param-name>jcifs.smb.client.username</param-name>
<param-value>PLACE DOMAIN ACCOUNT HERE (do not prefix with
"domain>\" )</domain></param-value>
</init-param>
<init-param>
<param-name>jcifs.smb.client.password</param-name>
<param-value>PLACE DOMAIN PASSWORD HERE</param-value>
</init-param>
]]>

```

5b. Add the following filter-mapping just before the "login" filter-mapping**Filter-Mapping**

```

<filter-name>NtlmHttpFilter</filter-name>
<url-pattern>/*</url-pattern>

]]>

```

6. Set the <authenticator> in the "confluence\WEB-INF\classes\seraph-config.xml" file to the following

```
]]>
```

RELATED TOPICS

- [Release Notes](#)
- [Installing the SharePoint Connector](#)
- [Upgrading the SharePoint Connector](#)
- [Applying Specific Confluence Configurations](#)
- [Deploying the SharePoint Connector to More SharePoint Sites](#)

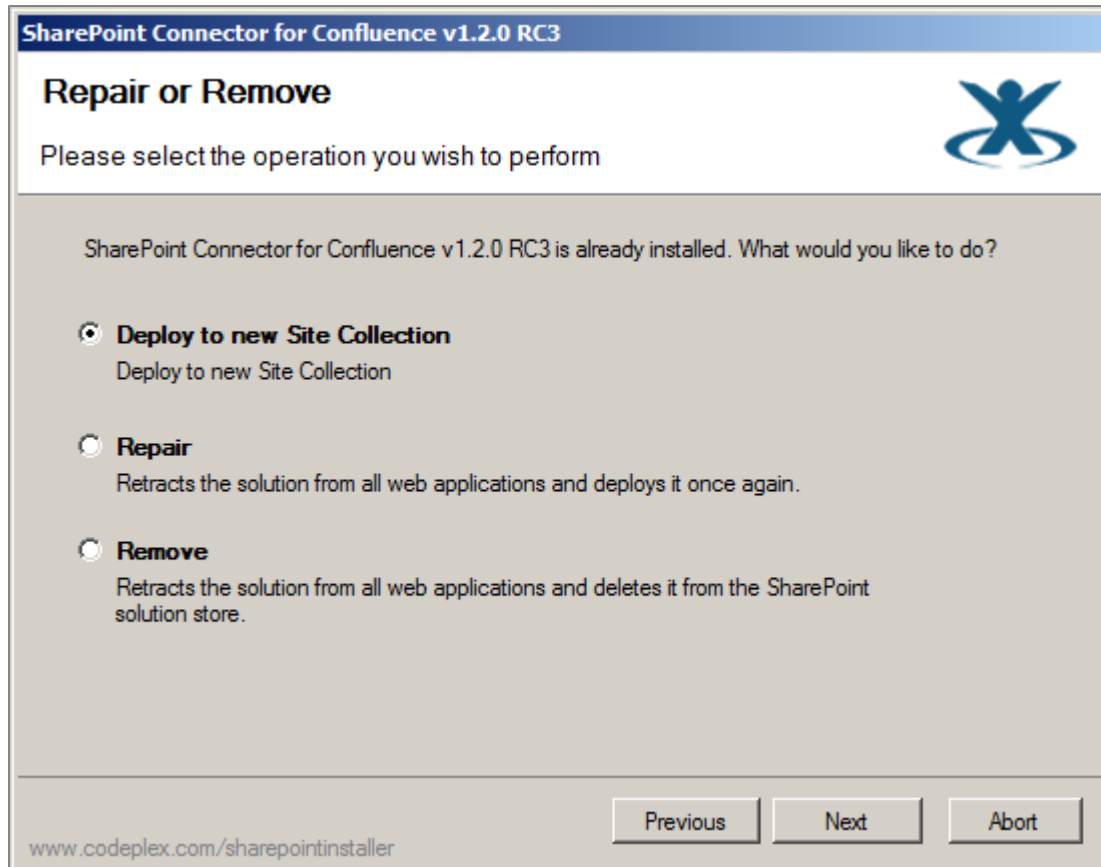
Deploying the SharePoint Connector to More SharePoint Sites

This page tells you how to install the SharePoint Connector onto additional SharePoint site collections, at some time after the initial installation. This page applies to the **SharePoint Connector 1.3**.

