Jv Jive Interactive Intranet

9.x Administrator Guide

Jive for SharePoint 2010

Aurea

Unlimited Possibility

Notices

For details, see the following topics:

- Notices
- Third-party acknowledgments

Notices

Third-party acknowledgments

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

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

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

Table of Contents

Aurea global support

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

- Search the articles on the Aurea Knowledge Base for solutions to your issues.

- Search the product documentation and other product-related information that are also available on Support Central.

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

You can also find the setup files on Support Portal.

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

1

Jive for SharePoint On-Prem overview

Documents uploaded to SharePoint 2010 v4, as uploaded documents to a Jive group, will be available for preview in Jive. You can easily move between the Jive site and SharePoint storage so that you can leverage Jive's rich social functionality (with likes, comments, shares, badges and so on) as well as SharePoint's robust document management functionality.

Jive for SharePoint 2010 v4 lets you synchronize a SharePoint site collection with a Jive place.

For details, see the following topics:

- System requirements
- Supported browsers
- Network architecture
- Informational architecture

System requirements

Here you can find the system requirements for installing Jive for SharePoint 2010 v4 add-on.

Jive-side requirements

- Jive 9.x
- Jive for SharePoint 2010 v4 add-on

Microsoft-side requirements

- SharePoint 2010 and accounts for all participating users
- If you want to see SharePoint content in Jive using the Office 365 preview instead of the Jive native preview, Office Web Apps Server must be installed, and SharePoint needs to be configured to use it.

Supported browsers

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

- Microsoft Edge* (Chromium-based).
- Apple Safari 8 and 9 (on Macs only).
- Mobile Safari on iPhone and iPad for iOS 8 and 9 and later. (For a browser-independent native iOS phone app, be sure to look for the Jive Daily Hosted app, if your community uses it, in the App Store.)
- Mobile Chrome on Android devices for Android 4.4 and later. (For a browser-independent native Android phone app, be sure to look for the Jive Daily Hosted app, if your community uses it, in Google Play.)
- Mozilla Firefox*.
- Google Chrome*.

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

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

Important notes and restrictions

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

Network architecture

Here you can find the descriptions of the connection workflow between Jive and SharePoint.

The following diagrams show the network layout for Jive for SharePoint On-Prem v4 in On Premise or Hosted environments:

Jive for SharePoint 2013 v4 – on Prem
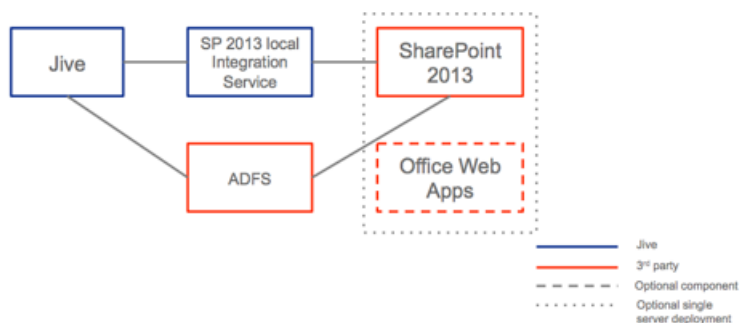
Jive for SharePoint 2013 v4 – Hosted
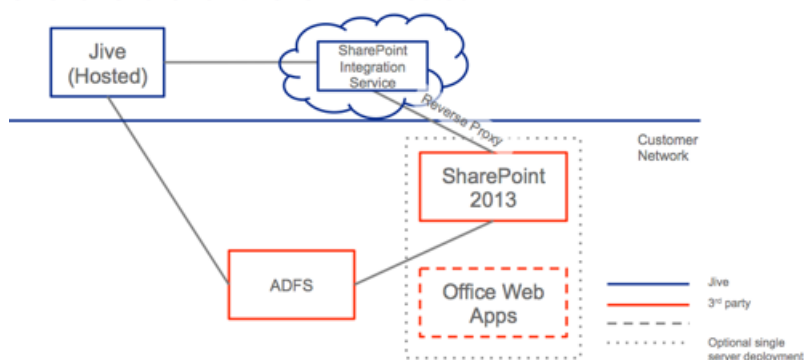
Informational architecture

Jive for SharePoint add-on's main functionality is connecting a Jive place to a SharePoint site.

The following list shows a hierarchy of objects within SharePoint:

SharePoint Tenant

- Site collection
    - Site
        - Document Library

In Jive, spaces and projects have hierarchical relationships, but groups do not.

Any space, group, or project you create in Jive can be mapped to a SharePoint Team site and will automatically contain a document library named Jive Documents, where documents created in Jive will be stored.

However, you can modify the hierarchy below the site level (only) on the SharePoint side without disturbing the linkage between the Jive place and the SharePoint site, including the following:

- Adding additional levels of hierarchy under the Jive Documents document library

- Adding other non-Jive-linked libraries that are not stored under Jive Documents

Note that only files you place in the Jive Documents document library below the level of the Jive-linked site will be synchronized into Jive. Files you create in Jive after you add hierarchy will continue to be created at the root level of the Jive Documents library. You can move them into sub-levels under Jive Documents from the SharePoint side, and they will continue to be synchronized from both directions.

The following diagram shows an example of more complex linkages between Jive places and SharePoint sites. Note that all Jive places map to the Jive Documents document library under the specific SharePoint site.
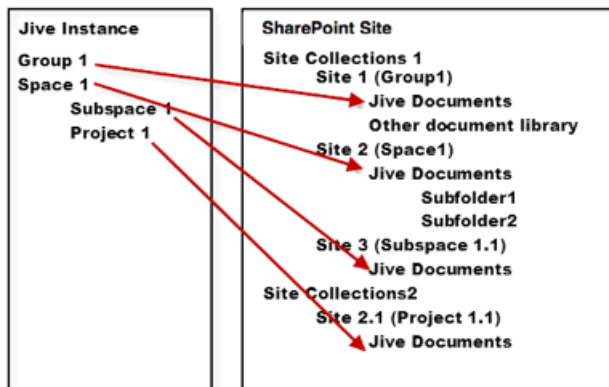
Note: Currently, the only supported configuration is a newly created Jive place that automatically creates a SharePoint site in the site collection you specify.

2

Administering Jive for SharePoint

Once you install the Jive for SharePoint add-on and set it up, users can create places using Jive for SharePoint as the external file storage as shown in the following image.

For details, see the following topics:

- Installation prerequisites
- Setting up permissions
- Installing SharePoint integration add-on
- Configuring Jive for SharePoint connections
- Creating and configuring storage instances
- Completing user mapping
- SharePoint connection settings
- Creating places linked to SharePoint
- Disconnecting your place from SharePoint

Installation prerequisites

There are a few prerequisites that you need to complete for SharePoint before installing the Jive for SharePoint 2010/2013 add-on in Jive.

You should complete the following tasks before installing Jive for SharePoint 2010/2013 add-on:

1. Decide whether you're going to use Claims via ADFS or NTLM protocol for user authentication. For more information, see Plan for user authentication methods

in SharePoint Server on Microsoft portal at https://docs.microsoft.com/en-us/SharePoint/security-for-sharepoint-server/plan-user-authentication.

