



Mashup Sites for SharePoint 2010 Installation & Configuration

Version 3.1.1

Copyright

Copyright © 2011, JackBe Corp. and its affiliates. All rights reserved.

Terms of Use

This documentation may be printed and copied solely for use in developing products for the PRESTO ENTERPRISE MASHUP SOFTWARE PLATFORM.

JackBe, Corp. reserves the right to revise this documentation and to make changes in content from time to time without obligation on the part of JackBe, Corp. to provide notification of such revision or changes.

JackBe, Corp. AND ITS SUPPLIERS MAKE NO REPRESENTATIONS OR WARRANTIES THAT THE DOCUMENTATION IS FREE OF ERRORS OR THAT THE DOCUMENTATION IS SUITABLE FOR YOUR USE. THE DOCUMENTATION IS PROVIDED ON AN "AS IS" BASIS.

JackBe, Corp. AND ITS SUPPLIERS MAKE NO WARRANTIES, TERMS OR CONDITIONS, EXPRESS OR IMPLIED, EITHER IN FACT OR BY OPERATION OF LAW, STATUTORY OR OTHERWISE, INCLUDING WARRANTIES, TERMS, OR CONDITIONS OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND SATISFACTORY QUALITY.

TO THE FULL EXTENT ALLOWED BY LAW, JackBe, Corp. ALSO EXCLUDES FOR ITSELF AND ITS SUPPLIERS ANY LIABILITY, WHETHER BASED IN CONTRACT OR TORT (INCLUDING NEGLIGENCE), FOR DIRECT, INCIDENTAL, CONSEQUENTIAL, INDIRECT, SPECIAL, OR PUNITIVE DAMAGES OF ANY KIND, OR FOR LOSS OF REVENUE OR PROFITS, LOSS OF BUSINESS, LOSS OF INFORMATION OR DATA, OR OTHER FINANCIAL LOSS ARISING OUT OF OR IN CONNECTION WITH THIS DOCUMENTATION, EVEN IF JackBe, Corp. OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

IF THIS DOCUMENTATION IS PROVIDED ON A COMPACT DISC, THE OTHER SOFTWARE AND DOCUMENTATION ON THE COMPACT DISC ARE SUBJECT TO THE LICENSE AGREEMENT ACCOMPANYING THE COMPACT DISC.

Trademarks

JackBe®, Presto®, the Jackbe logo and Presto logo are trademarks or registered trademarks of JackBe Corporation.

Microsoft®, SharePoint®, ASP®, .NET® and the Microsoft Internet Explorer logo, Windows®, Windows logo are registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

All other product and brand names may be trademarks or registered trademarks of their respective owners.

Installation and Configuration

Contents

Introduction	4
Installing Mashup Sites for SharePoint	4
Requirements and Prerequisites.....	4
What Is Installed	4
Installation Steps.....	4
Planning Authentication	7
User Authentication Experiences.....	7
Authentication Designs.....	7
SSO + Token Authentication	9
No SSO + Cookie Authentication.....	10
No SSO, Manual Authentication	10
Configuring Mashup Sites for SharePoint	11
Activating Mashup Sites for SharePoint Features	11
Enabling Mashup Sites for SharePoint Features in Farms	11
Enabling Mashup Sites for SharePoint Web Parts for Site Collections.....	11
Manually Enabling Mashup Sites for SharePoint Features for a Site.....	12
Setting up Single Sign-On for Mashup Sites for SharePoint	12
Configure the Secure Store Service	12
Create Secure Store Target Applications	12
Create or Manage SSO Token Server Names.....	15
Configuring Mashup Server Connections in SharePoint.....	16
Adding a Mashup Server Connection.....	17
Editing a Mashup Server Connection.....	20
Enabling Cookie Forwarding for Mashup Server Overrides.....	22
Setting the Default Sandbox Mode for Apps	22
Farm and Site Administration	23

Introduction

This document describes the prerequisites and process for installing and configuring Mashup Sites for SharePoint 2010. It also covers basic administration features.

The installation process involves deploying the Mashup Sites for SharePoint solution to SharePoint 2010 farms. See [Installing Mashup Sites for SharePoint](#) for details.

Configuration involves activating features across your farms and sites, setting up authentication mechanisms between SharePoint and Mashup Servers and defining connections to Presto Mashup Servers. See [Planning Authentication](#) and [Configuring Mashup Sites for SharePoint](#) for details.

See also [Farm and Site Administration](#).

Installing Mashup Sites for SharePoint

Requirements and Prerequisites

Mashup Sites for SharePoint requires the following items to be configured prior to installation:

- ▶ **Microsoft SharePoint Server (MSS) 2010** and optionally the Secure Store Service (SSS) to provide single sign-on capabilities and greatly enhance the user experience. Single sign-on is only available with MSS 2010 and SSS enabled.

MSS 2010 also provides additional Web Parts for Inter-Web Part communication including mashup and App Web Parts from Mashup Sites for SharePoint.

- ▶ **Microsoft .NET Framework 3.5.**

Although not required for general use of Mashup Sites for SharePoint, publishing Apps from Mashup Server to SharePoint and registering SharePoint services in Mashup Server both require either **NTLM v2** or **Basic** authentication.

What Is Installed

Installing Mashup Sites for SharePoint deploys the following:

- ▶ WSP Package – contains the features and content needed to use Mashup Sites for SharePoint.
- ▶ Updates to the web.config file of the target web application to give permission for use of the DLLs deployed

Installation Steps

The installation wizard for Mashup Sites for SharePoint performs two major tasks:

- ▶ Unpack and register Mashup Sites for SharePoint with Windows. You must use the automated wizard to perform this task.
- ▶ Deploy the Mashup Sites for SharePoint solution to the selected web applications or site collections in your SharePoint farm.

You can choose to deploy the Mashup Sites for SharePoint solution manually, if needed.

Note: You must be logged directly into the SharePoint server using a SharePoint administrator user account for installation. See [Troubleshooting](#) for additional information.

1. Log into the SharePoint server using a SharePoint administrator user account, if you have not already logged in.
2. Download the Mashup Sites for SharePoint installation package for SharePoint 2010 from the [Mashup Developer Community](#).
3. Double-click the MashupSitesForSharePoint2010(v3.1.1).msi to start the installation wizard.

The installation welcome screen opens. Click **Next**.

4. If needed, change the default folder where the installer will unpack the Mashup Sites for Sharepoint deployment files. Click **Next**.
5. Click **Next** again to confirm the installation. The wizard unpacks Mashup Sites for Sharepoint.

Important: If you prefer to manually deploy the Mashup Sites for SharePoint solution in your SharePoint farm or you encounter errors during automated deployment, you can close the installation wizard at this point. Follow the manual deployment instructions in the *readme.txt* file in the folder where you unpacked Mashup Sites for SharePoint.

6. Click **Next** in the Deployment confirmation screen to automatically deploy the Mashup Sites for SharePoint solution.

The deployment wizard performs a set of system checks to ensure that all deployment requirements are met before proceeding. Click **Next** once these system checks are completed to continue with the deployment.

See the [Troubleshooting](#) section for suggestions to resolve common problems discovered in these system checks.

7. The End-User License Agreement displays. Read the license agreement and accept the terms. Click **Next**.
8. Choose the web applications or site collections for this SharePoint farm where you wish to deploy the Mashup Sites for SharePoint solution. Click **Next**.

Deployment begins.