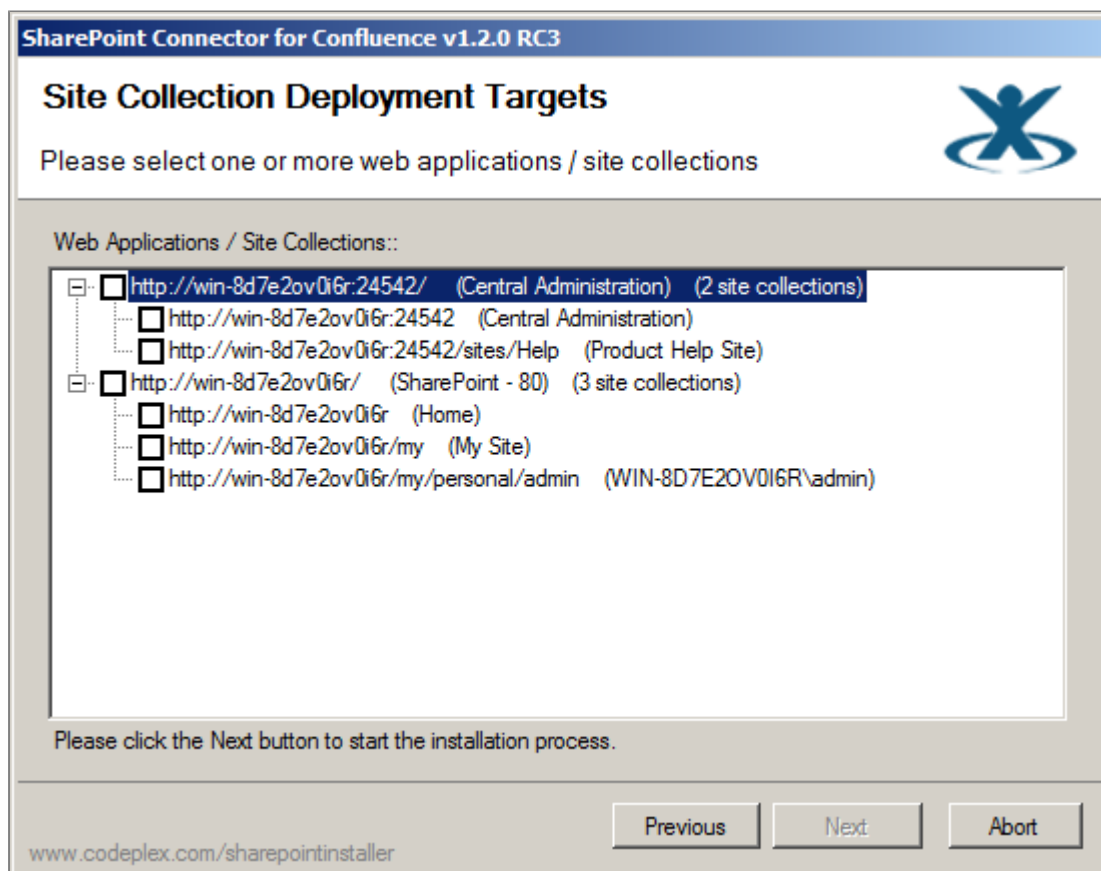
Background information: When you first install the SharePoint Connector into SharePoint, you choose one or more SharePoint site collections where you want the connector deployed. See the installation guides for [SharePoint 2007](#) and for [SharePoint 2010](#). After the initial installation, you can deploy the SharePoint Connector to additional SharePoint site collections at any time, as described below.

To install the SharePoint Connector onto additional SharePoint sites:

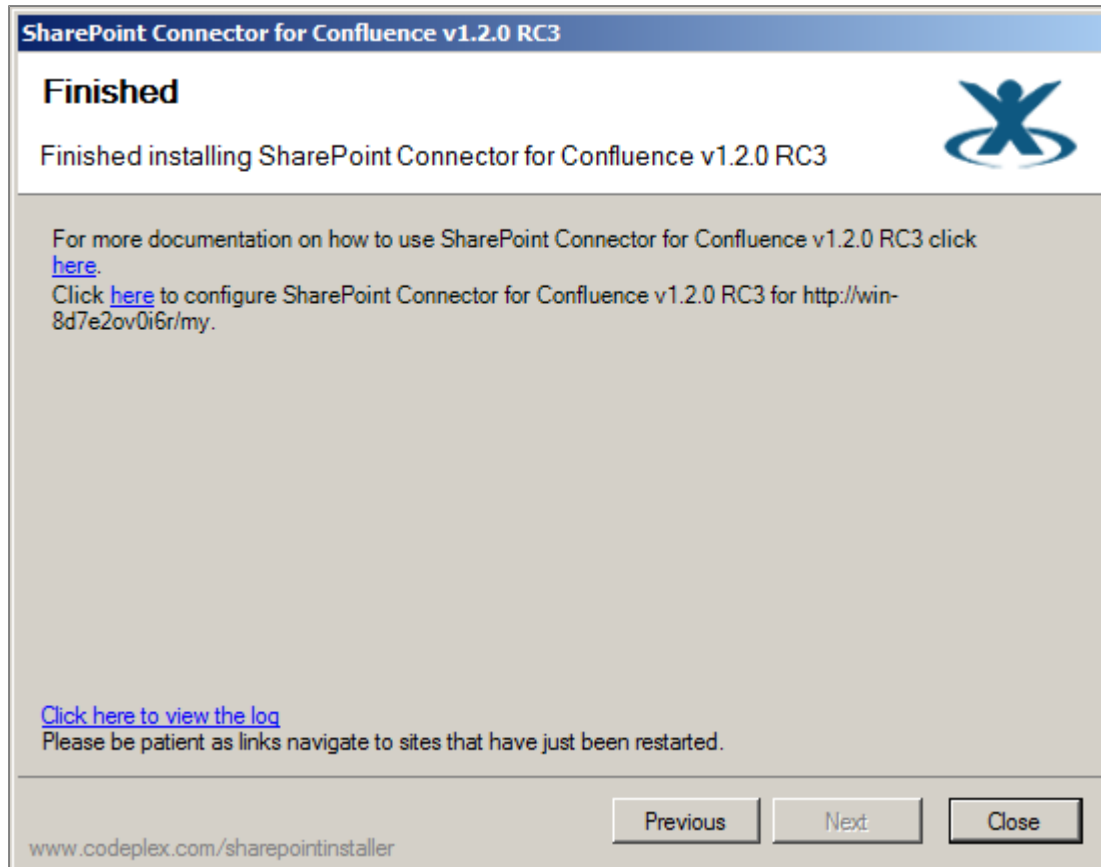
1. Go to your 'SharePoint Installer' directory, where you previously extracted the contents of the downloaded SharePoint Connector zip file. (See the installation guides for [SharePoint 2007](#) and for [SharePoint 2010](#).)