2. If you are using Claims via ADFS for user authentication, you should do the following:

   a. Install ADFS on a Windows Server 2012 R2 x64. For more information, see ADFS server requirements on page 18.

   b. Configure Jive to use Claims. For more information, see Configuring Jive to use Claims on page 11.

   c. Configure ADFS to send Claims using a custom rule. For more information, see Configuring ADFS to send claims using custom rules on page 14.

Configuring Jive to use Claims

You need to configure Jive to use Claims before installing the Jive for SharePoint add-on.

Fastpath: Admin Console: System > System properties

To configure Jive to use Claims:

1. In the Admin Console, go to **System** > **System Properties** .

2. Add the following system properties:

   a) Set `registration.domainRestriction.domains` to `jivesoftware.com,jive-land.com,jivelandia.com`.

      The property refers to the Jive domains of the clients.

   b) Set `jive.use.strict.https` to `false`.

      This property is optional.

3. Contact Support to set up the following for you:

   a) Set up `registration.domainRestriction.domains` and `jive.use.strict.https` system properties.

   b) Configure SAML SSO, if required.

4. To use Claims ID mapping instead of email mapping:

   a) Go to **People** > **Settings** > **Global Profile Settings** .

   b) Click **Create new field**.

   c) In **New Profile Wizard: Step 1 of 2**, choose the **Text Field** type, then click **Continue**.

   d) In **New Profile Wizard: Step 2 of 2**, in **Filed Name**,

   e) Under **Translations**, type `Claims ID` for the **English** translation.

5. Under **Attributes**, select **Required**.

6. Click **Finish**.

   You should now see the new parameter under **Other Profile Fields** on the **Profile Settings** page, as shown in the following image:

7. To configure SSO:

   a) Go to **People** > **Settings** > **Single Sign On** .

   b) On the **SAML** tab, click **Enable**.

c) Copy the content from the following federation file and paste into the large text box on the **Metadata** tab: `https://adfs3.iqc01.com/FederationMetadata/2007-06/FederationMetadata.xml`.

- `iqc01.com`: The domain name of the servers (ADFS, SharePoint, Web Apps).

- `adfs3`: The hostname of the ADFS.

d) Click **Save all SAML Settings**.

e) Go to the **User Attributes Mapping** tab.

f) Complete the form by adding the URLs into the **Username**, **Email**, **First Name**, and **Last Name** fields, as shown in the following image:

SAML Settings

Metadata	User Attribute Mapping

Name	Attribute Name	Federated
External Identifier:	Use Subject NameID or ☐ Override with Assertion Attribute	
Username:	Use Subject NameID or ☑ Override with Assertion Attribute	
Username:	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress	☑
Email:	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress	☑
First Name:	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname	☑
Last Name:	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname	
Title:		☐
Department:		☐
Phone Number:		☐
Hire Date:		☐
Mobile Phone Number:		☐
Address:		☐
Home Phone Number:		☐
Biography:		☐
Alternate Email:		☐
Home Address:		☐
Location:		☐
Company:		☐
Claims ID:	ADFSClaimsID	☑

g) Click **Save all SAML Settings**.

Configuring ADFS to send claims using custom rules

To complete the prerequisites for Jive for SharePoint, an ADFS administrator with IT expertise needs to send claims by using a custom rule.

The following steps must be performed by the ADFS administrator with IT expertise.

To configure a custom rule for sending claims in ADFS:

1. Open up the ADFS console.
2. Click **trust relationships** and then right-click **relying party trust** > **Add Relying Party Trust** as shown in the following image:
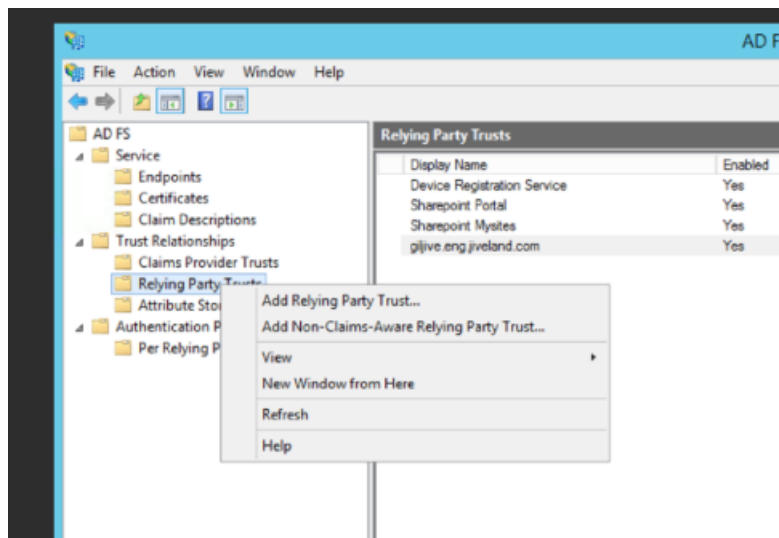
3. Open the Jive URL in a new tab and add `saml/metadata` to the end. For example:

   `https://giljive.eng.jiveland.com:8443/saml/metadata`

4. If the file is not automatically downloaded as XML, download and rename it with a .xml extension.

5. In the ADFS Console, click **Select Data Source** > **Import data about the relying third party from a file** , as shown in the following image:
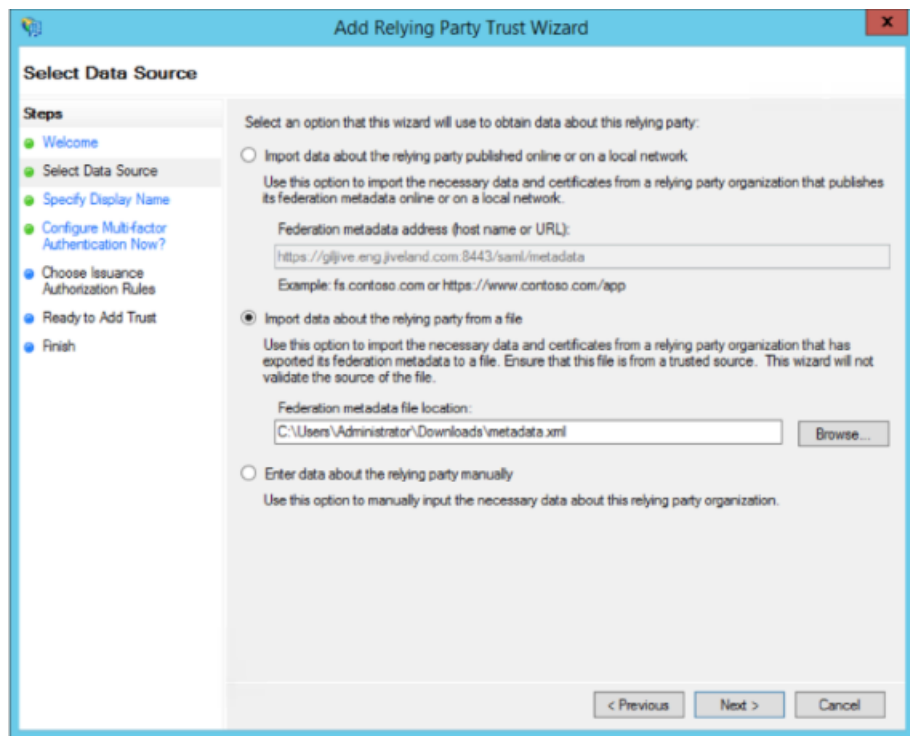
6. Type or browse to the Federation metadata file location, and then click **Next**.