Note: If you create a new site collection after Mashup Sites for SharePoint has been deployed and want to use the Presto Web Parts in this new site collection, you may activate Mashup Sites for SharePoint features for the new site. See [Error! Reference source not found.](#) for instructions.

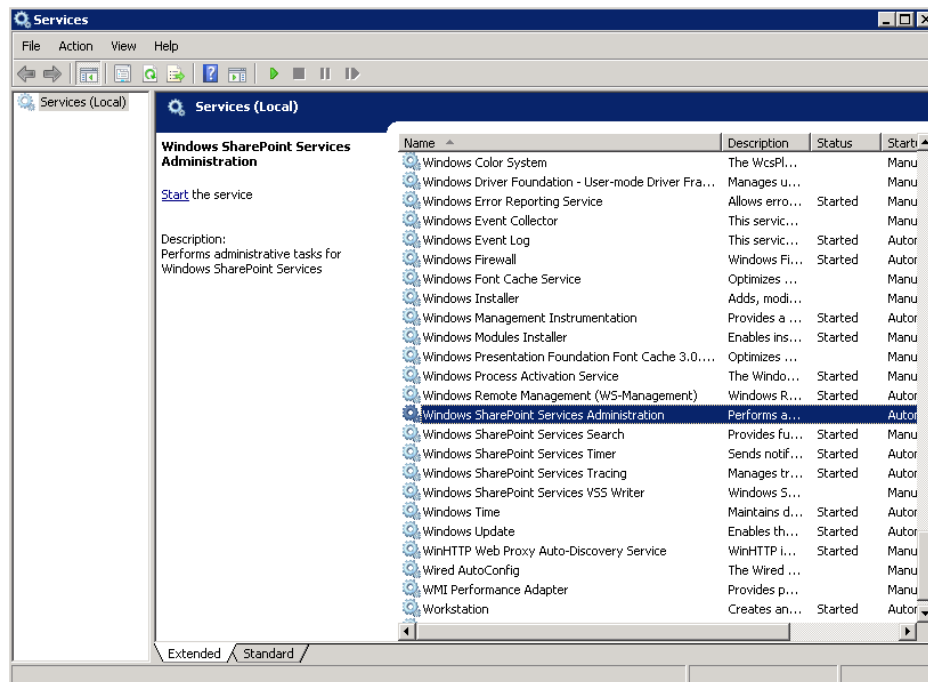
9. Click **Close** once deployment is complete

Troubleshooting

System Check: Administration Service Not Started

This error occurs during system checks performed before the Mashup Sites for SharePoint solution is deployed. Please ensure you are logged in to the SharePoint server with an administration account and execute the following steps.

1. Click the **Abort** button to stop the current installation.
2. Navigate to Services (For Microsoft Windows Server 2008, click **Start** > Administrative Tools > Services).
3. Click the **Name** column to sort the list of services.
4. Find the service named windows SharePoint Services Administration.



5. Right-click windows SharePoint Service Administration and click **Start**.
6. Restart the Mashup Sites for SharePoint installation. See [Error! Reference source not found.](#)

System Check: You do NOT have permission to install and deploy SharePoint solutions!

This error occurs during systems checks performed before deploying the Mashup Sites for SharePoint solution. This appears to happen only on systems running Microsoft Windows Server 2008. If you encounter this problem, click Abort to stop the deployment. Then restart the installation as an administrator. Right-click the MashupSitesForSharePoint.msi and choose **Run as Administrator**.

If deployment continues to fail, a SharePoint administrator must manually deploy the Mashup Sites for SharePoint solution. Follow the manual deployment instructions in the `readme.txt` file in the folder where you unpacked Mashup Sites for SharePoint.

Planning Authentication

There are several options you can use to implement and optimize authentication between your SharePoint installation and Presto Mashup Servers. This allows you to set up an appropriate level of security and user experience when your environment has bi-directional authentication between SharePoint and one or more Mashup Servers.

The challenge for user authentication with Mashup Sites for SharePoint is that users, who are already authenticated in SharePoint, must also authenticate with one or more Mashup Servers as seamlessly as possible. For the best user experience, a user should only be required to login to a system once and gain authorization to remote systems using their current identity.

User Authentication Experiences

There are three potential authentication experiences for users working with Web Part pages that contain mashups or Apps. From best experience to worst, these are:

- ▶ **True Single Sign-On:** with this experience, a user logs into SharePoint. Their SharePoint credentials are used without any additional login challenges to authenticate with Mashup Servers for any mashups or Apps the user may work with in Web Part pages.
- ▶ **Initial Challenge Only:** this experience limits additional login challenges to a single challenge for the first mashup or App that a user encounters in a Web Part page. In addition to logging in with SharePoint, a user must login with Mashup Servers once during a session in SharePoint (a browser session). Each new session in SharePoint may require this additional login to Presto.
- ▶ **All Challenges:** no authentication information is shared between SharePoint and Presto with this design. Users must login with Mashup Servers for **every** mashup or App that requires authentication. Obviously, this is the least user-friendly experience.

Authentication Designs

The user experiences that you can deliver using Mashup Sites for SharePoint depend on your SharePoint environment and how SharePoint and Mashup Servers are deployed. The factors that determine an authentication architecture include:

- ▶ **SharePoint Version and Authentication:** using Microsoft SharePoint Server (MSS) 2010:
 - **With the Secure Store Service** to provide a true single sign-on experience for Mashup Sites for SharePoint users. Other factors in your environment also play a part in supporting single sign-on.

The Secure Store Service stores user credentials for additional applications, such as Presto Mashup Servers, accessed from SharePoint. User credentials are organized by *target application*, also known as an *SSO Application Name*, allowing the Secure Store service to handle credentials for different applications. You can store user credentials under one SSO Application name to provide credentials that several Mashup Servers share, allowing users

to access mashups and Apps from those Mashup Servers seamlessly, or keep credentials for some Mashup Servers separate using different SSO Application Names.

- **Without Secure Store Service:** this prevents a true single sign-on experience, but can still support an initial challenge experience depending on other factors in your SharePoint environment.

Note: *Mashup Sites for SharePoint is not currently compatible with third-party single sign-on solutions, such as Netegrity SiteMiner, that are agent-based. If your SharePoint environment uses a third-party SSO solution, users may work in Presto Hub with SharePoint to create mashables, mashups and Apps. However, users cannot use Mashup Sites for SharePoint actions in SharePoint and cannot publish mashups or Apps to SharePoint.*

- ▶ **SharePoint and Presto Mashup Server Domains:** how you deploy Mashup Servers in your SharePoint environments affects the choices for authentication. If single sign-on is not possible, deploying SharePoint servers and Mashup Servers in the same domains enables the use of cookies to simplify authentication.
- ▶ **User Repository:** sharing the same user repository, such as an Active Directory or LDAP Directory, for both SharePoint servers and Presto Mashup Servers supports a true single sign-on experience. This enables Mashup Servers to use the same credentials as SharePoint.