2. Run `Setup_WebParts.exe`. (This is the same executable as the one you ran when you first installed the connector.)
3. Click the **'Next'** button on the welcome screen to start the installation process.
4. The SharePoint web part installer performs a 'System Check' to ensure that all pre-installation and configuration requirements have been met.
 - If all the checks succeed, click **'Next'**.
 - If any of the checks fails, you will need to fix the problem first.
5. The **'Repair or Remove'** screen appears. Select **'Deploy to new Site Collection'** and click **'Next'**.
[Screenshot: Deploying the SharePoint Connector to additional sites](#)



6. The '**Site Collection Deployment Targets**' screen appears. Select the required site collections or applications and click '**Next**'.
Screenshot: Choosing the SharePoint sites



7. The installer will deploy the connector to the selected sites. When complete, the '**Finished**' screen appears.
Screenshot: Deployment complete



RELATED TOPICS

Installing the SharePoint Connector

SharePoint Connector FAQ

- [Comparing SharePoint Versions and Editions](#)
- [Planning your Authentication Configuration](#)
- [NTLM and Anonymous Access](#)
- [Introduction to SharePoint and Confluence Terminology](#)
- [How the SharePoint Connector Manages Permissions](#)
- [Connecting to Multiple SharePoint Sites](#)
- [Manual SharePoint Feature Installation](#)
- [Using the SharePoint Connector with Confluence Clustered](#)
- [Using the SharePoint Connector with a Confluence Starter License](#)

Other resources

See the [general FAQ](#) on the Atlassian website, and the [user forum](#) for the Confluence SharePoint Connector.

Comparing SharePoint Versions and Editions

The **SharePoint Connector 1.2 and later** supports both **SharePoint 2007** and **SharePoint 2010**. Below is summarised information on both versions of SharePoint.

On this page:

- [SharePoint 2007](#)
 - [Versions and Editions of SharePoint 2007](#)
 - [Finding Out Which Version of SharePoint 2007 You Have](#)
 - [Confluence SharePoint Connector Features Supported in SharePoint 2007](#)
- [SharePoint 2010](#)
 - [Versions and Editions of SharePoint 2010](#)
 - [Finding Out Which Version of SharePoint 2010 You Have](#)
 - [Confluence SharePoint Connector Features Supported in SharePoint 2010](#)

SharePoint 2007

Versions and Editions of SharePoint 2007

Microsoft offers two primary versions of SharePoint 2007:

- **Windows SharePoint Services (WSS) v3.** This is the free/unlicensed version of SharePoint that is built upon Windows Server 2003/2008, SQL Server 2000/2005, IIS, ASP.Net 2.0, and .NET 2.0/3.0. All you need is a licensed copy of Windows Server 2003 or Windows Server 2008. There are no other licensing costs unless you want the full-fledged version of SQL Server.
 - Refer to Microsoft's [WSS 3.0](#) page for more information about this product.
 - To download and install WSS 3.0, refer to the [WSS 3.0 download page](#).
 - Be aware that WSS 3.0 is free for Windows Server 2003.
- **Microsoft Office SharePoint Server (MOSS) 2007.** This is the licensed version of SharePoint that is built upon WSS v3. It has two primary versions: MOSS 2007 Standard and MOSS 2007 Enterprise. There are a host of other licensing options as well, such as the ability to use Microsoft Search Server 2008 or Microsoft Search Server 2008 Express with WSS instead of MOSS.
 - To download and install a trial version of MOSS 2007, refer to the [MOSS 2007 Trial download page](#).

For more details on the differences between these versions see the following documents from Microsoft:

- [How to buy Microsoft Office SharePoint Server 2007](#)
- [Microsoft Office SharePoint Server 2007 product comparison download](#)
- [Microsoft Enterprise Search Products Comparison](#)

Finding Out Which Version of SharePoint 2007 You Have

To determine whether you have WSS 3.0 or MOSS 2007 installed, go to Windows **Start -> Control Panel -> Add/Remove Programs**.

- If you see 'Microsoft Office SharePoint Server 2007' in the list, then MOSS 2007 has been installed.
- If you see only 'Microsoft Windows SharePoint Services' in the list (and not 'Microsoft Office SharePoint Server 2007') then you only have WSS 3.0 installed.

Confluence SharePoint Connector Features Supported in SharePoint 2007

To see the SharePoint Connector features available with each edition of SharePoint 2007, refer to our [planning guide](#).

From a user's point of view, the SharePoint Connector features in SharePoint 2007 are exactly the same as in SharePoint 2010.

SharePoint 2010

Versions and Editions of SharePoint 2010

Microsoft offers two primary versions of SharePoint 2010:

- **SharePoint Foundation 2010.** This is the free/unlicensed version of SharePoint. It replaces Windows SharePoint Services (WSS) 2007. SharePoint Foundation is built upon Windows Server 2008, SQL Server 2008, IIS and .NET 3.5. All you need is a licensed copy of Windows Server 2008. There are no other licensing costs unless you want the full-fledged version of SQL Server.
 - Refer to this [TechNet article](#) for more information about SharePoint Foundation 2010.
 - To download and install SharePoint Foundation 2010, refer to the [Microsoft download page](#).
 - Be aware that SharePoint Foundation 2010 is free for Windows Server 2008.
- **Microsoft SharePoint Server 2010.** This is the licensed version of SharePoint, offering a business collaboration platform for the enterprise. It replaces Microsoft Office SharePoint Server (MOSS) 2007.