7. Click **Specify Display Name** and enter the display name.

8. Click **Configure Multi-factor** > **I do not want to configure multi-factor** , then click **Next**.

9. Select **Permit all users to access this relying third party** , then click **Next**.

10 In the **Ready to Add Trust** step, click **Next**.

11 In the **Finish** step, select the **Open the Edit Claims Rule dialog for this relying party trust when this wizard closes** option.

12 When the **Edit Claims Rules for Jive SSO Integration** dialog box opens, click **Add Rule**, as shown in the following image:
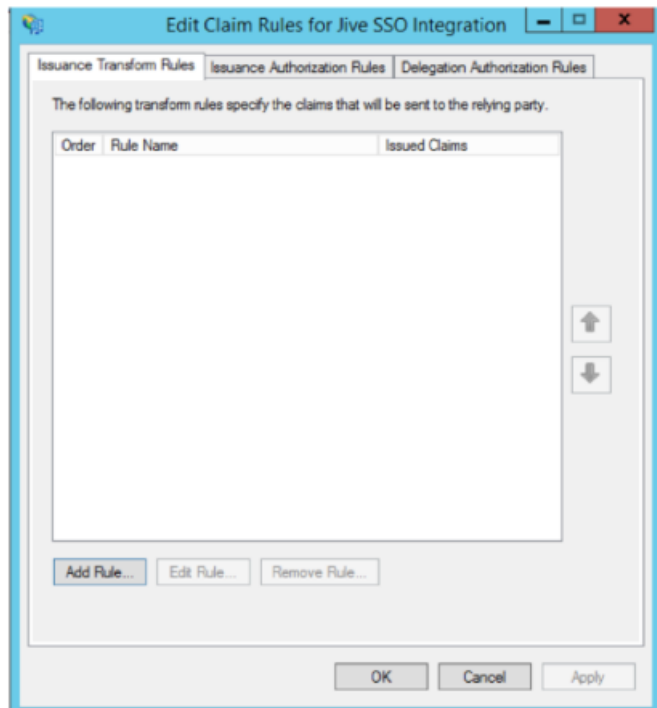
13 In the **Choose Rule Type** step, select **Send LDAP Attribute as Claims** , then click **Next**.

14 In the **Configure Claim Rule** step, type the Claim rule name, select **Active Directory**, and then select or type the following information in the table exactly as it appears below for Mapping of LDAP attributes to outgoing claim types:

LDAP Attribute	Outgoing Claim Type
ObjectGUID	Name ID
	Note: There is a space after Name.
Given-Name	Given Name
Surname	Surname
E-Mail-Address-es	E-Mail Address

15 Click **Finish**.

16 Once again, use the **Edit Claims Rules for Jive SSO Integration** dialog box to add a new rule by clicking **Add Rule**.

17 In the **Choose Rule Type** step, select **Send Claims Using a Custom Rule** , then click **Next**.

18 Type in the following text in the **Custom Rule** text box, at the same time customizing the settings for your environment:

- **adfs3**: Your ADFS server name.

- **iqc01.com**: The correct domain.

- **ADFSClaimsID**: The value you have entered as the Claims ID value in the SAML in the Jive Admin Console.

  The transformation rule has four parts:

  - **Type ==** "…": The source of information defined as schema URL.

    For e-mail address:
    ```
    http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress
    ```
    For User Principle Name (UPN):
    ```
    http://schemas.xmlsoap.org/ws/2005/05/identity/claims/upn
    ```

  - **Type =** "ADFSClaimsID": The name of the attribute ADFS sends to Jive on successful login. ADFSClaimsID is the name of the user mapping field to set in Jive's SAML Admin Console. ADFS and Jive must match.

  - **Value =** "i:05.t|adfs3.mydomain.com|" + c.Value: The Claims ID realized by SharePoint for user identification.

  - **ValueType =** c.ValueType: The type is not used actively; it is a text field in Jive user profile. You can leave as is.

  For more information on Claim Types, see ClaimTypes Members on Microsoft portal at https://docs.microsoft.com/en-us/previous-versions/windows-identity-foundation/ee727097(v=msdn.10).

Transformation Rules Examples

- **E-mail-based ClaimsID**

```
c:[Type ==
"http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress"] =>
issue(Type = "ADFSClaimsID", Value = "i:05.t|adfs3.mydomain.com|" +
                                          c.Value, ValueType
 = c.ValueType);
```

Result: `i:05.t|adfs3.mydomain.com|user@mydomain.com`

- **Classic NTLM ClaimsID**

```
c:[Type == " http://schemas.xmlsoap.org/ws/2005/05/identity/claims/upn"]
=> issue(Type = "ADFSClaimsID", Value = " i:0#.w|mydomain\" +
                                          c.Value, ValueType
 = c.ValueType);
```

Result: `i:0#.w|mydomain\user1`

Customize these rules per customer to match the right Claims ID supported by the customer's SharePoint environment. The Claims ID can change from the examples above, except for the classic NTLM Claims ID that is standard when using NTLM authentication.

You can check the User Diagnostic script to verify that Claims ID is supported by SharePoint.

19 Click **OK**, and then click **Finish**.

ADFS server requirements

Here you can find the ADFS server requirements reference.

Display name	Name
Active Directory Certificate Services	AD-Certificate
- Certification Authority	ADCS-Cert-Authority
- Certificate Enrollment Policy Web Service	ADCS-Enroll-Web-Pol
- Certificate Enrollment Web Service	ADCS-Enroll-Web-Svc
- Certification Authority Web Enrollment	ADCS-Web-Enrollment
Active Directory Domain Services	AD-Domain-Services
Active Directory Federation Services	ADFS-Federation
DNS Server	DNS
File and Storage Services	FileAndStorage-Services
- File and iSCSI Services	File-Services
- File Server	FS-FileServer
- Storage Services	Storage-Services

Display name	Name
Web Server (IIS)	Web-Server
- Web Server	Web-WebServer
- Common HTTP Features	Web-Common-Http
- Default Document	Web-Default-Doc
- Directory Browsing	Web-Dir-Browsing
- HTTP Errors	Web-Http-Errors
- Static Content	Web-Static-Content
- HTTP Redirection	Web-Http-Redirect
- Health and Diagnostics	Web-Health
- HTTP Logging	Web-Http-Logging
- Logging Tools	Web-Log-Libraries
- Request Monitor	Web-Request-Monitor
- Tracing	Web-Http-Tracing
- Performance	Web-Performance
- Static Content Compression	Web-Stat-Compression
- Security	Web-Security
- Request Filtering	Web-Filtering
- Client Certificate Mapping Authentic…	Web-Client-Auth
- IIS Client Certificate Mapping Authe…	Web-Cert-Auth
- Windows Authentication	Web-Windows-Auth
- Application Development	Web-App-Dev
- .NET Extensibility 4.5	Web-Net-Ext45
- ASP	Web-ASP
- ASP.NET 4.5	Web-Asp-Net45
- ISAPI Extensions	Web-ISAPI-Ext
- ISAPI Filters	Web-ISAPI-Filter
- Management Tools	Web-Mgmt-Tools
- IIS 6 Management Compatibility	Web-Mgmt-Compat
- IIS 6 Metabase Compatibility	Web-Metabase
- IIS Management Scripts and Tools	Web-Scripting-Tools