Note: *currently there is a known issue for authentication challenges for mashups published in Mashup Web Parts when the user repository is shared. For mashups users will be challenged initially for mashups.*

The combination of these factors produce three authentication architectures that you can use. The following table summarizes which architectures can be applied to specific environments and the resulting user experience:

Authentication Architecture	MSS + Secure Store	MSS + No Secure Store	SharePoint / Mashup Server in Same Domains	SharePoint / Mashup Server in Different Domains	SharePoint / Mashup Server Share User Repository	User Experience
SSO + Token Authentication	✓		✓	✓	✓	True SSO
	✓		✓	✓		Initial challenge
No SSO + Cookie Authentication		✓	✓			Initial challenge
			✓			Initial challenge
No SSO, Manual Authentication		✓		✓		All challenges
				✓		All challenges

SSO + Token Authentication

This authentication design can be used when both criteria are true:

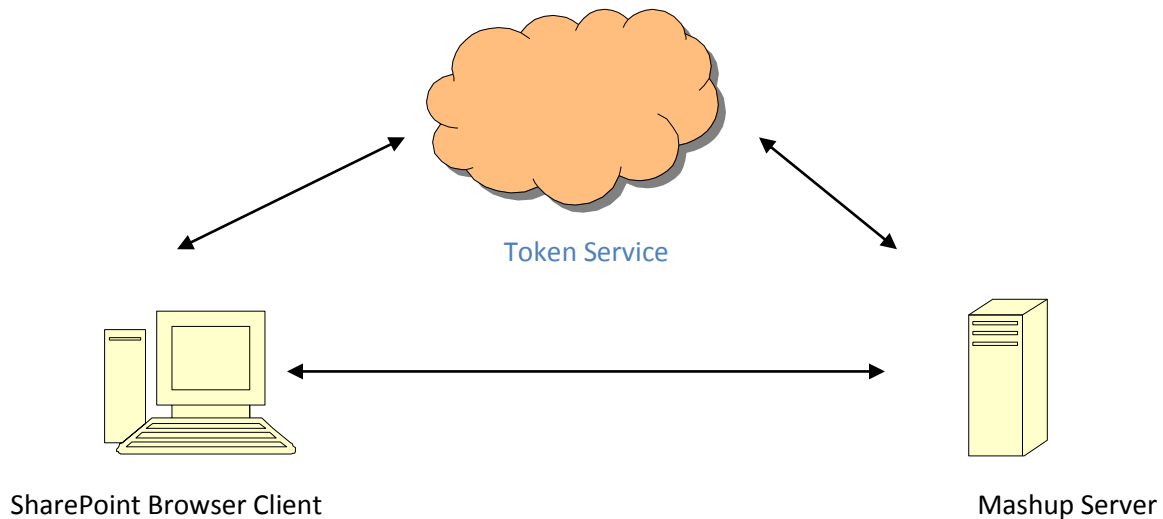
- ▶ You have MSS 2010 in your environment
- ▶ You have chosen to use the Secure Store service

This solution uses the Token Service that is installed with Mashup Sites for SharePoint. The Token Service generates a token ID for a user's SharePoint session when they access mashups or Apps. The requests sent to the Mashup Servers that host these mashups or Apps include:

- ▶ A ticket with the user's token ID
- ▶ An SSO Token Server Name.

Mashup Servers use this name to find connection information to the Token Service. This name ensures that connection information to the Token Service is not passed directly in requests.

Both SharePoint and Mashup Servers must be configured with the SSO Token Server Name and the connection information to communicate with the Token Service. Mashup Servers use this SSO Token Server Name to connect to the Token Service and redeem the user ticket and credentials.



The actual user experience with an SSO + Token solution depends on whether the Mashup Servers and SharePoint servers share an Active Directory as their user repository.

With a Shared User Repository

If SharePoint and the Mashup Servers for your mashup sites also share the same user repository, such as an Active Directory or LDAP Directory, this results in a true single sign-on experience for users. Users login to SharePoint and no further login challenges are issued when they access mashups or Apps in Mashup Servers in this domain. Mashup Servers retrieve user credentials via tokens and then authenticate these credentials and retrieve user authorization information against the shared user repository.

Note: Mashup Servers use only basic user credentials (username and password). They do not accept NTLM credentials which include Windows domains as part of the user name.

With Distinct User Repositories

If SharePoint and the Mashup Servers in this domain do not share a user repository, users receive one additional login challenge the first time they access mashups or Apps hosted in a Mashup Server for a given SSO Application Name (a target application) in SharePoint configuration.

The credentials they enter for this initial login challenge are then stored by the Secure Store service under the SSO Application configured for that connection. For all subsequent requests to Mashup Servers with that same SSO Application name, Mashup Servers retrieve user credentials via tokens and the Token Service and then authenticate them and retrieve user authorization information from the Presto User Repository.

You can have each SSO Application store user credentials for one or several Mashup Server connections in SharePoint.

No SSO + Cookie Authentication

This authentication design can be used when you have MSS 2010 in your environment, but have chosen **not** to use the Secure Store service **and** the SharePoint servers and Mashup Servers for your mashup sites are located in the same domain.

Same Domains

Domains are the same for SharePoint and Mashup Servers when the domain names fit either of these patterns:

**.domain-name.type*

domain-name.type:different-port

For example, if the SharePoint server domain is site1.com, then a Mashup Server in the domain ms.site1.com or site.com:8080 would be in the same domain.

Note: *the patterns for matching domain names are a restriction of Internet browsers.*

With cookie forwarding, a user must login once with a Mashup Server. These credentials are stored as a cookie in the browser where the user is working in SharePoint. This cookie is passed by the browser to the Mashup Server in subsequent requests so no further login challenges are issued.

Note: *Mashup Servers use only basic user credentials (username and password). They do not accept NTLM credentials which include Windows domains as part of the user name.*

No SSO, Manual Authentication

This design is required when you have chosen **not** to use the Secure Store service **and** some Mashup Servers reside in different domains than your SharePoint servers.

Because user credentials are not stored in the Secure Store repository, Mashup Servers cannot retrieve these credentials via the Token Service. Because the SharePoint and Mashup servers are in different domains, cookie forwarding cannot bridge this gap.

This results in manual authentication, requiring users to login to each Mashup Server as they access mashups or Apps hosted by that Mashup Server to create a session or when an existing session with a Mashup Server expires.

Configuring Mashup Sites for SharePoint

You should first determine the authentication mechanisms you will need based on your SharePoint environments and the Mashup Servers that SharePoint will connect to. See [Planning Authentication](#) for the concepts and options you need to determine an appropriate authentication plan.

Once you know what authentication mechanisms you need, configuration for Mashup Sites for SharePoint includes:

- ▶ **Activating Mashup Sites for SharePoint Features:** you must activate features before continuing with other configuration steps.
- ▶ **Setting Up Single Sign-On for Mashup Sites for SharePoint:** this is required if you are using MSS and the Secure Store Service.
- ▶ **Configuring Mashup Server Connections in SharePoint.**

Activating Mashup Sites for SharePoint Features

Mashup Sites for SharePoint adds specific actions to SharePoint farms and sites. It also defines a Mashup Site template which you or users can use and two new Web Parts for mashups and Apps respectively.

To begin configuration, you must first enable Mashup Sites for SharePoint features for each SharePoint farm and site collection where users should be allowed to work with mashups and Apps. See [Enabling Mashup Sites for SharePoint Features in Farms](#) and [Enabling Mashup Sites for SharePoint Web Parts for Site Collections](#).

You can also choose to manually enable Mashup Sites for SharePoint features for individual sites that are not Mashup Sites. See [Manually Enabling Mashup Sites for SharePoint Features for a Site](#).

Enabling Mashup Sites for SharePoint Features in Farms

First, enable Mashup Site features for the appropriate SharePoint farms:

1. Open SharePoint Central Administration as a farm administrator.
2. Click **System Settings** and click **Manage Farm Features** in the Farm Management category.
3. Find the Presto Custom Farm Site Actions item and click **Activate** to activate these features or **Deactivate** to deactivate them.

