Glyma Deployment Instructions

Version

Copyright 2015 Christopher Tomich and Paul Culmsee and Peter Chow

Licensed under the Apache License, Version 2.0 (the "License"); you may not use this file except in compliance with the License. You may obtain a copy of the License at

http://www.apache.org/licenses/LICENSE-2.0

Unless required by applicable law or agreed to in writing, software distributed under the License is distributed on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied. See the License for the specific language governing permissions and limitations under the License.

This code can be obtained from https://github.com/chris-tomich/Glyma

Table of Contents

[Introduction 1](#_Toc424208670)

[Pre-Requisites 1](#_Toc424208671)

[Purpose of Document 1](#_Toc424208672)

[Intended Audience 1](#_Toc424208673)

[Manual Deployment Process 2](#_Toc424208674)

[Deploy Glyma SharePoint Solutions to SharePoint Farm 2](#_Toc424208675)

[Provision the Glyma Node Service application 4](#_Toc424208676)

[Provision the Glyma Export Timer Job 8](#_Toc424208677)

[Create the Glyma Databases 9](#_Toc424208678)

[Provision the Glyma search custom connector 11](#_Toc424208679)

[Registering the Glyma search custom connector 11](#_Toc424208680)

[Configuring the Search schema 13](#_Toc424208681)

[Creating a Glyma content source 17](#_Toc424208682)

[Configure a SharePoint site collection for Glyma 19](#_Toc424208683)

[Verify the deployment 28](#_Toc424208684)

[Scripted Deployment Process 32](#_Toc424208685)

[Execute the scripted deployment 32](#_Toc424208686)

[Restart the Glyma Node Services 33](#_Toc424208687)

[Provision the Glyma search custom connector 33](#_Toc424208688)

[Creating a Glyma content source 34](#_Toc424208689)

[Configure a SharePoint site collection for Glyma 34](#_Toc424208690)

[Verify the deployment 34](#_Toc424208691)

[Manual Rollback Process 35](#_Toc424208692)

[Revert the configuration of the site collection 35](#_Toc424208693)

[De-activate features in the site collection 35](#_Toc424208694)

[Remove the files deployed to the site collection. 35](#_Toc424208695)

[Remove the Glyma Node Service application 35](#_Toc424208696)

[Remove the Glyma search custom connector 37](#_Toc424208697)

[Remove the Glyma SharePoint solutions 39](#_Toc424208698)

[Remove the Glyma databases 39](#_Toc424208699)

[Scripted Rollback Process 40](#_Toc424208700)

[Revert the configuration of the site collection 40](#_Toc424208701)

[De-activate features in the site collection 40](#_Toc424208702)

[Remove the files deployed to the site collection. 40](#_Toc424208703)

[Executed the scripted rollback 40](#_Toc424208704)

[Remove the Glyma search custom connector 41](#_Toc424208705)

[Remove the Glyma databases 41](#_Toc424208706)

[Troubleshooting 43](#_Toc424208707)

[Map Selection dialog box is not displayed in Glyma Mapping web part 43](#_Toc424208708)

[The Glyma Mapping web part is unable to communicate with the Glyma Node Service application 43](#_Toc424208709)

[The connectivity of a Site Collection to Glyma databases is misconfigured 46](#_Toc424208710)

[The Glyma database permissions are misconfigured 47](#_Toc424208711)

[The Glyma Security Context has not been set 47](#_Toc424208712)

[Unable to see the Export Tab in the Glyma Management Console 47](#_Toc424208713)

[Missing Glyma features in the site collection 47](#_Toc424208714)

[Appendix A: Glyma Architecture 49](#_Toc424208715)

[Glyma System Architectural Concepts and Overview 49](#_Toc424208716)

[Glyma Solution and Feature Architecture 49](#_Toc424208717)

[Glyma System Operations 51](#_Toc424208718)

[Glyma Security Framework 52](#_Toc424208719)

[Client-side Glyma Components 53](#_Toc424208720)

[Glyma Silverlight Application 53](#_Toc424208721)

[Glyma HTML 5 Viewer Application 54](#_Toc424208722)

[Glyma Pre-Requisites 54](#_Toc424208723)

[SharePoint Web Front End Server Glyma Components 54](#_Toc424208724)

[Glyma HTML 5 JSON Viewer Service 54](#_Toc424208725)

[Glyma SOAP Web Service 55](#_Toc424208726)

[SharePoint Application Server Glyma Components 55](#_Toc424208727)

[Glyma Node Service 55](#_Toc424208728)

[Glyma Databases 55](#_Toc424208729)

[Glyma Search Custom Connector 55](#_Toc424208730)

# Introduction

Glyma can be deployed in a number of configurations. This document describes the most complete option which includes components deployed to web front-end (WFE) servers, application servers and database servers in a SharePoint farm.

The deployment can be performed using a manual deployment process or a scripted deployment process. The scripted deployment process currently only performs a partial deployment of Glyma (using details in a XML configuration file) and requires some manual steps.

## Pre-Requisites

Glyma currently supports the following server software:

* SharePoint 2010 or SharePoint 2013
* SQL Server 2008 R2 or SQL Server 2012

Before you begin to install and configure Glyma, do the following:

* Read Appendix A to understand the Glyma architecture and how the various components interact
* Ensure you have Full-Text Indexing enabled on the database servers.
* Ensure you have a server with SQL Server Shared Management Objects (SMO) installed and PowerShell enabled to execute the Glyma database creation PowerShell Cmdlets.
* Ensure you have created or selected the web application to install Glyma onto
* Ensure the version of PowerShell is 2.0 or higher.