Display name	Name
.NET Framework 3.5 Features	NET-Framework-Features
- .NET Framework 3.5 (includes .NET 2.0 and 3.0)	NET-Framework-Core
.NET Framework 4.5 Features	NET-Framework-45-Fea…
- .NET Framework 4.5	NET-Framework-45-Core
- ASP.NET 4.5	NET-Framework-45-ASPNET
- WCF Services	NET-WCF-Services45
- HTTP Activation	NET-WCF-HTTP-Activat.
- TCP Port Sharing	NET-WCF-TCP-PortShar.
Group Policy Management	GPMC
Remote Server Administration Tools	RSAT
- Role Administration Tools	RSAT-Role-Tools
- AD DS and AD LDS Tools	RSAT-AD-Tools
- Active Directory module for Windows …	RSAT-AD-PowerShell
- AD DS Tools	RSAT-ADDS
- Active Directory Administrative …	RSAT-AD-AdminCenter
- AD DS Snap-Ins and Command-Line …	RSAT-ADDS-Tools
- AD LDS Snap-Ins and Command-Line Tools	RSAT-ADLDS
- Active Directory Certificate Services Tools	RSAT-ADCS
- Certification Authority Management T…	RSAT-ADCS-Mgmt
- DNS Server Tools	RSAT-DNS-Server
SMB 1.0/CIFS File Sharing Support	FS-SMB1
User Interfaces and Infrastructure	User-Interfaces-Infra
- Graphical Management Tools and Infrastructure	Server-Gui-Mgmt-Infra
- Server Graphical Shell	Server-Gui-Shell
Windows Internal Database	Windows-Internal-Dat…
Windows PowerShell	PowerShellRoot
- Windows PowerShell 4.0	PowerShell
- Windows PowerShell 2.0 Engine	PowerShell-V2
- Windows PowerShell ISE	PowerShell-ISE
Windows Process Activation Service	WAS

Display name	Name
- Process Model	WAS-Process-Model
- Configuration APIs	WAS-Config-APIs
WoW64 Support	WoW64-Support

Setting up permissions

Because SharePoint has a different permissions model than Jive, you need to understand the permissions of Jive places to set up SharePoint-side permission groups correctly.

Caution: After you set up your Jive and SharePoint connection according to the permissions recommendations described here, be careful about making changes made to permissions outside the automatic provisioning of the system. You should also block regular users from being able to modify the shared permissions of files within Jive-associated document libraries.

When you connect SharePoint to Jive, you're connecting a site collection to a *place*. Jive has three types of places that can be linked to a SharePoint site: social groups, spaces, and projects. Groups have a different permissions model from spaces and projects. For more information, see Jive places: spaces, groups, and projects in the Jive 9.x Community Manager Help.

Restricting Jive places to specific site collections

When you configure the SharePoint add-on, the best practice is to identify one or more site collections that users can choose from when creating a Jive group, space, or project. If you identify more than one, place creators select from a drop-down list.

If you do not specify the site collections, users are required to specify the URL of a site collection, and there are no restrictions on where the SharePoint content is stored. For most administrators, security considerations will dictate the need to place content in specific site collections.

Jive space and project permissions

Access to Jive spaces and projects is governed by associating it with a Jive user group which define permissions for groups of users. There are three types of user groups in Jive.

A single Jive instance may contain all three kinds of user groups.

Permission groups are different than social groups, which are places in Jive. There are three types of permission groups in Jive. A single Jive instance may contain all three kinds of permission groups.

- A custom user permissions group configured in Jive.

- A custom user permissions group provisioned from LDAP or another directory server.

- The built-in Jive groups Everyone and All Registered Users. Everyone includes all users in Jive. All Registered Users excludes external and anonymous users.

Spaces and projects exist in a hierarchy and are subject to permissions that are set in the Jive Admin Console: spaces and projects inherit their permissions from any space that contains them. For example, if people belonging to the All Registered Users permissions group in Jive have access to a space, they also have access to any subspaces and projects located in that space, unless a permissions override is created. If you create a Jive project or space linked to SharePoint, you may want to make sure it is a restricted space. A project that inherits permissions from an unrestricted space could grant access to every member of the community. For more information, see Managing permissions and Managing user accounts and user groups in the Jive 9.x Community Manager Help.

On the SharePoint side, each site created on the Jive side is provisioned with the following three SharePoint permission groups:

- `[site name] Jive Contributor Users`

- `[site name] Jive Full Control Users`

- `[site name] Jive Read Users`

These are used in the following ways depending on the type of permission groups applied on the Jive side.

- For places that grant access to **custom permissions groups created in Jive**, each member of the Jive permission group is assigned to Jive Contributor Users or Jive Read Users according to whether their rights to the space are read/write or read/only rights. The user who created the space is assigned to the Jive Full Control Users group for the linked SharePoint site.

- For Jive places that grant access to **LDAP-provisioned permission groups**, it is assumed that SharePoint is integrated with LDAP and can directly access the same permissions for each user. These permissions are then used to assign rights to the linked SharePoint site.

- For Jive places that grant access to the built-in Jive permissions groups Everyone or All Registered Users, Jive grants access to the Everyone principal in SharePoint. This is the default behavior in Jive when creating a space. This principal can be mapped using the SharePoint add-on settings during the Jive-side setup. If the principal is NOT specified in this setup, it will be identical to the default SharePoint Everyone principal. If you need the number of users with access to Jive content to be smaller than the total number of SharePoint users defined in the default

Everyone principal, you should map the Everyone principal to a smaller group during add-on setup. For more information, see Installing SharePoint integration add-on on page 24.

Jive group permissions

Jive social groups do not exist in a hierarchy or inherit permissions from anywhere else in the community.

Instead, access is controlled by the type of group and by group membership. The following table shows who can access the four group types. The following table shows who can access the four group types.

	Private Unlisted	Private	PublicRestricted	Public
What is visible to non-members?	None	Group name only	All	All (no membership)
Who can see content?	Member	Member	Anyone	Anyone
Who can participate?	Member	Member	Anyone can interact with content and create discussions and questions. Only members can create other content types	Anyone
Who can invite new members?	Member or administrator	Member or administrator	Member or administrator	Anyone
Who can approve new members?	Administrator	Administrator	No membership	No membership

Other than Open groups, which always grant full access to all members of the community, the other group types have varying membership. The group of people who have permissions changes as people are invited to or leave the group (or are banned from it). SharePoint-side access is synchronized from the group membership. This means that other than SharePoint users with Full Control access, users with group membership on the Jive side have the same rights to the content in the linked site/document library on the SharePoint side.

An exception is that when the Everyone principal is not mapped in the SharePoint add-on settings, as described in Installing SharePoint integration add-on on page 24. Users who are not members of or following an Open group will not be able to access content on the SharePoint side.

Implications of groups for SharePoint permissions

When a restricted (Members Only, Private, or Private Unlisted) group is created, users have rights to the content on the SharePoint side according to their Jive-side group membership.