Activating this feature adds a new category, JackBe Presto Administration, in the Manage Applications section of Central Administration.

Enabling Mashup Sites for SharePoint Web Parts for Site Collections

Next, enable the new Web Parts for Mashup Sites for SharePoint in every site collection where users should be allowed to work with mashups or Apps:

1. Log in as the administrator for a site collection. If needed, navigate to the parent site for the entire collection.
2. Click **Site Actions > Site Settings**.
3. Click **Site Collection Features** in the Site Collection Administration section.
4. Find MS4SP Web Parts and click **Activate** to activate these features or **Deactivate** to deactivate them.

This adds the Mashup Web Part and the App Web Part as valid Web Parts that users can add to Web Part pages. These Web Parts allow users to publish mashups and Apps to SharePoint.

Manually Enabling Mashup Sites for SharePoint Features for a Site

When you create new sites using the Mashup Site template, Mashup Sites for SharePoint Features are automatically enabled. If you want to add these features to another type of site:

1. Login is as site administrator for the specific site.
2. Click **Site Actions > Site Settings**.
3. Click **Manage Site Features** in the Site Actions category.
4. Find MS4SP Custom Site Actions and click **Activate** to activate these features or **Deactivate** to deactivate them.

This adds a new category, JackBe Presto Administration, in Site Settings with functions that allow you to define connections to Mashup Servers and to set other Mashup Site for SharePoint configuration properties (see [Configuring Mashup Server Connections in SharePoint](#) for a complete list). This also adds the Register List action to allow users to register SharePoint Lists as mashable information sources in Presto.

Setting up Single Sign-On for Mashup Sites for SharePoint

If you have MSS 2010 and are using the Secure Store Service to provide single sign-on authentication for Mashup Sites for SharePoint, you must complete some configuration before you begin creating Mashup Server connections:

- ▶ [Configure the Secure Store Service](#).
- ▶ [Create Secure Store Target Applications](#).
- ▶ [Create or Manage SSO Token Server Names](#).

Configure the Secure Store Service

Typically, you create an instance of the Secure Store Service and configure this service when you install SharePoint using the configuration wizard. For more information on deployment and configuration for the Secure Store Service, see the Microsoft TechNet articles:

- ▶ [Plan the Secure Store Service](#)
- ▶ [Configure the Secure Store Service](#)

There are no additional requirements to configure the Secure Store Service for Mashup Sites for SharePoint.

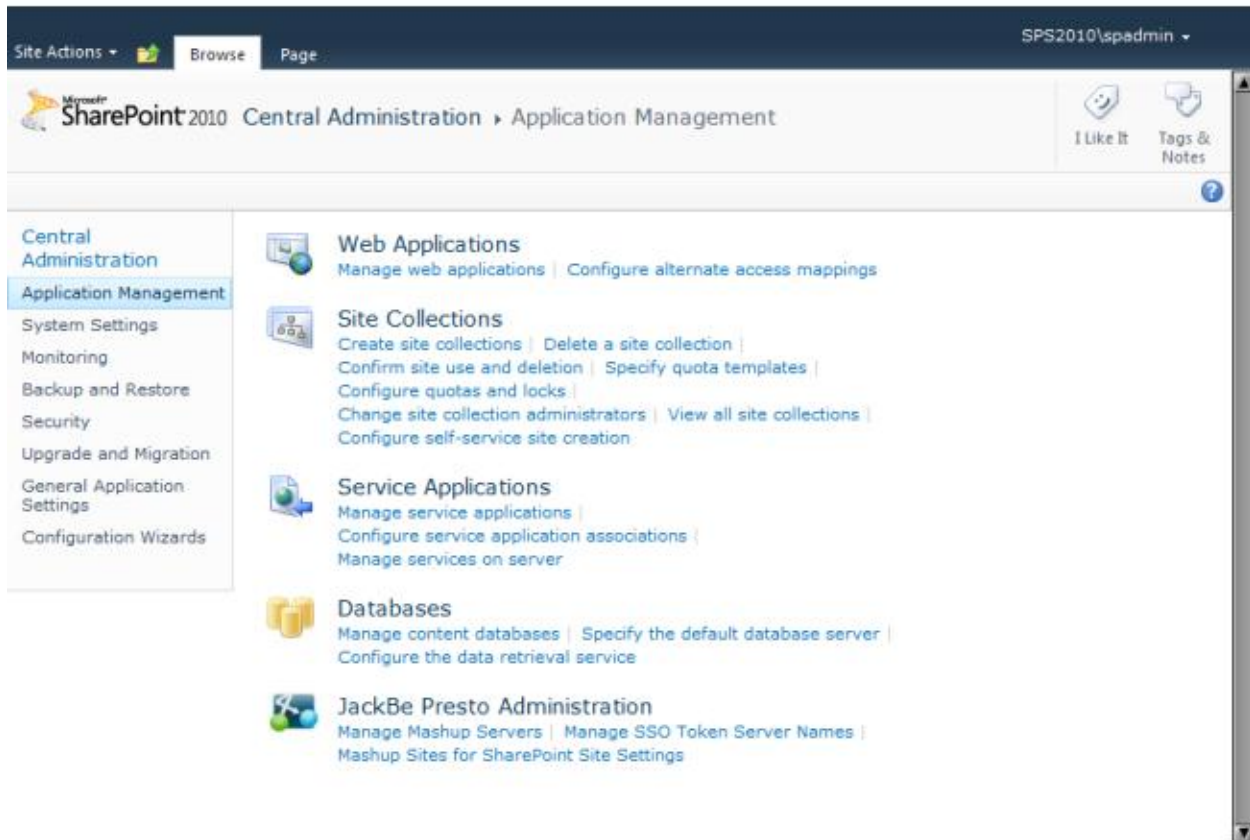
Create Secure Store Target Applications

Target applications organize user or group credentials for SharePoint users to access other systems, such as Presto Mashup Servers. You create a target application to provide credentials when users connect to Mashup Servers to find or work with mashups and Apps in Web Part pages.

To create target applications:

1. Open SharePoint Central Administration as a farm administrator.

2. Click **Application Management** and click **Manage service applications** in the Service Applications category



3. Select the Secure Store Service in the list and click **Manage** in the toolbar ribbon.
4. Click **New** and complete these properties:

SPS2010\spadmin

Central Administration > Create New Secure Store Target Application

Specify the settings for the new Secure Store Target Application. The settings that you specify here can be changed later at Secure Store Target Application page.

Target Application Settings

The Secure Store Target Application ID is a unique identifier. You cannot change this property after you create the Target Application.

The display name is used for display purposes only.

The contact e-mail should be a valid e-mail address of the primary contact for this Target Application.

The Target Application page URL can be used to set the values for the credential fields for the Target Application by individual users.

The Target Application type determines whether this application uses a group mapping or individual mapping. Ticketing indicates whether tickets are used for this Target Application. You cannot change this property after you create the Target Application.

Target Application ID

Display Name

Contact E-mail

Target Application Type

Target Application Page URL
 Use default page
 Use custom page

 None

Next Cancel

- **Target Application ID** = a unique ID for this target application.
- **Display Name** = the name to display to users for this target application. This is the SSO Application Name that users or administrators assign to Mashup Server connections.
- **Contact E-mail** = the email address of the primary contact for Mashup Sites for SharePoint and the Mashup Servers associated with this target application. This can be any valid email address.
- **Target Account Type** = the type of user account mapped by this target application. Typically, this is Individual Ticket, to allow individual user credentials to be mapped. You can also Group Ticket as a type to associate all users in groups to one set of credentials.
- **Target Application Page URL** = leave the Use default page option set.
- **Ticket Timeout** = if needed, change the default timeout period for tickets generated for this Target Application.