## Purpose of Document

The purpose of this document is to describe the deployment process for Glyma.

## Intended Audience

The intended audience of this document are system administrators and developers who have an understanding of SharePoint’s service application framework, the search service application and the solution deployment framework.

# Manual Deployment Process

Glyma is manually deployed using the steps below.

1. Deploy the Glyma SharePoint solutions to the SharePoint farm.
2. Create the Glyma databases.
3. Provision the Glyma Node Service application.
4. Provision the Glyma search custom connector.
5. Create a Glyma search content source.
6. Configure a SharePoint site for Glyma.
7. Verify the deployment.

## Deploy Glyma SharePoint Solutions to SharePoint Farm

1. Copy the Glyma SharePoint solutions to a SharePoint WFE or application server. Currently, the SharePoint solutions include:

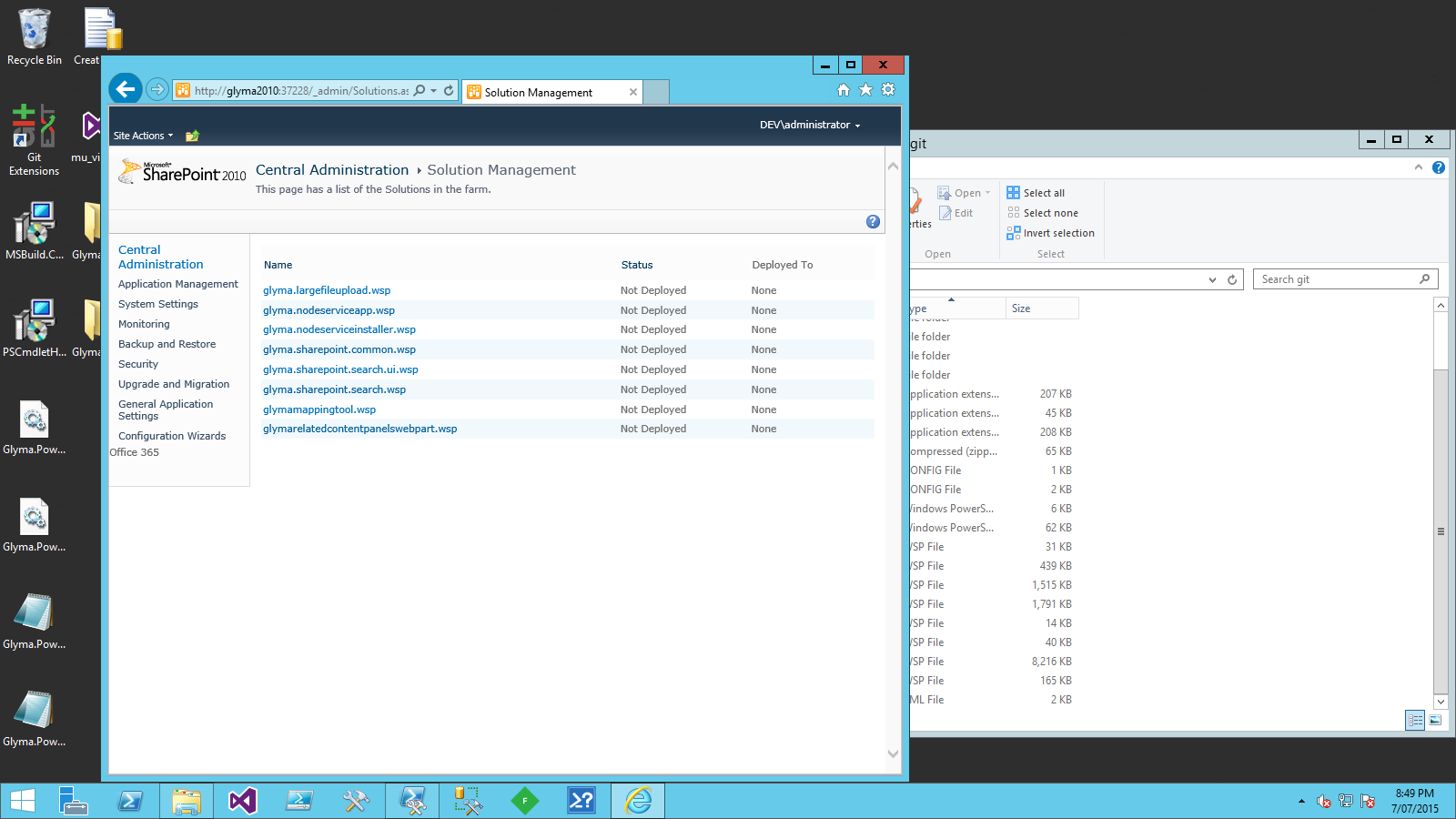
* Glyma.LargeFileUpload.wsp
* Glyma.NodeServiceApp.wsp
* Glyma.NodeServiceInstaller.wsp
* Glyma.SharePoint.Common.wsp
* GlymaMappingTool.wsp
* GlymaRelatedContentPanelsWebPart.wsp
* Glyma.SharePoint.Search.wsp
* Glyma.SharePoint.Search.UI.wsp

Note: Consult figure 1 in appendix A for a description of each of these components.