By default, only people who are members of (or are following) an Open group have access to content on the SharePoint side. Until users join or are added to the group, Open group content is not visible on the SharePoint side. If this does not reflect your security model, you have the option to configure the SharePoint add-on to identify the Everyone principal, as described in Installing SharePoint integration add-on on page 24. Specifying the Everyone principal defines the list of users who have read-write access to Open group content.

Members of the SharePoint Online Full Control Users group have full rights to all SharePoint-connected places in the Jive community and can also delete content on either side of the integration. Jive group membership does not affect their permissions to content on the SharePoint side.

Jive group type	SharePoint Full Control users	SharePoint Contributor users	SharePoint Read users
Open	Group creator	Everyone*	
Members Only	Jive admins**, Group creator	All group members	Everyone*
Private	Jive admins, Group creator	All group members	
Private Unlisted	Jive admins, Group creator	All group members	

* Requires an Everyone principal in SharePoint to be mapped in the add-on settings during Jive-side setup. For more information, see Installing SharePoint integration add-on on page 24.

** Requires the Full Control principal in SharePoint to be mapped in the add-on settings during Jive-side setup. For more information, see Installing SharePoint integration add-on on page 24.

Installing SharePoint integration add-on

Here you can find installation instructions for the SharePoint integration add-on.

To install SharePoint On-Prem add-on:

1. Log in to Jive using an administrator account.
2. In the user interface, select **Your avatar** > **Add-Ons** .

   The All Add-ons page is displayed.

3. Click the **Available** tab.

4. Click **Install** next to the **SharePoint On-Prem** add-on.
5. Confirm the message that appears by clicking **Install**.

The add-on is installed and appears on the **Installed** tab. The SharePoint integration is now available for selection in **Storage Management** > **Add Integration** > **Provider Type** list.
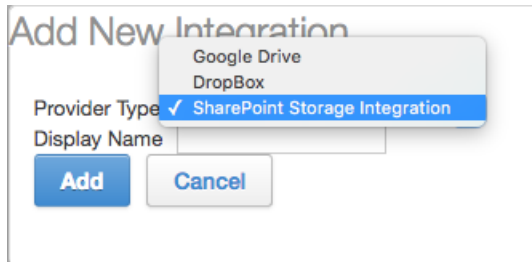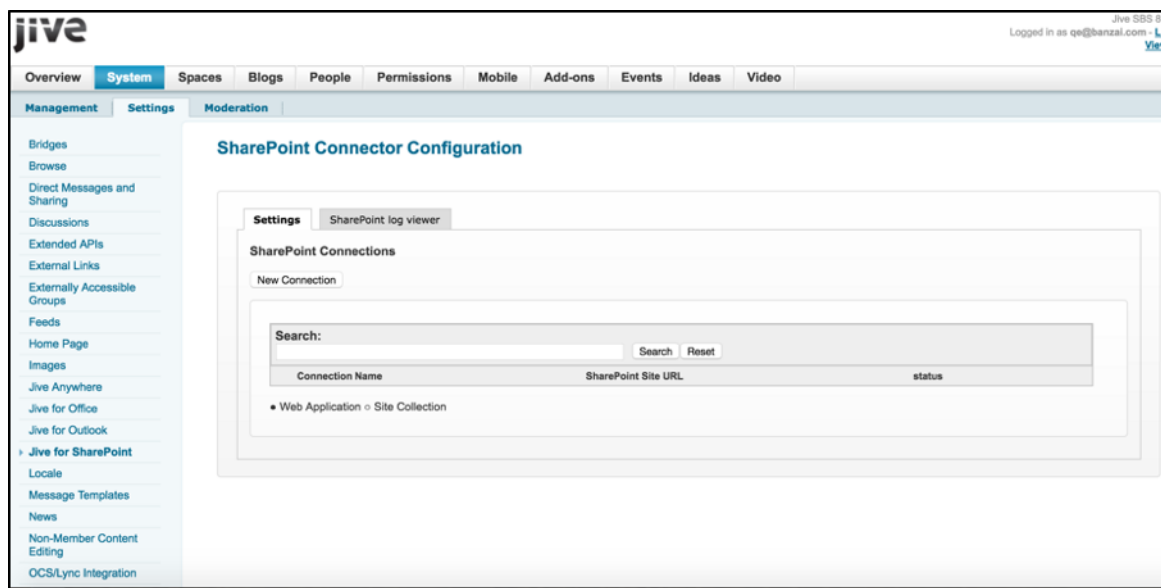
Configuring Jive for SharePoint connections

You create and configure a new connection from the Jive Admin Console.

Fastpath: **Admin Console: System** > **Settings** > **Jive for SharePoint**

To create and define a new connection:

1. In the Admin Console, go to **System** > **Settings** > **Jive for SharePoint** .

2. Click **New Connection**.

   This opens the **New Connection** dialog box.

3. Enter the connection details as follows:

   • **SharePoint version**: Select your SharePoint installation version: **2010**.

   • **Connection Name**: Type a name for the connection that you can easily find later.

4. In **Authentication Type**, select how Jive authenticates to SharePoint.

   The SharePoint-to-Jive authentication is always handled by sending a token to SharePoint via a service API.

   - If you select **Claims**, enter the appropriate values for **WCtx**, **WTRealm**, **WReply**, and **ADFS STS URL**. For more information about these fields, refer to your system administrator.

     Extend the SharePoint web application to use a different authentication type and different address. This enables your regular web application to continue working with Claims. For more information, see Extend a Web application (SharePoint Server 2010) on Microsoft portal at https://technet.microsoft.com/en-us/library/cc261698.aspx.

   - If you select **NTLM**, in **SharePoint Integration network domain** field, specify the network domain name of the SharePoint Integration Admin user.

5. Complete the connection properties by configuring the following settings:

   - **Integration Site Collection URL**: The site collection that is used for several server-to-server activities that are required for the bi-directional communication between the Jive server and the SharePoint web application. Main activities include:

     - Jive to SharePoint network connectivity validation
     - Sub-site or site collection creation process

   - **SharePoint Integration Admin user name**: A SharePoint user that is used as the integration administrator.

     The SharePoint Integration Admin is added as a Full Control admin for any new site created on SharePoint by Jive (in addition to the user who created the site). This account serves as a fallback user for any operation, on either Jive or SharePoint, done by a user in one side of the integration and who is not mapped to a user on the other side of the integration.

     You should set the SharePoint Integration Admin with the following permission level:

     - If the connection is used for creating sub-sites, Site Collection Admin of the integration Site Collection.
     - If the connection is used for creating Site Collection, Site Collection Admin of the integration Site Collection and a Farm Admin.

   - **SharePoint Integration Admin Password**: The password for the SharePoint Integration Admin.

6. Click **Next**.

   The system validates the connection configuration and displays the Site Details page.

7. Specify the connection permission groups as follows:

   - **Jive-All-Users Permission Group(s)**: One or more Active Directory security groups. Use a semicolon (;) to specify more than one group.

     Users in the specified security groups are granted with View/Edit permissions to Open or Members Only Jive places; and View/Edit permissions to the connected SharePoint sites. Typically, the specified security groups contain all the users who require access to the Jive community connected to SharePoint.