 - Refer to this [TechNet article](#) for more information about SharePoint Server 2010.
 - To download and install a trial version of SharePoint Server 2010, refer to the [Microsoft download page](#).

For more details on the differences between these versions, see the [Microsoft SharePoint Products home page](#).

Finding Out Which Version of SharePoint 2010 You Have

To determine whether you have SharePoint Foundation 2010 or SharePoint Server 2010 installed, go to Windows **Start -> Control Panel -> Programs -> Programs and Features**.

- If you see 'Microsoft SharePoint Server 2010' in the list, then SharePoint Server 2010 has been installed.
- If you see only 'Microsoft SharePoint Foundation 2010' (and not 'Microsoft SharePoint Server 2010') then you only have SharePoint Foundation 2010 installed.

Confluence SharePoint Connector Features Supported in SharePoint 2010

To see the SharePoint connector features available with each edition of SharePoint 2010, refer to our [planning guide](#).

From a user's point of view, the SharePoint Connector features in SharePoint 2007 are exactly the same as in SharePoint 2010.

Planning your Authentication Configuration

Configuring the authentication setup for Confluence and SharePoint is the most complex aspect of this integration. Please refer to our planning guide and decision flowchart in [Planning your Environment with SP 2007](#).

NTLM and Anonymous Access

NTLM and Anonymous Access Not Supported

There is currently no supported solution that allows anonymous access to Confluence while using NTLM as the authentication method for Confluence.

Unsupported Solutions Will Cause Problems

Some brave souls have suggested the following two solutions, when using [Confluence with IIS](#). Both suggestions are unsupported and both offer problems:

- Use two ports/URLs, one for anonymous users and one for NTLM users.
- Develop a custom redirection page within IIS.

(Not Supported) Using Two Ports and Two Base URLs



Beware! Confluence recognises only one base URL

This approach will cause problems because Confluence cannot recognise 2 base URLs. Therefore you are risking unexpected behaviour from Confluence if you allow access via 2 different ports.

With this approach, you would send all anonymous users to the Tomcat port (for example, 8080) and send all NTLM users to the IIS port. If someone uses the anonymous port and tries to access content that is not available to anonymous users, they will be presented with the Confluence login page. At that point they can enter their Active Directory credentials, and are then using Active Directory integration instead of NTLM.

(Not Supported) Developing a Custom Redirection Page

With this approach everyone uses the IIS URL, and IIS is configured to allow anonymous access. Your development team would need to create a custom solution as follows:

- Create a custom page within IIS. It could be called `login-redirect.aspx` in the root of the IIS web. This page would examine the query string for the name 'os_destination' and perform a redirect to the value of that query string.
- In IIS, configure the above page **not** to allow anonymous access.
- Modify the `confluence\login.vm` file to redirect to the custom page created above (`login-redirect.aspx`). It would pass along the 'os_destination' query string value'.



If you are interested in NTLM and anonymous access, you can track these two issues: [CSI-286](#) and [CSI-287](#)

Introduction to SharePoint and Confluence Terminology

This page contains a beginner's guide to the terms used in Confluence and SharePoint. It is useful for people who know either Confluence or SharePoint, but do not yet have a good understanding of both.

SharePoint Terminology

SharePoint has the following concepts:

- Farm
- Web Application
- Site Collection
- Site

In SharePoint a farm is the top level entity. An enterprise may have a production farm and a development/test farm for their intranet. You typically do not have multiple farms to cover something like an intranet except in circumstances such as regional separation across the globe. The same applies to an extranet or a public facing website. There can be many servers within a farm and they can perform different roles such as a search index server, a web front end server, database servers, etc.

A farm can have multiple web applications. A web application is usually a security boundary since it maps to an IIS web site which can have some added control over access. For example, one web application may allow anonymous access and another may not.

A web application can have multiple site collections. A site collection is simply a collection of sites. It has a single top level site, also called the root site. Each site can have any number of child sites.

You might have a site collection per department or you might have all departments in the same site collection. If you use 'My Sites', you will have a separate site collection per user.

Confluence Terminology

Confluence has the following concepts:

- Installation
- Cluster node
- Space
- Page

An enterprise may have several Confluence installations (similar to SharePoint farms). Each Confluence installation can be hosted in a single server or on several cluster nodes.

A single Confluence installation can have multiple spaces. A space can have multiple pages. The pages can be organised in a hierarchical fashion where one page is the parent of another page.

RELATED TOPICS

[Comparing SharePoint Versions and Editions](#)
[Updating your SharePoint Connector License Details](#)
[Installing the SharePoint Connector](#)

How the SharePoint Connector Manages Permissions

On this page:

- If a user has permission to view a SharePoint site, but they do not have permission to view a Confluence space, will they be able to see content from that Confluence space in a web part of the SharePoint site?
- Will Sharepoint site permissions be respected in integrated search? How does it work the other way, searching in Sharepoint for content that is in Confluence?

If a user has permission to view a SharePoint site, but they do not have permission to view a Confluence space, will they be able to see content from that Confluence space in a web part of the SharePoint site?

When embedding Confluence content in SharePoint: The SharePoint Connector always checks the permissions of the user currently logged in to SharePoint before displaying the Confluence content. The user requires 'view' permission in Confluence in order to see the content of the web part, and the Confluence page's 'Edit' is disabled if the user does not have 'edit' permission in Confluence.

When embedding SharePoint content in Confluence: List security and row security is checked before rendering a SharePoint List macro provided that the 'Enable sp-list permission trimming' option is enabled in Confluence on the 'SharePoint Integration Administration' screen.