5. Click **Next**.
6. Leave the default fields that appear for user credentials. Click **Next**.
7. If needed, find and add other SharePoint administrators or users to the **Target Application Administrators** list who should be allowed to manage this target application. The farm administrator has access by default.
8. If needed, find and add other SharePoint administrators or users to the **Ticket Redeemers** list who should be able to redeem tickets for this target application.
9. Click **OK**.

Once you have a target application, you can create or update Mashup Server connections with this SSO application information. See [Configuring Mashup Server Connections in SharePoint](#) for instructions.

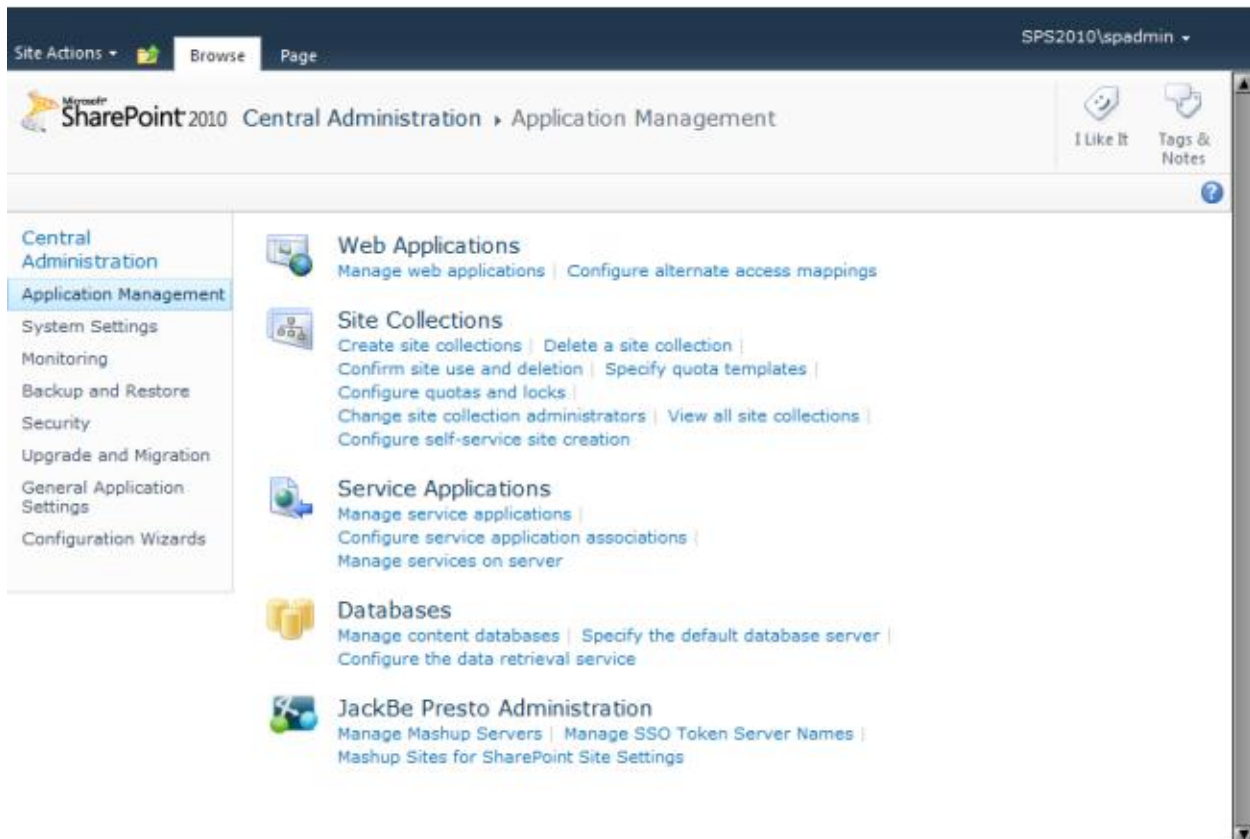
Create or Manage SSO Token Server Names

You must create a SSO Token Server names for each domain with a SharePoint farm or server that connects to Presto Mashup Servers. SSO Token Server Names are a placeholder that is substituted in requests for the host portion, such as <http://myOrg.com>, of the actual URL that Mashup Servers use to connect to this Token Service. Mashup Sites for SharePoint sends the SSO Token Server Name to Mashup Servers which use this name to interact with the Token Service to validate SSO credentials when users connect to the Mashup Server. See [SSO + Token Authentication](#) for more information.

Note: *in addition to configuration in SharePoint, each Mashup Server that has a connection in SharePoint must also have configuration for the SSO Token Server Name. For more information, see [Configuring Connections to SharePoint](#).*

To create or manage SSO Token Server Names:

1. Open SharePoint Central Administration as a farm administrator.
2. Click **Application Management** and click **Manage SSO Token Server Names** in the JackBe Presto Administration category.



3. To add a name, click **New Token Server Name** and complete these properties:
 - **SSO Token Server Name** = this is the placeholder value to display for this Token Service. This is also used in requests to Mashup Servers to allow them to find the correct connection information for this Token Service.
 - **SSO Token Server URL** = the URL to this Token Service.

Then click **OK**.

4. To edit or delete a name, click the down arrow for an existing SSO Token Server Name and select **Edit SSO Token Server Name** or **Delete SSO Token Server Name**.

Configuring Mashup Server Connections in SharePoint

Mashup Sites for SharePoint allows you to connect to multiple Mashup Servers. After a connection is configured, users can publish mashups and Apps to SharePoint as native Web Parts.

Note: Before you begin this configuration, you must install and start the appropriate Mashup Servers. You must also define connections to your SharePoint site collections in Presto. See [Installing, Starting and Configuring Mashup Servers for SharePoint Connections](#) for links to instructions.

Farm administrators or site administrators can configure Mashup Server connections to farms, site collections or individual sites.

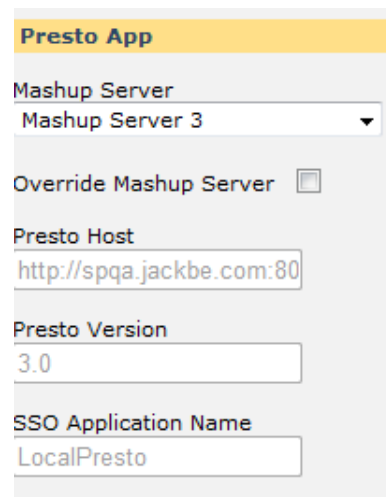
The visibility of that connection and the mashups and Apps hosted in a Mashup Server is based on where you define the connections in SharePoint.

It also works in conjunction with how connections to SharePoint are defined in the Mashup Server. For a discussion of the common patterns for configuring connections, see [Configuring Connections Between Presto and SharePoint](#).

Once users publish a Presto App or mashup to a Web Part, the Web Part has connection properties that are configured by Mashup Server configuration information, such as the following example:

Connection Selected: the selected Mashup Server connection provides the Host, Version, and SSO name details for the Web Part. These properties cannot be changed with this configuration.

Mashup Server connections provide a convenient way for administrators to pre-configure access to Mashup Server(s).