   - **Jive-Admins Permissions Group(s)**: One or more Active Directory security groups. Use a semicolon (;) to specify more than one user group.

     Users in the specified groups are granted with full permissions to all Jive-linked SharePoint sites. The group members must be admins on the Jive side.

- **Jive Server URL**: The URL that SharePoint uses to get to Jive. This is used by the Jive's WSP component to perform connectivity validation from SharePoint to Jive.

- **SharePoint Container Creation Policy**: The SharePoint container policy to use when a Jive place is connected to a new SharePoint container.

  - **Sub-site**: A new SharePoint sub-site is created in the selected location. This option requires you to select a parent SharePoint site.

  - **Site Collection**: A new SharePoint Site Collection is created under the Farm root path. For more information, see Creating places linked to SharePoint on page 39.

8. Click **Next** to configure federated search settings.

   The Search Settings page is displayed.

   Federated search enables users to search for content in SharePoint sites from Jive. Federated search is available under the **Bridged Communites** section in the advanced search page.

9. Click **Configure Search Options**.

The community search properties are displayed.

10Enter the searched community details as follows:

- **Display name in community search**: A name for this community search. This name appears under the Federated Search section in the Jive Search page.

- **SharePoint Search URL**: The search URL in the connected SharePoint site.

- **Search Scope**: The scope of the search. Leave the default option: **By Site / Site Collection**.

- **Scope value**: The search scope in the connected SharePoint site.

- **Maximum results count**: The maximum number of search results.

- **Storage Instance**: The default storage instance for this SharePoint integration. You can select different Storage Instances if it exists.

11 Click **Add** to save this searched community.

The community search you have defined is added to the Search Settings page.

12 Click **Add Community Search** to add more searched communities.

13 If required, edit or delete the search configuration:

- Click ⚙ to edit the community search settings.

- Click 🗑 to delete the community search settings.

14 Click **Finish** to create the connection.

The connection is added to the list of SharePoint Connections on the Jive for SharePoint page.
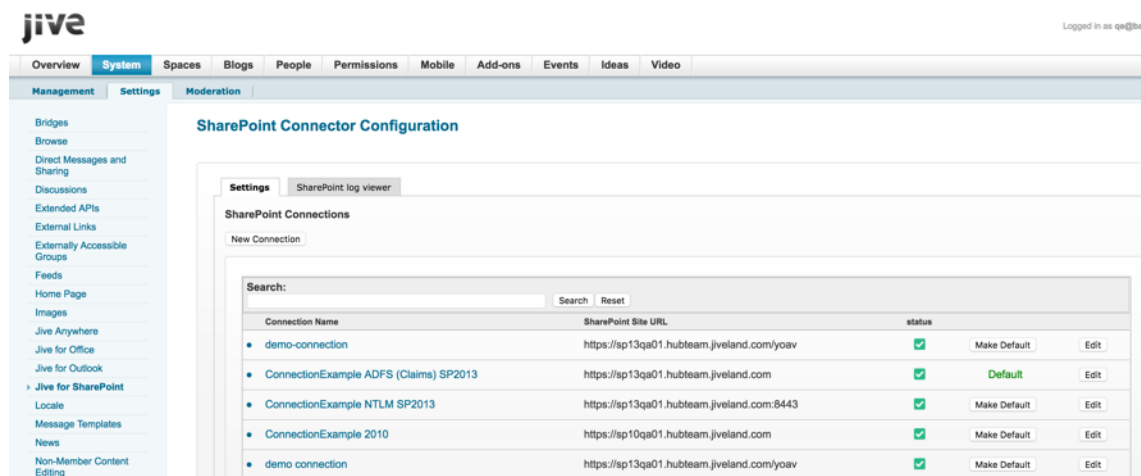
Creating and configuring storage instances

The Storage Management tab in Add-ons enables you to define default configurations for SharePoint as a Storage Provider. Do this if you want different default behavior for a specific site collection, or if you want to limit access to a specific site collection.

With this setup, you can configure which Jive user permission groups can see which site collections, and assign their default behavior.
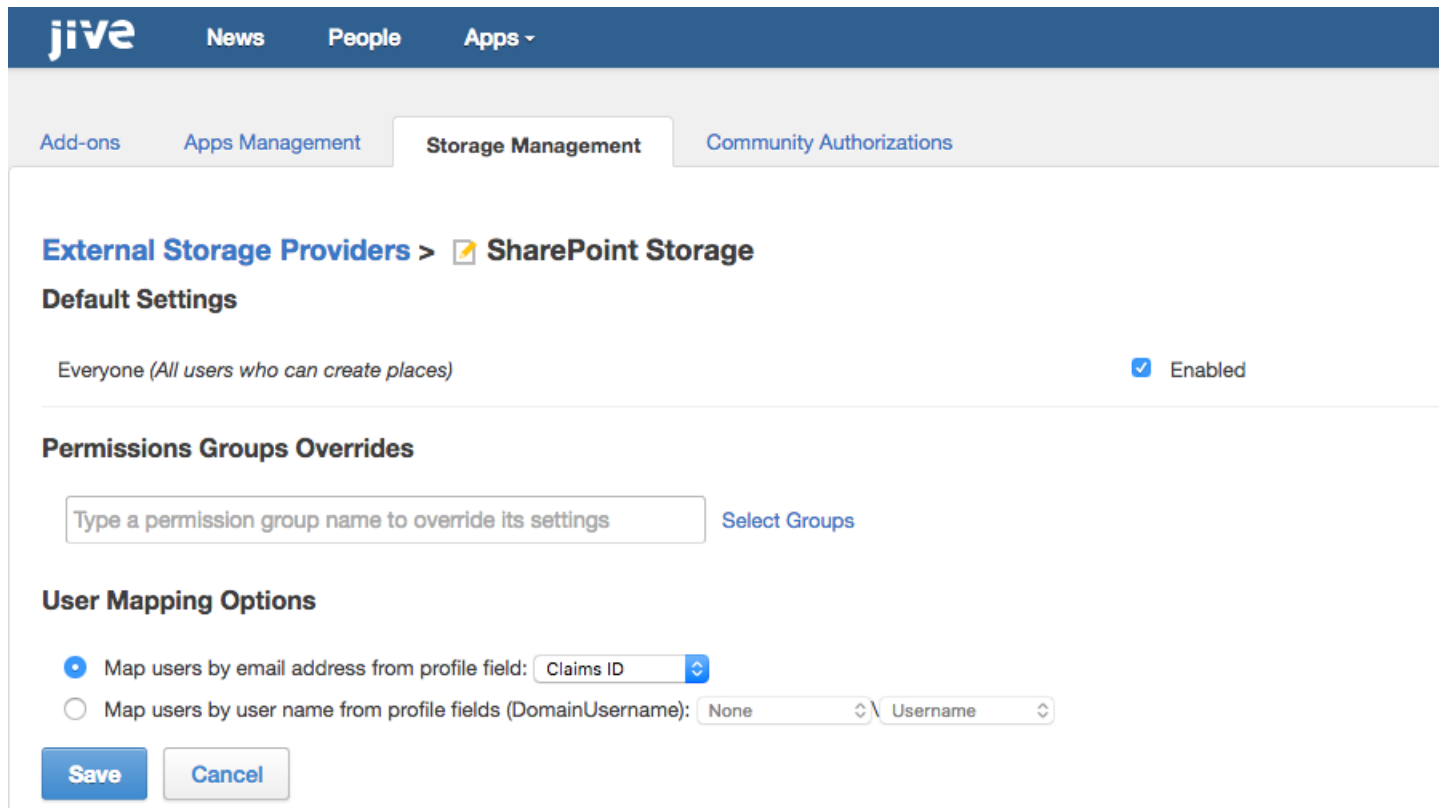
To create a storage instance:

1. Log into Jive using an administrator account.
2. In the user interface, go to **Your avatar** > **Add-Ons** and then select the **Storage Management** tab.
3. Click **Add Integration**.