Will Sharepoint site permissions be respected in integrated search? How does it work the other way, searching in Sharepoint for content that is in Confluence?

If you want to search content in both Confluence and Sharepoint, the SharePoint Connector's Federated Search is the solution. The Federated Search web part also ensures that the correct user-level security is applied to any search results returned from Confluence.

RELATED TOPICS

[Installing and Configuring the Confluence Plugins for SP 2007](#)
[Installing and Configuring the Confluence Plugins for SP 2010](#)
[Configuring the SharePoint Federated Search on SP 2007](#)
[Configuring the SharePoint Federated Search on SP 2010](#)

Connecting to Multiple SharePoint Sites

A single SharePoint Connector license can be used to connect a single Confluence instance to multiple SharePoint sites. Refer to the following documentation for full details:

- [Installing and Configuring the Confluence Plugins for SP 2010](#)
- [Installing and Configuring the Confluence Plugins for SP 2007](#)

Manual SharePoint Feature Installation

If you have trouble running the SharePoint Installer for the SharePoint Connector for Confluence, you can try to install it manually instead.

The SharePoint Installer comes with several files:

- Atlassian.Confluence.SharePoint.Version2007.wsp
- Atlassian.Confluence.SharePoint.Version2010.wsp
- EULA.rtf
- MsiBanner.bmp
- Release Notes.txt
- Setup_WebParts.exe
- Setup_WebParts.exe.config

The automatic install is done through the executable file, **Setup_WebParts.exe**, which requires all of the files listed above to present in the same directory. To do a manual install, you only need the wsp file appropriate for your version of SharePoint. For SharePoint 2007 (including Windows SharePoint Services 3.0), you need the **Atlassian.Confluence.SharePoint2007.wsp** file. For SharePoint 2010, you need to the **Atlassian.Confluence.SharePoint2010.wsp**. A WSP file is a [Solution Package](#) which contains everything SharePoint needs for the installation. Unfortunately, installing a WSP through SharePoint is a little tedious, which is why we have used the [SharePoint Solution Installer](#) to ease the installation experience. However, if you are having problems using the installer provided, the steps are below.



If you choose to do a manual install because of a problem with the automated install, please post an entry on the [Forum](#) to let us know what problems you had with the automated install and if the manual install helped.

Manual Installation Steps for SharePoint 2010.

Step 1: Add Solution to SharePoint Farm

1. Log in to a SharePoint server in your farm as a SharePoint farm administrator.
2. Run the following command from a Windows command prompt:

```
\Atlassian.Confluence.SharePoint2010.wsp"
]]>
```

Step 2: Deploy Solution to Web Application(s)

1. Open **SharePoint 2010 Central Administration** from the Start menu under **Microsoft SharePoint 2010 Products**.
2. Click on the **System Settings** menu item in SharePoint 2010 Central Administration.
3. Click on the **Manage Farm Solutions** link.
4. Click on **atlassian.confluence.sharepoint2010.wsp**.
5. Click on the **Deploy Solution** link.
6. Select the **Now** option under **Choose when to deploy the solution:**.
7. Select which web application you would like to deploy the solution under **Choose a web application to deploy this solution:**.
8. Click **OK**.

Step 3: Activate Solution for Web Application(s)

1. Load the Site Collection Features administration page for the site collection hosted in the web application that the solution was deployed to in Step 2. For example, if your site collection is located at <http://sharepoint/mysite> then go to http://sharepointserver/mysite/_layouts/ManageFeatures.aspx?Scope=Site
2. Locate the row titled **Confluence Integration** and click on the **Activate** button next to it.

Step 4: Configure the SharePoint Connector for Confluence

1. Follow the steps in the installation guide to [Install and Configure the SharePoint Feature on SharePoint 2010](#).

Manual Un-Install Steps for SharePoint 2010

1. Log in to a SharePoint server in your farm as a SharePoint farm administrator.
2. Ensure that the SharePoint 2010 Administrative Service is running by running the following command from a Windows Command Prompt:

3. Open **SharePoint 2010 Central Administration** from the Start menu under **Microsoft SharePoint 2010 Products**.
4. Click on the **System Settings** menu item in SharePoint 2010 Central Administration.
5. Click on the **Manage Farm Solutions** link.
6. Click on **atlassian.confluence.sharepoint2010.wsp**.
7. Click on the **Retract Solution** link.
8. Select the **Now** option under **Choose when to deploy the solution:**.
9. Select which web application you would like to retract the solution from under **Choose a Web application to retract this solution:**.
10. Click **OK**.

Manual Installation Steps for SharePoint 2007

- Log in to a SharePoint server on your farm as a SharePoint farm administrator.
- Open a command prompt (Start->Run then type "cmd") and do the following:
 - Navigate to "Bin" directory within your SharePoint installation (eg. "C:\Program Files\Common Files\Microsoft Shared\Web Server Extensions\12\BIN" for SharePoint 2007 and "C:\Program Files\Common Files\Microsoft Shared\Web Server Extensions\14\BIN" for SharePoint 2010).
 - Type the following command:

```
\Atlassian.Confluence.SharePoint.wsp" ]]>
```

- Open SharePoint 3.0 Central Administration (under Start->Administrative Tools).
 - Navigate to Operations->Solution Management.

- Click on "atlassian.confluence.sharepoint.wsp".
 - Click the "Deploy Solution" link.
 - Choose where to deploy this solution (e.g., "All content Web applications" or a particular web application).