The screenshot shows a configuration window titled "Presto App". It contains the following fields and controls:

- Mashup Server:** A dropdown menu currently showing "Mashup Server 3".
- Override Mashup Server:** A checkbox that is currently unchecked.
- Presto Host:** A text input field containing "http://spqa.jackbe.com:80".
- Presto Version:** A text input field containing "3.0".
- SSO Application Name:** A text input field containing "LocalPresto".

Connection Override: this image shows Web Part properties where the Mashup Server connection has been overridden.

The override option ensures that users can control settings at a granular level if needed.

For more information about overriding Mashup Servers, see the Modify Web Part Settings section in the MS4SP User Guide.



The screenshot shows the 'Presto App' configuration interface. It includes a dropdown menu for 'Mashup Server' set to 'Mashup Server 3', a checked 'Override Mashup Server' checkbox, a 'Presto Host' text box with 'http://spqa.jackbe.com:80', a 'Presto Version' text box with '3.0', and an 'SSO Application Name' text box with 'LocalPresto'.

See [Installing, Starting and Configuring Mashup Servers for SharePoint Connections](#)

Before you configure connections in SharePoint with Mashup Servers, you must install them. You can download the Presto Installation package from the Mashup Developer Community at <http://www.jackbe.com/enterprise-mashup/>. See [Presto Installation](#) for Mashup Server installation instructions.

You must also start each Mashup Server. See [Starting and Stopping the Mashup Server](#) for startup instructions.

You must determine how connections should be configured for both SharePoint and the Mashup Servers and then define connections to your SharePoint farms and site collections in each Mashup Server. See [Configuring Connections Between Presto and SharePoint](#) for examples of connection configurations and instructions on adding SharePoint connections to Presto.

Adding a Mashup Server Connection and [Editing a Mashup Server Connection](#) for instructions. You can also manage site-wide settings. See [Disabling Cookie Forwarding for Mashup Server Overrides](#) and [Setting the Default Sandbox Mode for Apps](#) for more information.

Installing, Starting and Configuring Mashup Servers for SharePoint Connections

Before you configure connections in SharePoint with Mashup Servers, you must install them. You can download the Presto Installation package from the Mashup Developer Community at <http://www.jackbe.com/enterprise-mashup/>. See [Presto Installation](#) for Mashup Server installation instructions.

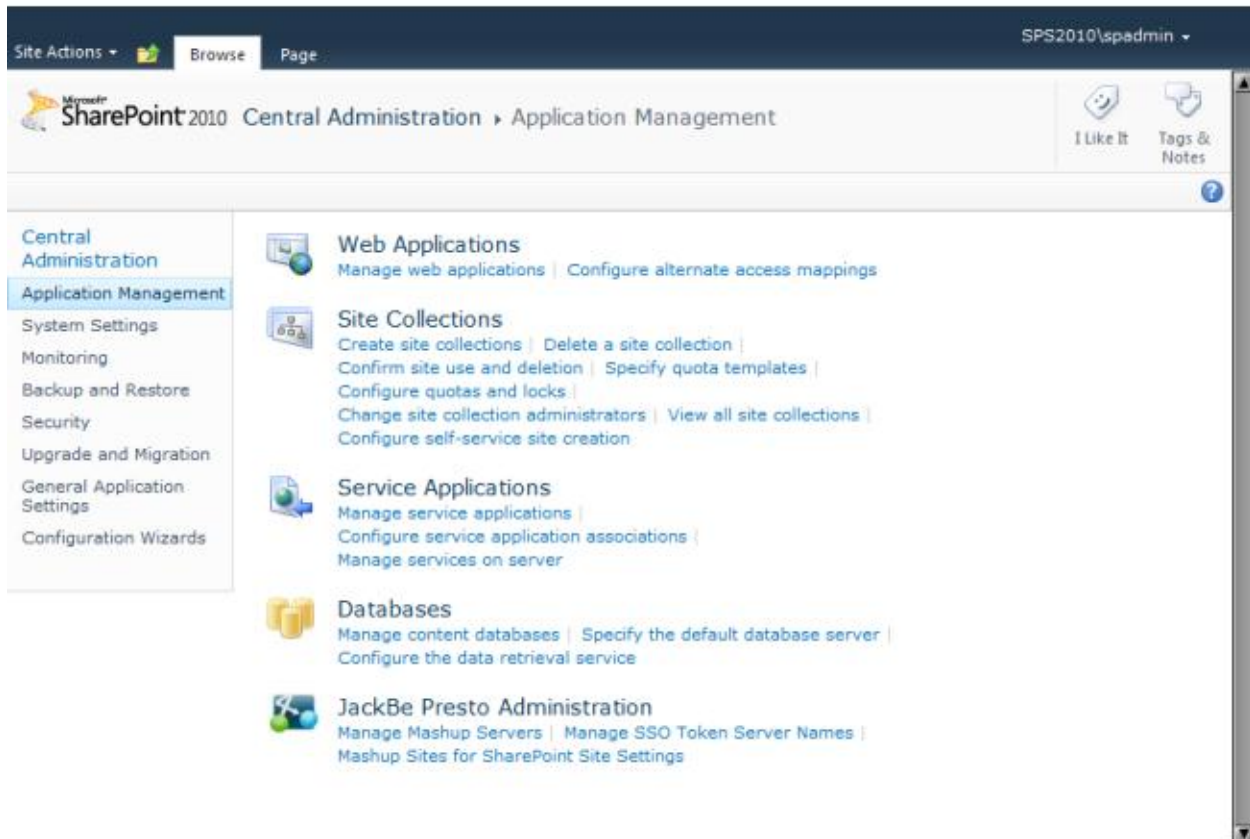
You must also start each Mashup Server. See [Starting and Stopping the Mashup Server](#) for startup instructions.

You must determine how connections should be configured for both SharePoint and the Mashup Servers and then define connections to your SharePoint farms and site collections in each Mashup Server. See [Configuring Connections Between Presto and SharePoint](#) for examples of connection configurations and instructions on adding SharePoint connections to Presto.