   The **Add New Integration** dialog box is displayed.
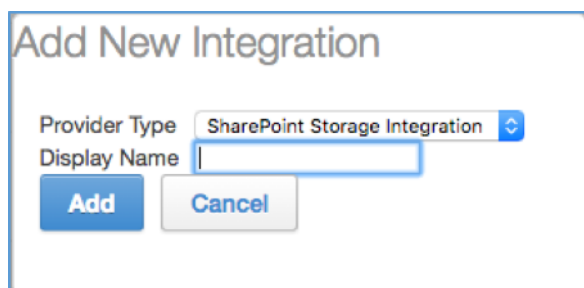
4. In **Provider Type**, select **SharePoint Storage Integration**, type in a name you will be able to identify easily, and click **Add**.

5. Under **User Mapping Options**, select the appropriate mapping field depending on the selected authentication type.

6. Click **Edit Settings**.

7. In the **Edit Instance Settings** dialog box, enter the instance properties:

   • **SharePoint connection**: The SharePoint connection URL you have created in the previous step.

   • **Preview Policy**: The preview method when uploading office documents.:

      • For SharePoint 2013, you can select either **Jive** preview or **Microsoft Office Web Application 2013** preview.

      • For SharePoint 2010, only **Jive** preview is available.

   • **New Group Policy**: The type of sites users can connect in this storage instance. Available options are:

      • **Only New Site**: When creating a place and connecting it to SharePoint a new SharePoint site is always created.

      • **Only Existing Site**: Requires choosing an existing site to which the Jive place connects.

      • **Existing Site & New Site**: Allows users choosing the site's location.

   • On the right-hand side, click the **+** icon and add at least one site collection under which new groups are created.

You can use the same site collection specified in the SharePoint connection you have created, or add new site collections. The site collections must have complete URLs.

8. Click **Validate** to validate the values of this storage instance.

A successful validation message indicates a validated instance.

9. Click **Save**.

10Click **Save** again in the **Default Settings** page.

The storage instance is saved and displayed in the **External Storage Providers** page.

Completing user mapping

After you set the parameters for storage configuration, you should complete user mapping.

Fastpath: **Your avatar** > **Add-ons** , then **Storage management** tab

After mapping configurations are set successfully, the log-in will forward to the SSO (single sign-on) authentication process. The authentication window opens, and when you enter the right credentials, finally forwards to the Jive instance.

Mapping by Claims ID

To add the claims ID as part of the mapping fields:

1. In the Jive user interface, select **Your avatar** > **Add-ons** .
2. On the **Storage Management** tab, click **Edit Instance** next to the integration to want to configure.
3. Under **User Mapping Options**, select **Map users by user name from profile field**, and then select **None** > **TheClaimsID** , as shown in the screenshot below.

Mapping by email

To map users by email:

1. In the Jive user interface, select **Your avatar** > **Add-ons** .

2. On the **Storage Management** tab, click **Edit Instance** next to the integration to want to configure.

3. Under **User Mapping Options**, select **Map Users by email address from profile field**, and then select **Email Address**.

Mapping by Domain/Username

To map users by Domain/Username:

1. In the Jive user interface, select **Your avatar** > **Add-ons** .

2. On the **Storage Management** tab, click **Edit Instance** next to the integration to want to configure.

3. Under **User Mapping Options**, select **Map Users by username from profile fields**, and then select **ENG Domain Name** > **ENG Username** .

4. In AD FS management, add those rules: `Jive ENG Username` and `Jive ENG Domain Name`.

Jive ENG Username
```
c:[Type == "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/upn"]
=> issue(Type = "ADFSNTLMUN", Value = RegExReplace(c.Value, "@[^\n]*", ""),
ValueType = c.ValueType);
```

Jive Domain Name
```
c:[Type ==
"http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname"]
=> issue(Type = "ADFSNTLMDOMAIN", Value = "ENG", ValueType = c.ValueType);
```

5. In the Jive Admin Console, go to **People** > **Profile Settings** , and click **Create new fields**.

6. Create new fields with the **Text** type selected: `ENG Username`, `ENG Domain Name`, and `ENG Domain Name`.

7. Change the SAML settings in Jive as follows:

   a. Go to **People** > **Settings** > **Single Sign-On** > **SAML** > **User Attribute Mapping**.

   b. Set `ADFSNTLMUN` in **ENG Username** and `ADFSNTLMDOMAIN`" in **ENG Domain Name**. Mark them both as **Federated**.

   a. "Click **Save All SAML Settings**

SharePoint connection settings

While installing your SharePoint On-Prem add-on, you need to configure the add-on. To do this, use the following reference material to complete the ADFS settings and permissions form.

SharePoint Tenant Root URL	The URL of the SharePoint server. You can find this URL by navigating to one of the sites in SharePoint you're planning to link to Jive and copy the path up to the first forward slash. For example, if your site is located at `https://my.sharepoint.com/sites/site1/`, type `https://my.sharepoint.com`.	
Allow SharePoint Connection Type	Select one of the following options from the list:	
	Only Existing Site	Requires that users connect their Jive place to an existing SharePoint site when they create or configure their Jive place.
	Only New Site	Requires that SharePoint creates a new site for Jive Places syncing to SharePoint.
	Existing Site and New Site	Lets users choose to use an existing or create a new site when they create or configure their Jive place.
Authentication Settings	**Claims** or **NTLM** authentication method are available.	

	In **Admin Username**, you should provide the domain, backslash, site collection admin. For example, type `domain.com\admin`. In **Password**, type the password for this user in the password field. This admin must have at least Site Collection Administrator access in SharePoint. This user will serve as the service account for the Jive integration. Make sure it is well-secured because it will need to have access to all the site collections you create as part of the integration.
SharePoint everyone user group	The name of the Everyone permissions group in SharePoint. If you specify this group, the users included will have read-write access to all content created in an Open group in Jive, even if they have not been added to the Jive group. This saves admins the work of having to add members to Open group content to grant access on the SharePoint side. Secret, Private, and Members-Only groups restrict content on both sides of the integration according to the Jive-side group settings, regardless of whether you supply Everyone information here.
Sharepoint full control (admins)	Type the name of the Full Control admins permissions group in SharePoint. This group will have access to all SharePoint-connected groups in Jive. The best practice is to create a restricted group of admins in this principal who will be able to access all the Jive places and Jive-linked site collections. For more information, see Setting up permissions on page 21.
Add New Site Collection list available for creating places	If you want users creating a place to be restricted to specific site collections, click the **+** sign next to **Add New Site Collection list available for creating places** and type the location of a site collection. You can add more site collections by clicking **+** again. Users can choose from the list of site collections when creating a group. Note that as the user configuring the add-on, you must have access to these site collections, or you won't be able to complete the configuration and will see a configuration error.
	Caution: Specifying at least one site collection is the best practice because it limits the SharePoint locations where place creators can create sites, and also prevents errors in specifying a URL. If you specify one or more locations, users are not prompted to supply the URL of a site collection.