 - Click OK.
 - Repeat the 3 steps immediately above if you did not choose "All content Web applications" and you want to deploy it to other web applications.
- (Optional) Click on "atlassian.confluence.sharepoint.search.wsp" if applicable and click the OK button.
- Open a browser to a SharePoint site collection where you deployed "atlassian.confluence.sharepoint.wsp".
 - Log in as a site collection administrator if you are not already logged in as one.
 - Navigate to Site Settings (Site Action->Site Settings or Site Action->Modify All Site Settings->Site Settings).
 - Click "Site collection features" under the "Site Collection Administration group".
 - If you don't see the group you are not logged in as a site collection administrator.
 - If you only see a "Go to top level site settings" link under the group then you are not at the top level site - click this link to get there.
 - Activate the "Confluence Integration" feature if it is not already activated.
- Follow the instructions for [Configuring the SharePoint Web Part on SP 2007](#) and optionally [Configuring the SharePoint Federated Search on SP 2007](#).

Manual Un-Install Steps for SharePoint 2007

- Log into a SharePoint server on your farm as a SharePoint farm administrator.
- Open SharePoint 3.0 Central Administration (under Start->Administrative Tools).
 - Navigate to Operations->Solution Management.
 - Click on "atlassian.confluence.sharepoint.wsp".
 - Click Retract Solution.
 - Click OK.
 - Wait a minute or so and refresh your browser until you see "Not Deployed" for the solution.
 - Click on "atlassian.confluence.sharepoint.wsp".
 - Click Remove Solution and OK.

Using the SharePoint Connector with Confluence Clustered

When clustering Confluence, a SharePoint Connector license is required for each Confluence clustered node.

Using the SharePoint Connector with a Confluence Starter License

The SharePoint Connector is not compatible with the Confluence Starter License. The SharePoint Connector license that you purchase must match the corresponding Confluence license. Because we do not offer a starter licence for the SharePoint Connector, the SharePoint Connector will not recognise a Confluence Starter Licence.

As a result, you will see a message like this if you are using a Confluence Starter License:

```
com.atlassian.confluence.extra.sharepoint.licensing.LicenseException: Didn't recognize Confluence
license type (Confluence: Starter). Another type needs to be added to the SharePoint Plugin.
```

As a workaround, you can get the SharePoint Connector going with an evaluation license. This kind of license will work with a Confluence Starter License.

Documentation under Review



This section of the SharePoint Connector documentation is under review.

- [SharePoint Connector FAQ under review](#)

SharePoint Connector FAQ under review

- What versions of Active Directory are supported as part of the SSO configuration? AD 2000 / 2003?
- Is SSO handled through an open source module?
- What is the support policy for the Confluence NTLM Authenticator - the plugin which Confluence uses to authenticate users with NTLM?
- What is the support policy?
- Does NTLM authentication work today?
- I've heard about performance issues with the Confluence NTLM authenticator. Where can I track the progress being made against those issues?
- What is the roadmap for single sign-on with respect to AD and MOSS?
- When is Kerberos going to be supported as a SSO method?
- Why won't my web part show any data?
- Why do I have to log in to Confluence when clicking a Confluence link from SharePoint within a web part provided by the SharePoint

Connector for Confluence?

- Why do my images within the Confluence Page web part show as broken images?
- When I click on a link to Confluence from a SharePoint web part, the link takes me to a page that does not exist.
- Is SSL supported?
- Why am I sometimes getting login failed in the SharePoint "Confluence Settings" or on my Confluence Page web parts?
- I cannot successfully execute "Update SharePoint Config Settings" when testing the configuration from Confluence to SharePoint ("SharePoint Admin" screen). What could be the problem?
- I just changed the theme of my space in Confluence, but it isn't reflected in the Confluence Page web parts. Why is that?
- I just set the Confluence space and Page information for the Confluence Page web part, but the web part title is not showing up correctly. Why is that?
- I am authenticating users in Confluence with Active Directory and I have "authorized" users in the "Domain Users" Active Directory group to be able to access/participate in a specific Confluence space. However, the members of "Domain Users" do not appear to have access. Why is this?
- Do the servers need to be on the same network Subnet? Any requirements as far as domain names or computer names?
- Does the screen always have the Sharepoint / Confluence tabs at the top so users can navigate back and forth? What happens in a user changes the theme on a space? Does that affect navigation back and forth?
- Is single sign on available as web based (ie cookie or token oriented) or is it only NTLM? If only NTLM what about Mac users or Firefox?
- Does it change anything about group management? If I need to add a user to a group, do I have to do it in both systems?
- Do space permissions have any overlap or combined functionality with Sharepoint permissions?
- Which system's user profile information will be used?
- Other resources

What versions of Active Directory are supported as part of the SSO configuration? AD 2000 / 2003?

The SharePoint Connector has been developed and tested with ActiveDirectory 2003, but Active Directory 2000 should work also. If you find any incompatibilities, then please let us know.

Is SSO handled through an open source module?

When a user access SharePoint they are authenticated using Windows Integrated Security which could be using NTLM, Kerberos or something else. When a user access Confluence using Internet Explorer they are authenticated using NTLM if it is available. If NTLM is unavailable because of using a different browser or operating system Confluence will prompt for a user name / password. The credentials will then be checked against Active Directory.

What is the support policy for the Confluence NTLM Authenticator - the plugin which Confluence uses to authenticate users with NTLM?

The Confluence NTLM authenticator is a third-party contribution and is not currently supported by Atlassian. See [Planning your Environment with SP 2007](#) for supported configurations.