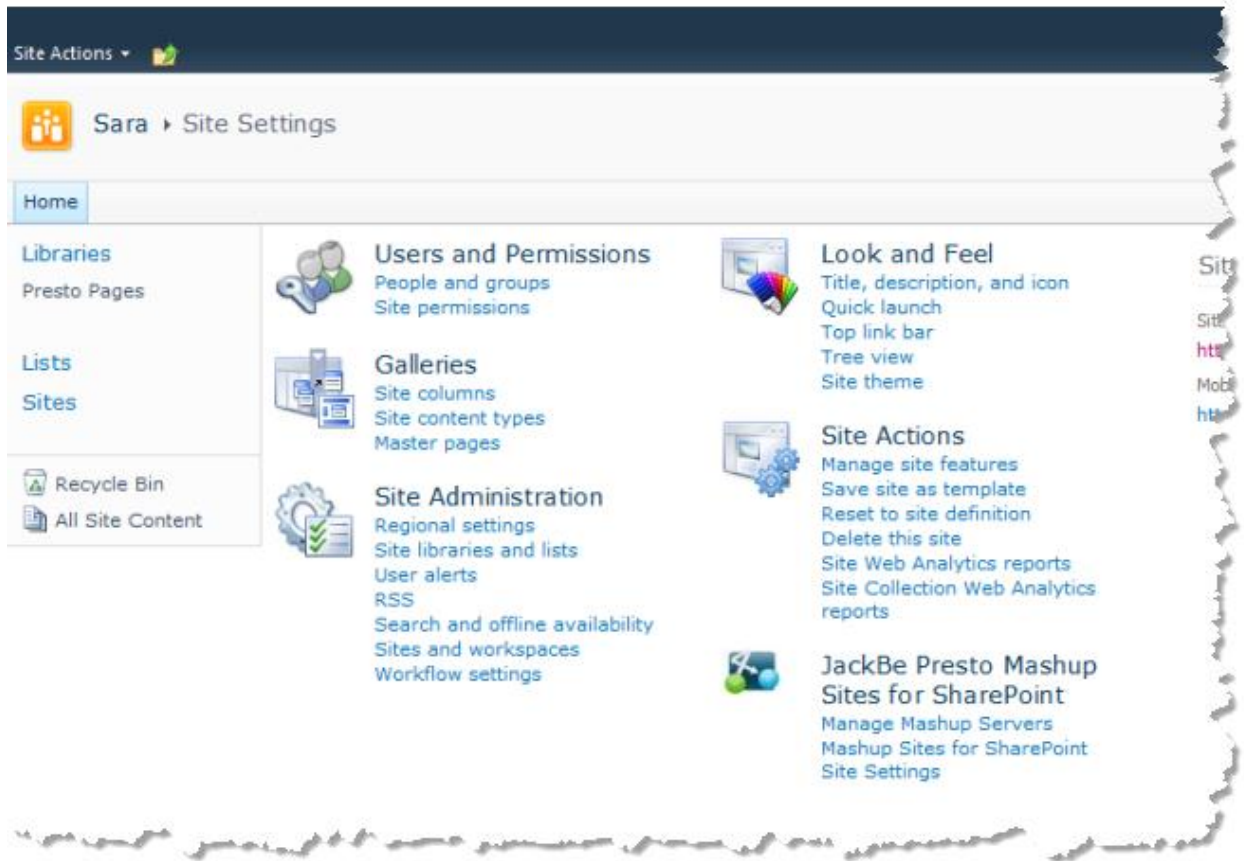
Adding a Mashup Server Connection

The scope of the connection that you create is determined by your account and the farm or site you begin this process from.

1. To create a connection to a Mashup Server in a farm:
 - a. Open SharePoint Central Administration as a farm administrator.
 - b. Click **Application Management** and click **Manage Mashup Servers** in the JackBe Presto Administration category.



2. To create a connection to a Mashup Server in a site collection or a specific site:
 - a. Login is as site administrator for the site collection or specific site. If needed navigate to the home page for the site you want.
 - b. Click **Site Actions > Site Settings**.



- c. Click **Manage Mashup Servers** in the JackBe Presto Administration category.
3. To add a new connection, click **New Mashup Server** from the Manage Mashup Server page. The Add Mashup Server page opens.
4. Complete basic properties for this connection:
 - **Name:** choose a name that describes the location or purpose of the Mashup Server you are connecting to
 - **URL:** enter the domain name and port for the URL to connect to this Mashup Server. For example: `http://mashups.myorg.com:8080`.
5. Set authentication properties for this connections based on your authentication plan. See [Authentication Designs](#) for more information on the types of authentication you can use.

If you are using SSO + Token authentication, set these properties:

- **SSO Enabled:** set this option to enable single sign-on authentication. You must have the Microsoft SharePoint Server (MSS) 2010 and use the Secure Store Service to provide single sign-on for Mashup Server connections.
- **Shares same Active Directory as Sharepoint:** set this option when the Mashup Server and SharePoint are sharing an Active Directory as the user repository. See Authentication Designs for more information on the impacts of sharing a user repository and authentication.
- **SSO Application:** if you have enabled SSO (see above), choose the appropriate target application to use for authentication of credentials when connecting to this Mashup Server.

If no SSO applications are listed, then SSO is not properly configured. See [Configure the Secure Store Service](#) for more information.

If you are using No SSO + Cookie authentication, set this property:

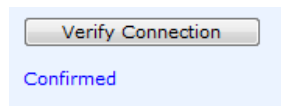
- **Cookie Forwarding:** set this option to allow cookies to handle authentication credentials between SharePoint servers in this farm and this Mashup Server. The Mashup Server must be in the same domain as this SharePoint farm.

If you are using No SSO, Manual authentication, clear all the SSO and Cookie properties.

6. Set the **Mashup Server Enabled** option to activate this connection and click **Verify Connection**.

If the connection fails, check to make sure the URL you entered is correct and the Mashup Server you are connecting to is running. See [Starting and Stopping the Mashup Server](#) for startup instructions.

A Confirmed message displays once your connection is verified.

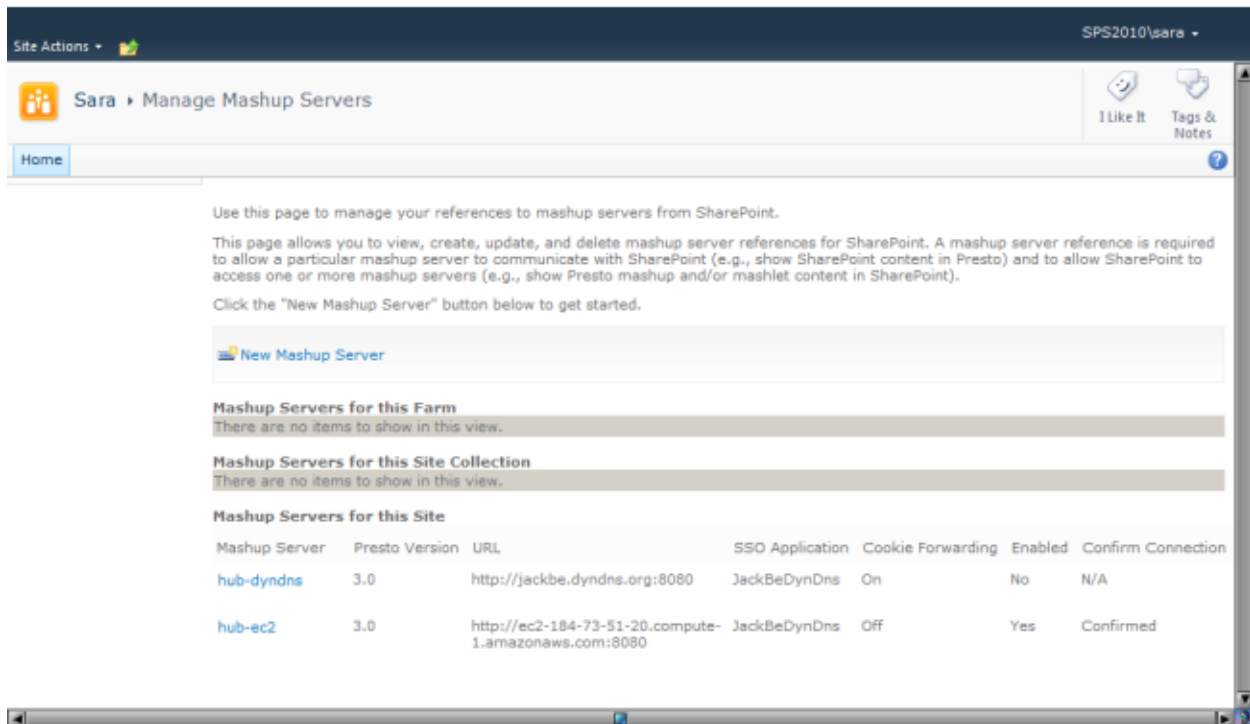


7. Once you have verified the connection, click **Ok**. The Manage Mashup Servers page appears, listing your new Mashup Server connection.