1. Deploy each SharePoint solution to the SharePoint farm by following the steps below for each file.
   1. Open the SharePoint Management Shell as an administrator on the server with the SharePoint solutions.
   2. Change the directory to the folder containing the SharePoint solutions.
   3. Execute the PowerShell command below to add the solution to the SharePoint solution store:

Add-SPSolution –LiteralPath <path to SharePoint solution file>

* 1. Open SharePoint Central Administration.
  2. Click the System Settings link in the Quick Launch.
  3. Click on the Manage farm solutions link and confirm the Glyma solution files are available to be deployed as per the diagram on the next page.

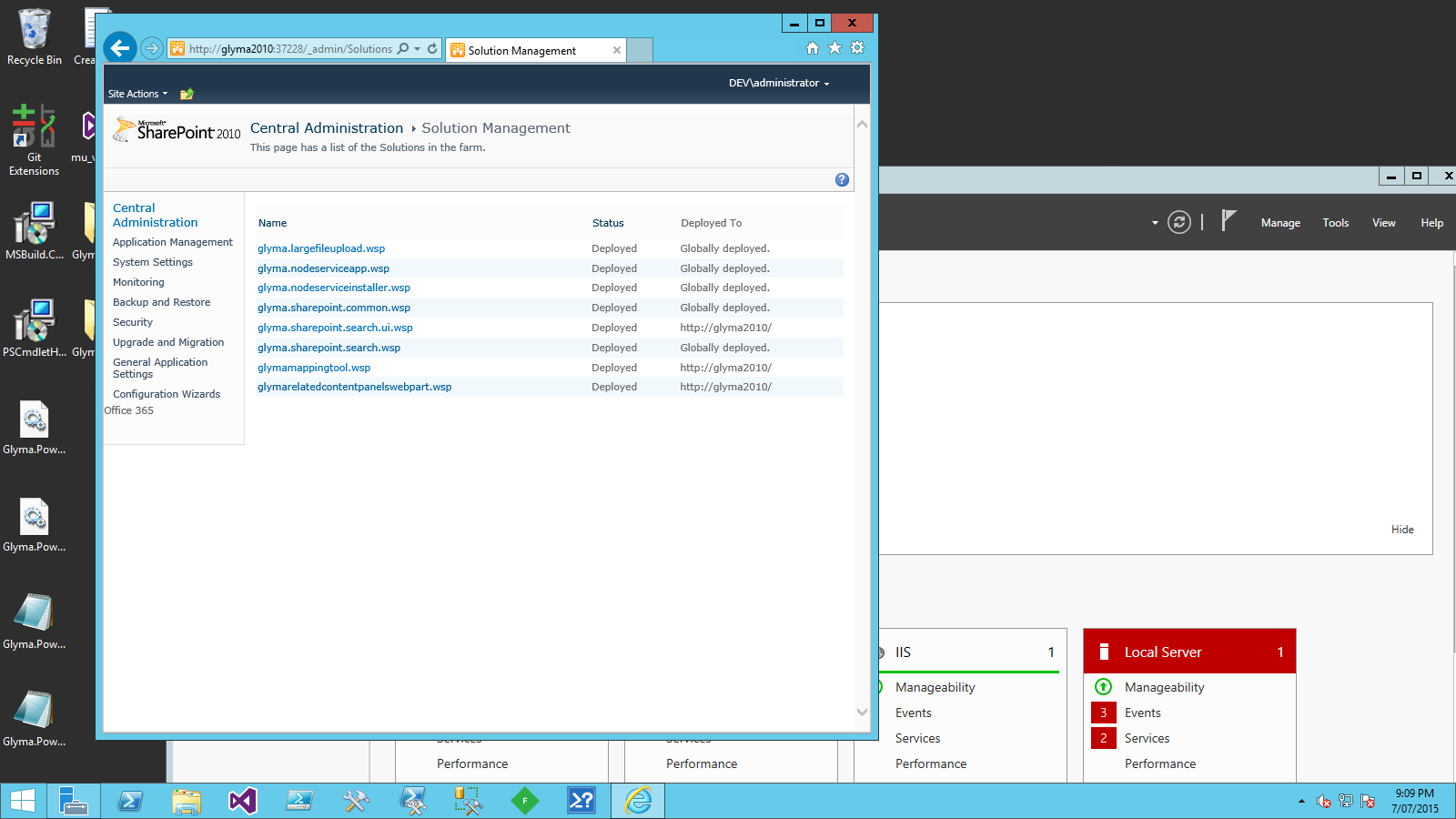


* 1. Click on the link for the SharePoint solution and deploy the SharePoint solution.

Some solutions are deployed globally and some are deployed to a particular web application. The implication is that you cannot deploy the latter solutions until you have created a web application.

Note: The solutions that need to be deployed to a particular web application are typically those that need to add safe control entries for the included web parts and controls to the web.config file. For example:

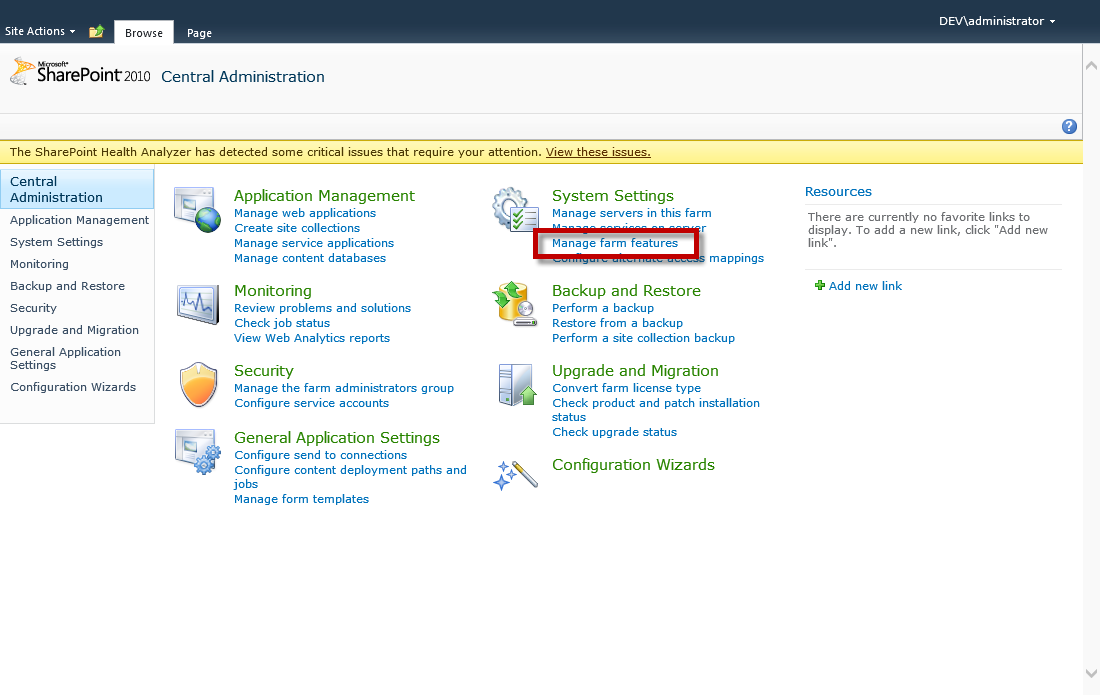
* Glymamappingtool.wsp
* GlymaRelatedContentPanelWebPart.wsp
* Glyma.SharePoint.Search.UI.wsp



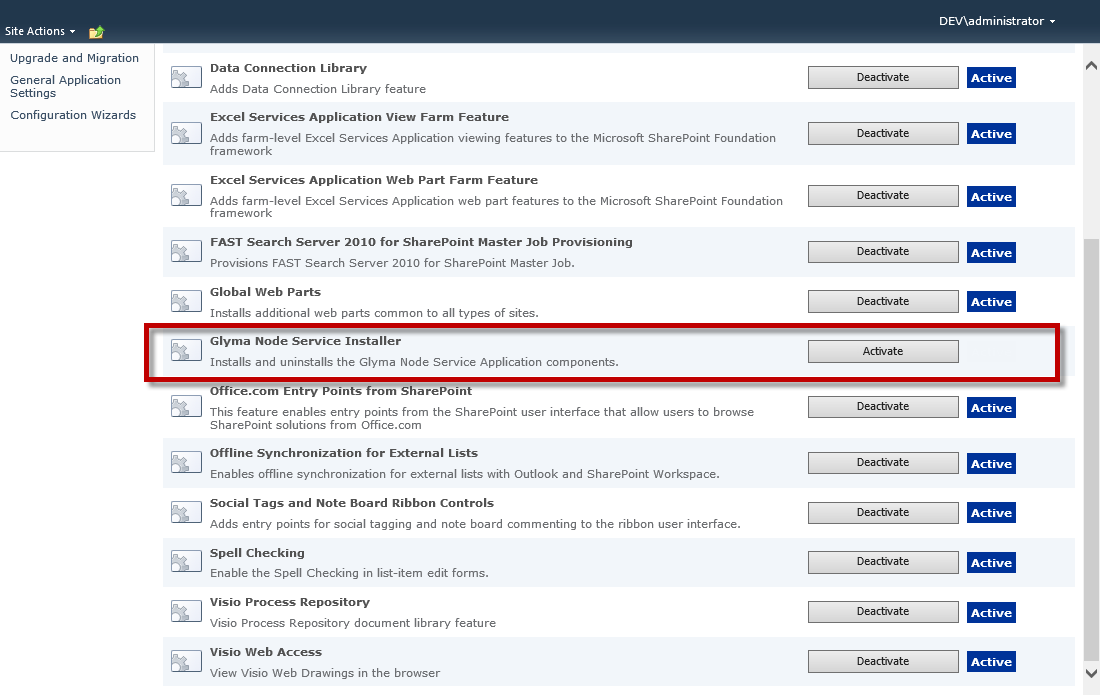
## Provision the Glyma Node Service application

Open SharePoint Central Administration and perform the following steps to provision the Glyma Node Service Application:

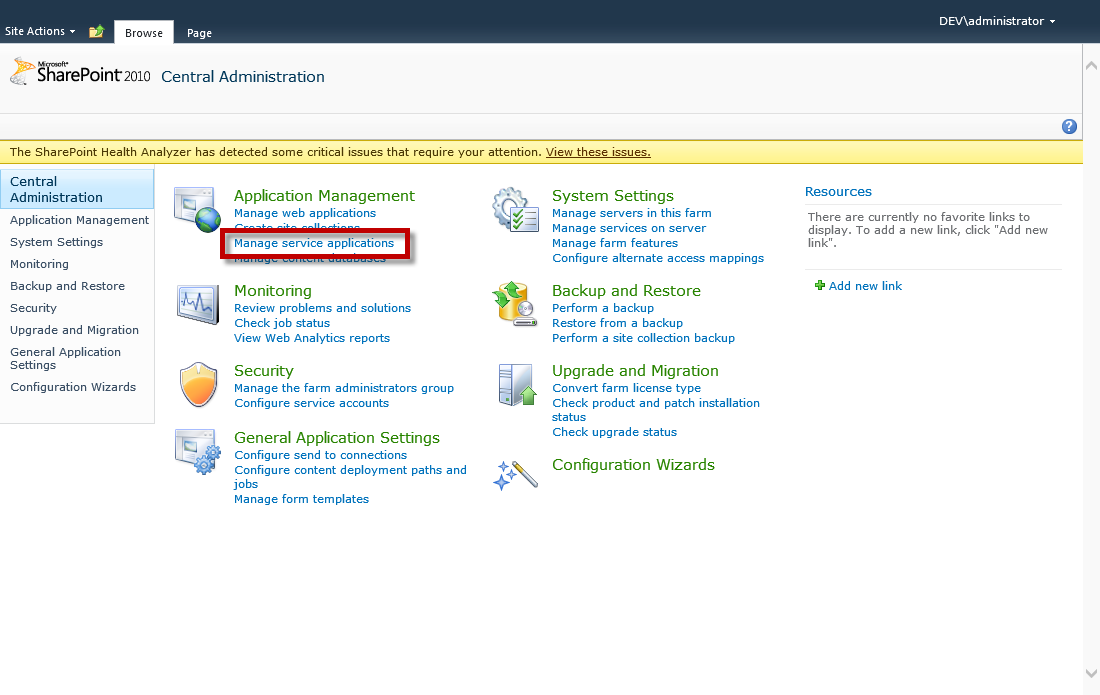
1. On the main Central Administration pag e, go to “Manage farm features” under “System Settings”.



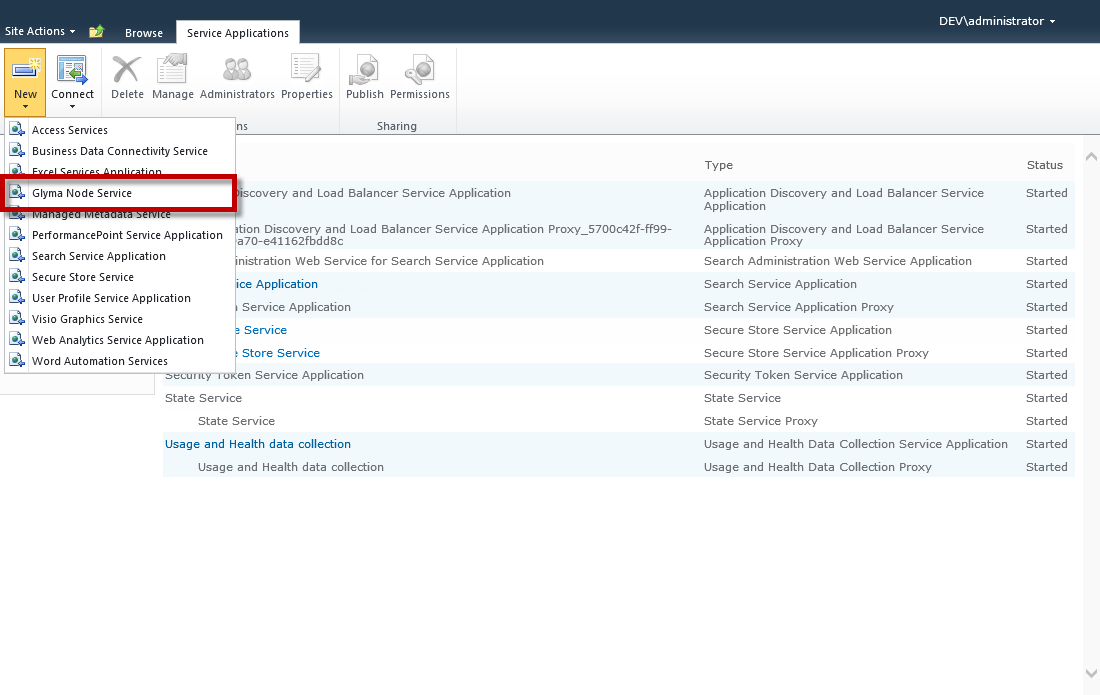
1. Activate the “Glyma Node Service Installer” feature.