What is the support policy?

The SharePoint Connector for Confluence is supported by Atlassian. If you have questions or issues, please file them in the Confluence project on <http://support.atlassian.com>. The [SharePoint Connector forum](#) will also remain active, and can be a valuable resource for getting help with the Connector.

Does NTLM authentication work today?

Yes. See [Supported NTLM Authentication with the SharePoint Connector] for more information.

I've heard about performance issues with the Confluence NTLM authenticator. Where can I track the progress being made against those issues?

This issue [can be tracked here](#)

What is the roadmap for single sign-on with respect to AD and MOSS?

Currently the SharePoint Connector is developed and tested using ActiveDirectory 2003 and MOSS 2007. No other versions of those products have been tested so far. Some features of the SharePoint connector also work with WSS.

When is Kerberos going to be supported as a SSO method?

There are no plans to support kerberos at this time. It is a possibility for the future.

Why won't my web part show any data?

There are several potential reasons why you cannot see data.

- The SharePoint server needs access to the Confluence server. Therefore Confluence must be running and the Confluence Settings page must have the appropriate URL to Confluence.
- In order for SharePoint to show Confluence content, it needs to use the Confluence SOAP Permission Checker Plugin to communicate. Go to the Plugin Manager to ensure it is installed and enabled. You can download it from the Plugin Repository.
- If you are not using SSO, the logged in user account in SharePoint must exist as an account within Confluence. Therefore, if your

Active Directory account used by SharePoint is MY_DOMAIN\my_user_name, then a Confluence account named my_user_name must exist in Confluence (or Confluence must be tied to Active Directory) and that user must have read access to the space/page you are trying to display in SharePoint.

- If all else fails, you can try some [troubleshooting steps](#) such as enabling tracing.

Why do I have to log in to Confluence when clicking a Confluence link from SharePoint within a web part provided by the SharePoint Connector for Confluence?

If you are not using Single Sign-on (SSO) and SharePoint is using Windows Integrated Security while Confluence is using Forms Based Authentication, this will always occur unless you have Confluence "remember my login on this computer". If you are using SSO this can be prevented by following the [recommended browser settings](#).

Why do my images within the Confluence Page web part show as broken images?

See [Images Are Broken in the Confluence Page Web Part in SharePoint](#).

When I click on a link to Confluence from a SharePoint web part, the link takes me to a page that does not exist.

Assuming the page really does exist, a likely problem is that the **Server Base Url** is not specified properly on the General Configuration administration page within Confluence. For example, if Confluence is not configured at the root of the domain (e.g., <http://confluence.mycompany.com/confluence> instead of <http://www.mycompany.com>) the **Server Base Url** needs to reflect that or links in web parts will have the incorrect values.

Is SSL supported?

Yes.

The SharePoint features (web parts, search) can access Confluence if it is running under SSL.

To learn more about this and how to configure SSL, see [Secure Sockets Layer \(SSL\) Configuration](#).

The SharePoint plugin within Confluence also supports SSL on SharePoint. You need only [configure your container to connect to SSL services](#). In most cases this just involves adding the SSL certificate from the SharePoint server to the keystore maintained by your Java VM and then specifying `http*s*://yourserver` as the way to reach your SharePoint server in the plugin's configuration.

Why am I sometimes getting login failed in the SharePoint "Confluence Settings" or on my Confluence Page web parts?

If you are not using the SSO option, you must specify a Confluence administrative username and password in the Confluence Settings page within SharePoint. The password is encrypted using a key specified in the <machinekey> setting in the web.config file for each Web Front End (WFE) within your SharePoint farm. SharePoint tries to make sure that the machine key is identical for each WFE, but if they are not, you will get the following error:

```
com.atlassian.confluence.rpc.AuthenticationFailedException: Attempt to login user '<administrative user account>' failed - incorrect password.
```

If this problem occurs, make sure all WFEs have the same machine key and do an IISRESET on each WFE for any that you change. You may then have to re-save the administrative password on the Confluence Settings page if the machine key you decided to use on each WFE does not match the machine key used to save the password in the first place.

I cannot successfully execute "Update SharePoint Config Settings" when testing the configuration from Confluence to SharePoint ("SharePoint Admin" screen). What could be the problem?

This problem recently occurred and did not present an obvious solution. The problem was resolved by resetting the default security template on the SharePoint server (see Method 1 as listed under <http://support.microsoft.com/kb/903071>).

Here are some other things to review if the default security template does not turn out to be the issue.

- Check all items listed in the [SharePoint Plugin Configuration Troubleshooting](#) page
- Make sure IIS Directory Security for the SharePoint web application is set to Windows Authentication
- SharePoint Central Administration is set to NTLM and not Negotiate/Kerberos
- Check Local Security Policy (Group policy) to make sure both the client/server are using consistent NTLM/LM formats see "Network security: LAN Manager authentication level" under Security Options

I just changed the theme of my space in Confluence, but it isn't reflected in the Confluence Page web parts. Why is that?

The CSS for a space is cached by SharePoint. The cache is set to expire after one hour. The new theme should be reflected in Confluence Page web parts within an hour of the change. Performing an IISRESET on SharePoint server(s) is currently the only way to expedite the process.

I just set the Confluence space and Page information for the Confluence Page web part, but the web part title is not showing up correctly. Why is that?

The configured Confluence service user does not have permission to access the page. Make sure the service user (set in the 'Confluence Settings' screen for the current SharePoint website) has appropriate permissions in Confluence.