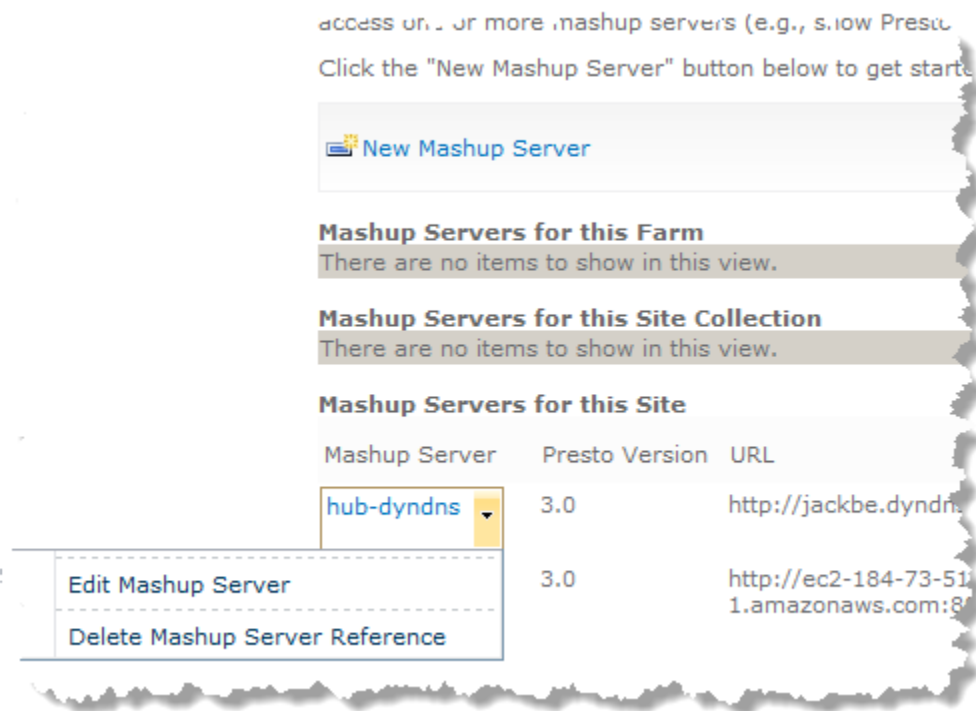
Editing a Mashup Server Connection

1. Find the Mashup Server Connection based on the scope of the connection:
 - a. For connections with a farm scope, open SharePoint Central Administration as a farm administrator. Click **Application Management** and click **Manage Mashup Servers** in the JackBe Presto Administration category.
 - b. For connections with a site collection or site scope, login is as site administrator for the site collection or specific site. Click **Site Actions > Site Settings**. Click **Manage Mashup Servers** in the JackBe Presto Administration category.

The Manage Mashup Servers page opens listing all existing connections in this scope.



2. Click the drop-down menu for the Mashup Server connection you need to edit and select **Edit Mashup Server**.



3. Update the properties you need to edit and click **Verify Connection**.

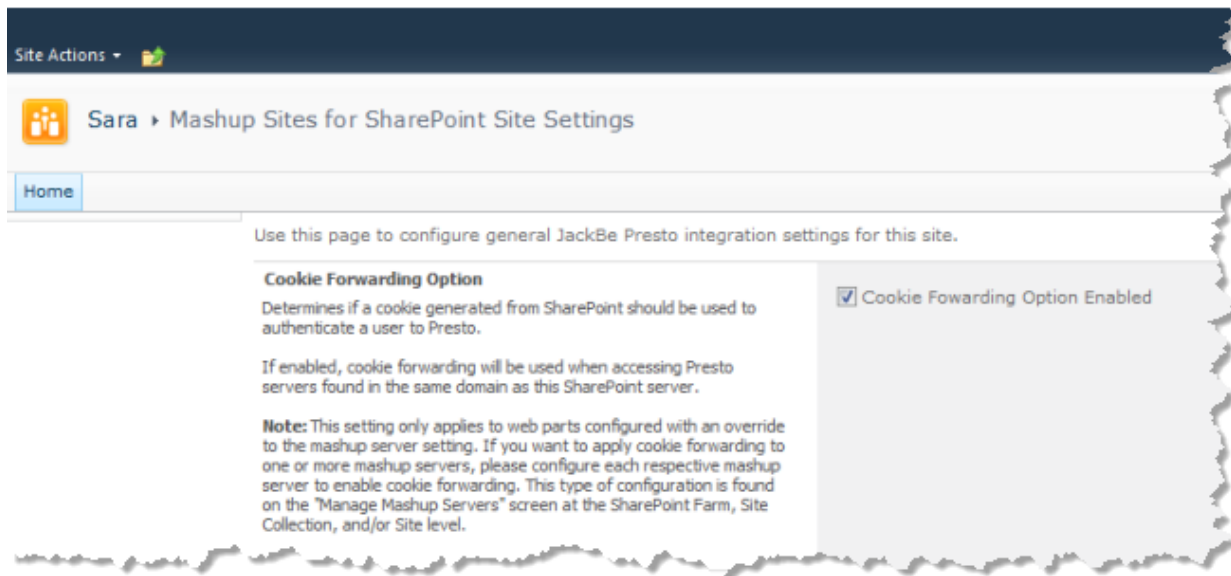
4. Once the connection is confirmed, click **Ok**.

Disabling Cookie Forwarding for Mashup Server Overrides

When users choose the preconfigured Mashup Server connection in Web Parts, all aspects of the connection including authentication is defined in the connection. With user overrides, cookie forwarding is enabled by default.

If you are using No SSO + Manual authentication, you should disable cookie forwarding for user overrides. You do this in site settings for a site collection or a specific site.

1. Login is as site administrator for the site collection or specific site.
2. Click **Site Actions > Site Settings**.
3. Click **Mashup Sites for SharePoint Site Settings**.
4. Clear the **Cookie Forwarding Option Enabled** option and click **OK**.



Setting the Default Sandbox Mode for Apps

The default Sandbox mode determines whether Apps are automatically isolated (in a sandbox) or not (embedded) in a Web Part page. You should apply a sandbox (isolate Apps) if publishing Apps into the Web Part Page typically changes the layout of the Web Part Page.

Note: users can override this property for individual Apps when they publish Apps to a Web Part page.

To set the default Sandbox mode:

1. Login is as site administrator for the site collection or specific site.
2. Click **Site Actions > Site Settings**.
3. Click **Mashup Sites for SharePoint Site Settings**.
4. Clear or set the **Default to Sandbox** option and click **OK**.

Farm and Site Administration

In addition to the basic configuration steps, SharePoint farm and site administrators can view version information for:

- ▶ Mashup Sites for SharePoint
- ▶ .Net Framework

This information is useful if you need to contact JackBe technical support.

For farms, open Central Administration as a farm administrator. Select **Application Management** and click **Mashup Sites for SharePoint Sites Settings** in the JackBe Presto Administration section.

For site collections or sites, login as the site administrator and click **Site Actions > Site Settings**. Click **Mashup Sites for SharePoint Site Setting** to view this information or set other site-wide properties. See [Disabling Cookie Forwarding for Mashup Server Overrides](#) or [Setting the Default Sandbox Mode for Apps](#) for more information.