Creating places linked to SharePoint

If your admin has enabled this functionality, create a new space or group, and connect it to a new or existing SharePoint site. Use the SharePoint site as storage only or storage plus Jive functionality.

To connect a Jive place to SharePoint as an external storage provider:

1. Create a new place or edit the Activity page of an existing place.
2. Next to **External file storage**, click **Change**.
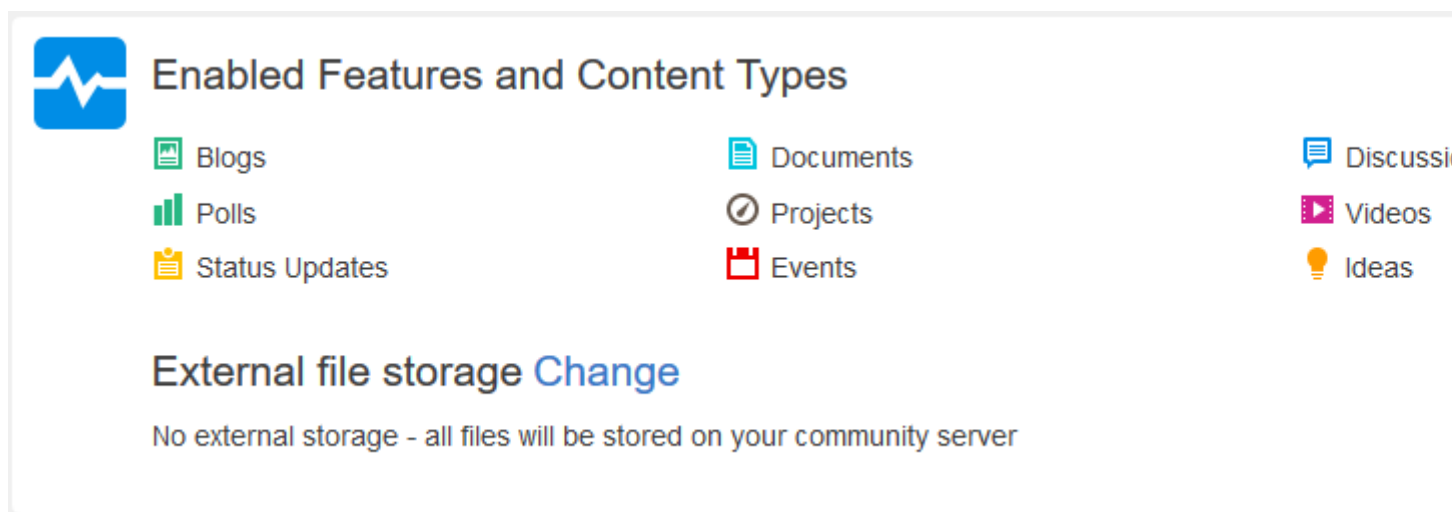
This open the **Enable Features and Content Types** dialog box.

3. Under **External file storage**, select your SharePoint storage instance and click **Apply**.

Enable Features and Content Types

Group Features

Select which features you want enabled in your group.

☑ Blogs	☑ Documents	☑ Discussions & Questions	☑ Polls	☑ Projects	☑ Videos
☑ Status Updates	☑ Events	☑ Ideas			

External file storage

Choose where to store files saved in this group.

○ **No external storage - all files will be stored on your community server**

○ ⓑ **Jive BOX**

○ Ⓞ **SPOnline**

◉ **SP-ON-PREM**

⚠ Only files you upload from now on will be stored in external storage. Any files or attachments that were alre created in this place will continue to be stored on the community server.

Apply   **Close**

4. Select the site collection to which you want to connect the new place.

The options you see in the **Site Collection** list are the site collections you have added.
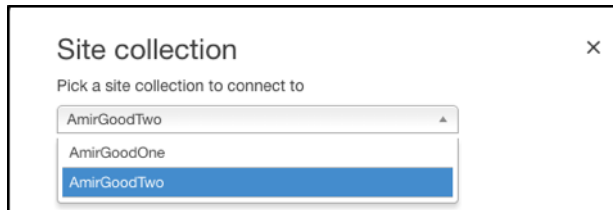
5. To connect to a new site:

   a) Under **SharePoint Site**, select **Create a new site under**.

   b) Use the **+/-** signs to expand or collapse the tree view and view subsites. A green site indicates that this site is already connected.

   c) Select the site under which the new site will be created.
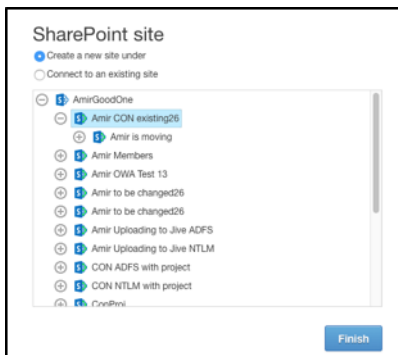
   d) Click **Finish**.

   This creates a new site under the site you select in the tree view.

6. To connect to an existing site:

   a) Under **SharePoint Site**, select **Connect to an existing site**.

   b) Use the **+/-** signs to expand or collapse the tree view and view subsites and select the site to which you want to connect the Jive place.

c) Click **Next**.
d) Select **Jive Document Library** to set the primary library. Files uploaded to the Jive place are synced to the primary library and files uploaded to the primary library are synced to the Jive Place.
e) Select **Additional Document Library** to set secondary libraries. Files uploaded to the secondary libraries are synced to the Jive place.
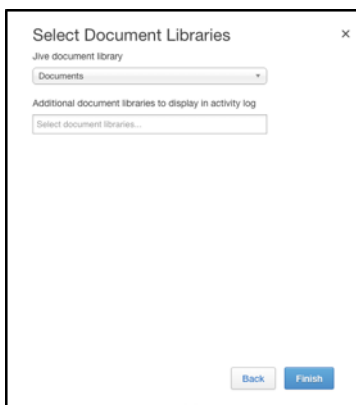
f) Click **Finish**.

This connects the place to the site you select in the tree view.

Disconnecting your place from SharePoint

You can disconnect your place from SharePoint if required.

When you disconnect your place from SharePoint, Jive leaves the external storage files intact in SharePoint so that they can be repurposed or safely deleted from the storage system. The file objects pointing to the external filed are maintained in Jive, including all their social collaboration activities (such as commenting and liking), and the link to download the file is converted to a permanent link pointing to the last known location of the file in the external storage system.

To disconnect your place:

1. Go to the Activity page of the place you want to disconnect from Sharepoint Online.

2. Select **Gear icon** > **Edit activity page** to get to the settings page of an existing place.

3. To switch to another storage provider, select another integration option.

4. To completely disable external file storage and save uploaded files to Jive, select **No external storage**.

5. Click **Apply** to apply the configuration.
6. Click **Save** to save the changes to the Activity page.