I am authenticating users in Confluence with Active Directory and I have "authorized" users in the "Domain Users" Active Directory group to be able to access/participate in a specific Confluence space. However, the members of "Domain Users" do not appear to have access. Why is this?

This appears to be a bug with Confluence integration with Active Directory. [CSI-206](#) in Jira captures the issue. To work around the issue, try placing the "authorized" users in an Active Domain group that does not contain spaces in the name (ex: Confluence).

Do the servers need to be on the same network Subnet? Any requirements as far as domain names or computer names?

The servers can be on different network subnets (with the following exceptions in effect - based on the environments we have tested)

- For Active Directory integration with NTLM to work properly, both the Confluence server and the SharePoint server should be part of the same domain
- If Active Directory is not used as a Confluence user repository, then the suggestion would be to use the Microsoft Single Sign-on Service (option "Using the internal Confluence user store" as defined in <http://confluence.atlassian.com/display/CONFEXT/Authentication+Configuration>)

Does the screen always have the Sharepoint / Confluence tabs at the top so users can navigate back and forth? What happens in a user changes the theme on a space? Does that affect navigation back and forth?

The 2.7/2.8 SharePoint decorators are used to add the "SharePoint" link to the top left corner. If the user changes the theme to something other than the 2.7/2.8 SharePoint decorator, the "SharePoint" link will be removed, but navigation between Confluence/SharePoint environments will not be affected.

Is single sign on available as web based (ie cookie or token oriented) or is it only NTLM? If only NTLM what about Mac users or Firefox?

- For Firefox users, please see the following link that describes specific browser settings to use for NTLM. <http://confluence.atlassian.com/display/CONFEXT/Recommended+Browser+Settings>
- If Active Directory and NTLM is not available or desired for Confluence, then the suggestion would be to use the Microsoft Single Sign-on Service (option "Using the internal Confluence user store" as defined in <http://confluence.atlassian.com/display/CONFEXT/Authentication+Configuration>). Note, the Single Sign-on Service option has a dependency on MOSS.

Does it change anything about group management? If I need to add a user to a group, do I have to do it in both systems?

It depends...

- If Active Directory is used for both products, then you may need to add an Active Directory user to Confluence/Confluence space. If you have an Active Directory domain group (with no spaces in the name - see Jira Item # ?) that contains all users that will access Confluence, you can assign the group once to Confluence and again once per space.
- If Active Directory is used for SharePoint only and Confluence is using a separate user repository, then yes, you will need to configure a user independently in both products.

Do space permissions have any overlap or combined functionality with Sharepoint permissions?

There really is no overlap. We have implemented permission checking from both sides (Confluence to SharePoint; SharePoint to Confluence) to help control a specific user from having inappropriate access to something.

Which system's user profile information will be used?

User profile will come from Active Directory (if used for either system). SharePoint will typically be configured to use Active Directory. If Confluence is configured to use another user repository, then Confluence will show user profile information from the respective user repository and SharePoint will show user profile information from Active Directory. Other than the above, the Confluence profile is not connected to the SharePoint profile.

Other resources

See the [General FAQ](#) on the Atlassian website, and the [User Forums](#) for the SharePoint Connector for Confluence.

Contributing to the SharePoint Connector Documentation

Would you like to share your SharePoint Connector hints, tips and techniques with us and with other SharePoint Connector users? We welcome your contributions. Have you found a mistake in the documentation, or do you have a small addition that would be so easy to add yourself rather than asking us to do it? You can update the documentation page directly.

Getting Permission to Update the Documentation

Our documentation wiki contains developer-focused documentation (such as API guides, plugin and gadget development guides and guides

to other frameworks) as well as product documentation (user's guides, administrator's guides and installation guides). The wiki permissions are different for each type of documentation.

- If you want to update the [Developer Network](#) or other developer-focused wiki spaces, just sign up for a wiki username then log in and make the change.
- If you want to update the [SharePoint Connector product documentation](#), we ask you to sign the Atlassian Contributor License Agreement (ACLA) before we grant you wiki permissions to update the documentation space. Please read the [ACLA](#) to see the terms of the agreement and the documentation it covers. Then sign and submit the agreement as described on the form attached to that page.

Following our Style Guide

Please read our short [guidelines for authors](#).

How we Manage Community Updates

Here is a quick guide to how we manage community contributions to our documentation and the copyright that applies to the documentation:

- **Monitoring by technical writers.** The Atlassian technical writers monitor the updates to the documentation spaces, using RSS feeds and watching the spaces. If someone makes an update that needs some attention from us, will make the necessary changes.
- **Wiki permissions.** We use wiki permissions to determine who can edit the various types of documentation spaces.
 - Developer documentation (API guides, plugin development and gadget development): Anyone can edit these spaces, provided they have signed up for a wiki username and logged in to the wiki.
 - Product documentation (user's guides, administrator's guides, installation guides): We ask people to sign the [Atlassian Contributor License Agreement](#) (ACLA) and submit it to us. That allows us to verify that the applicant is a real person. Then we give them permission to update the documentation.
- **Copyright.** The Atlassian documentation is published under a Creative Commons 'cc-by' license. Specifically, we use a [Creative Commons Attribution 2.5 Australia License](#). This means that anyone can copy, distribute and adapt our documentation provided they acknowledge the source of the documentation. The cc-by license is shown in the footer of every page, so that anyone who contributes to our documentation knows that their contribution falls under the same copyright.

RELATED TOPICS

[Contributing to the Confluence Documentation](#)
[Author Guidelines](#)
[Atlassian Contributor License Agreement](#)