1. On the main Central Administration page, go to “Manage service application” under “Application Management”.

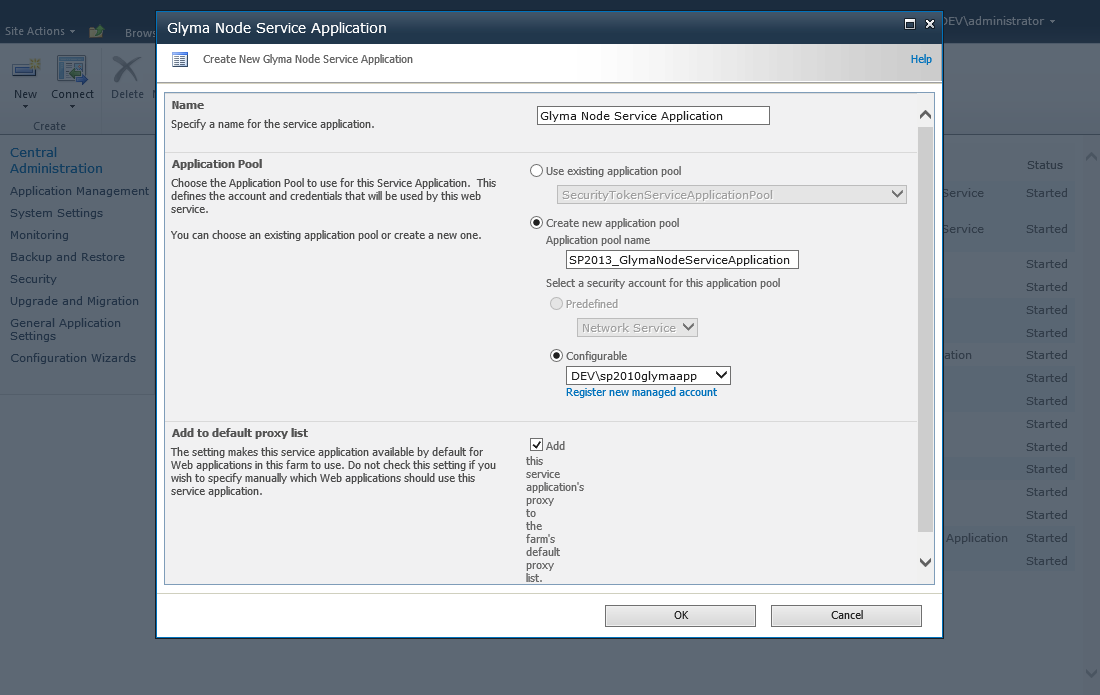


1. On the “Manage Service Applications” page, click on “New” and click on “Glyma Node Service”.

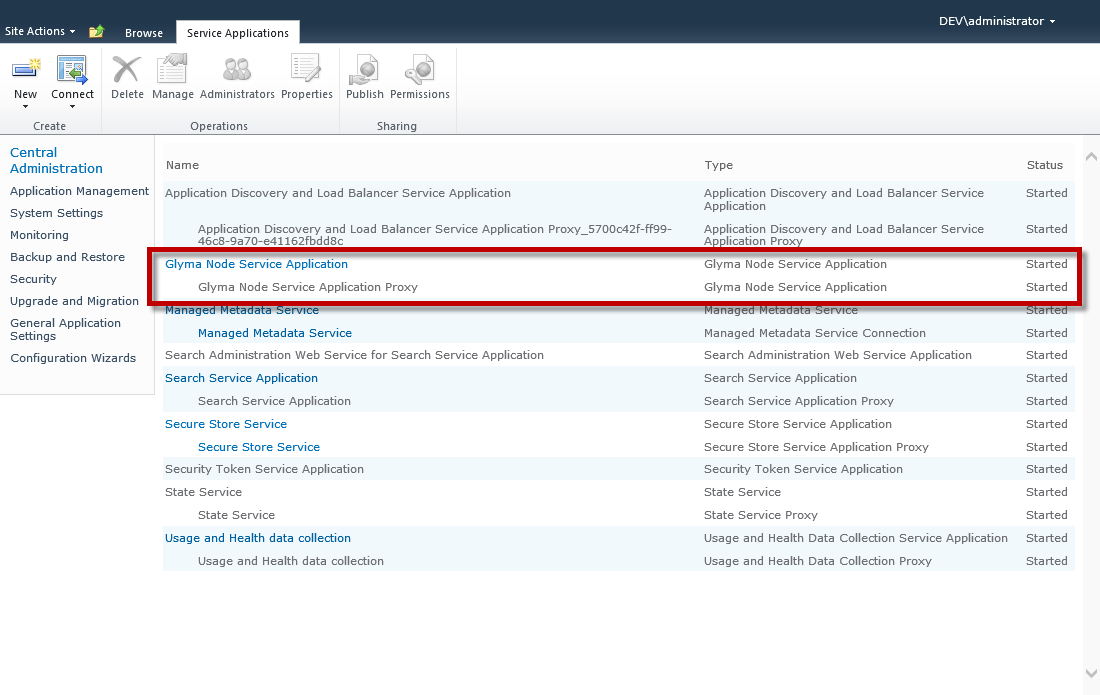


1. Fill in the details for the new Application Service.

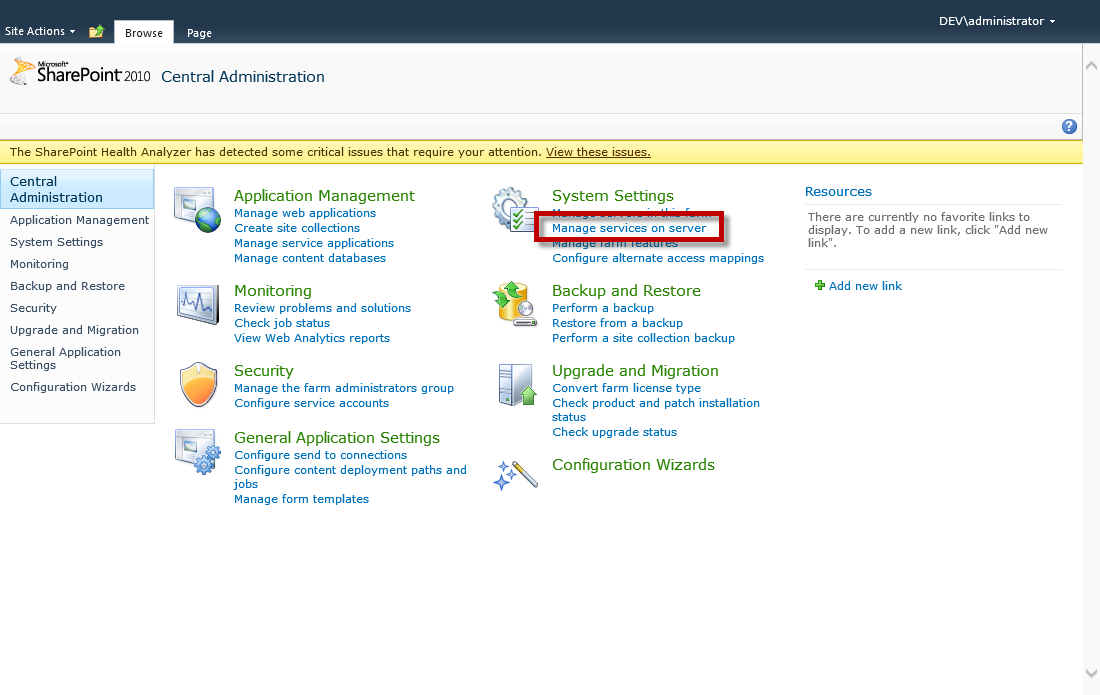
Note: Ensure the account that is used in the “Application Pool” area of this form is the account that is used for the “-GlymaServiceApplicationPoolAccount” parameter value for the “New-GLDatabase” Cmdlet used in step 5 of the **“**Create the Glyma Databases**”** section of this document.



1. Press “Ok” and the “Glyma Node Service Application” and the “Glyma Node Service Application Proxy” will now be provisioned.

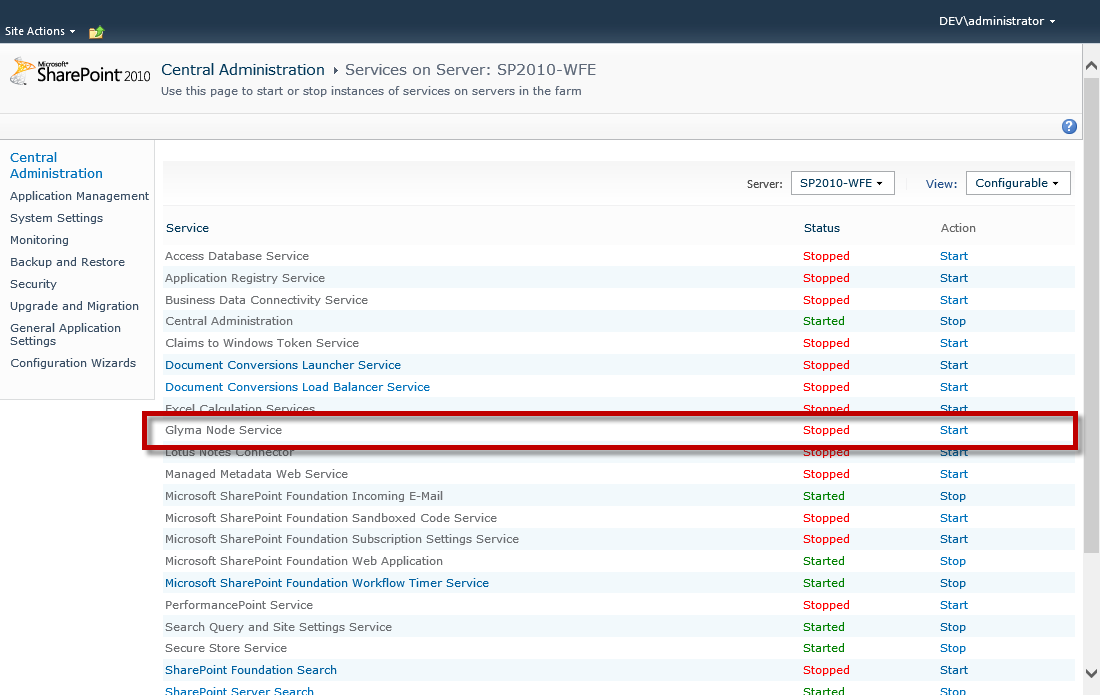


1. On the main Central Administration page, go to “Manage services on server” under “System Settings”.



1. Restart the “Glyma Node Service” on all the servers that will run the service (this will usually be the application servers). The process of starting and stopping the services may take between 5 – 10 minutes.

Note: By default, some of the servers may already have the “Glyma Node Service” started. If the server doesn’t require this service to be running e.g. a WFE server, you may stop this service.



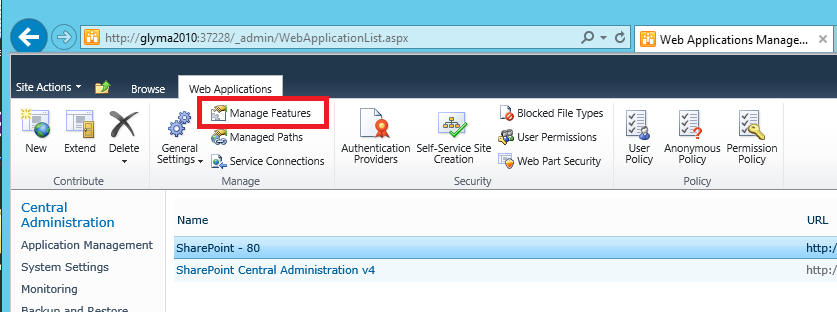
1. If you’re upgrading Glyma from a previous version, you will also need to perform an IIS reset on all the servers running the “Glyma Node Service” service.

## Provision the Glyma Export Timer Job

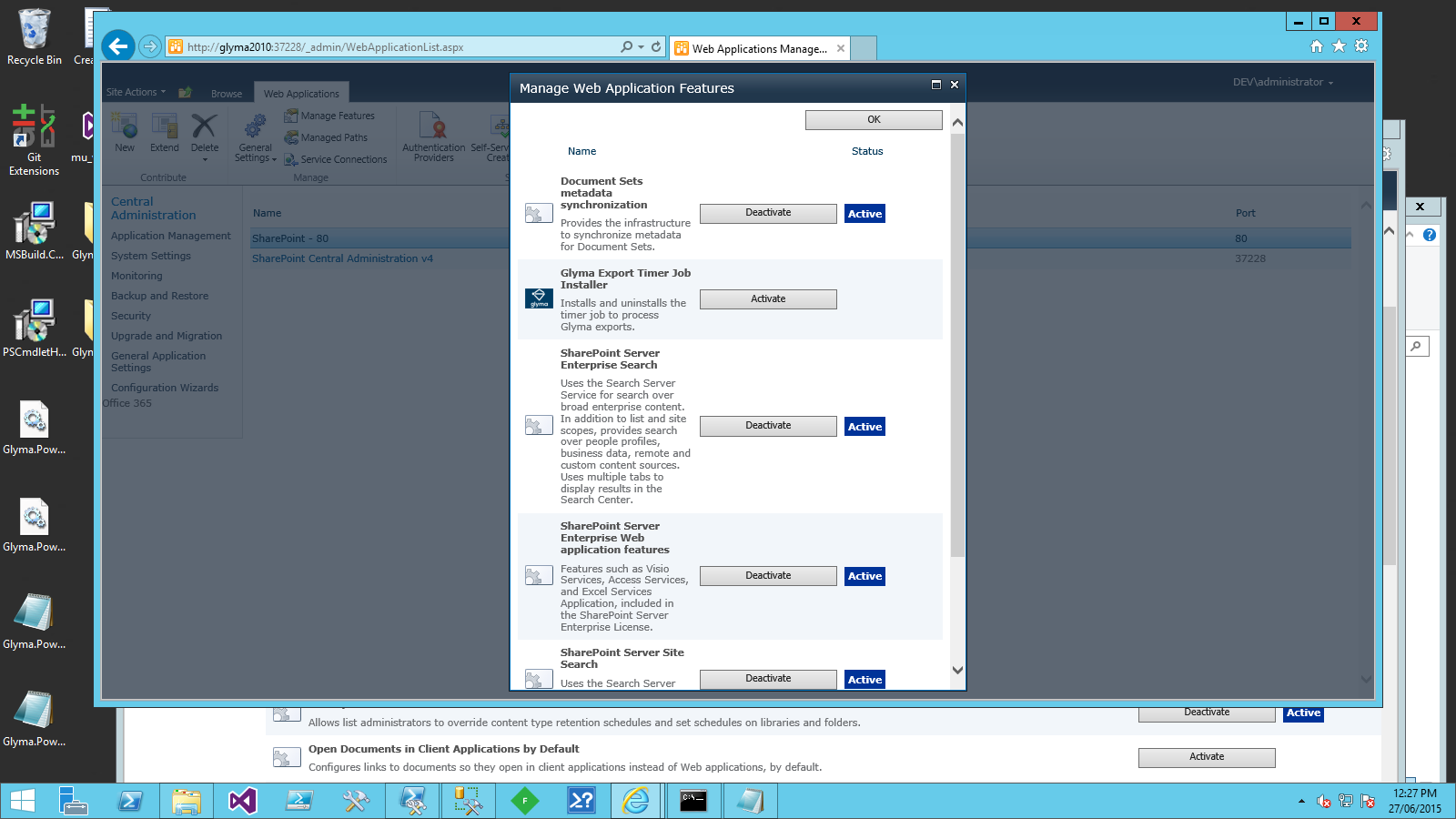
Glyma provides the ability to export maps to Word, PDF or Compendium formats. To enable this functionality, each web application that will be hosting Glyma maps needs to be configured.

Open SharePoint Central Administration and perform the following steps to provision the Glyma Export Timer Job:

1. On the main Central Administration page, go to “Manage Web Applications” under “Application Management”.
2. Select the appropriate web application and choose Manage Features from the ribbon



1. Activate the Glyma Export Timer Job feature



## Create the Glyma Databases

A set of Glyma database are typically created for each site collection. They are accessed by the:

* Glyma node service application
* The application pool account for the web applications Glyma is deployed to
* The SharePoint search crawler account.

Ensure you know the names for these accounts as Glyma will grant them permissions to the database. *Note: You do not need the password for these accounts.*

The Glyma databases are deployed by performing the steps below.

Note: You must have the SQL Server SMO installed to perform this operation.

If you are performing these steps on a *non -SharePoint server*, perform the initial steps below.

1. Copy the files, Glyma.Powershell.dll and Glyma.Powershell.SharePoint.dll, to the server.
2. Open a PowerShell console as an administrator.
3. Import the Glyma PowerShell modules by executing the following commands:

Import-Module "<Path to assembly>\Glyma.Powershell.dll"

Import-Module "<Path to assembly>\Glyma.Powershell.SharePoint.dll"

Go to step 4.

If you are performing these steps on a SharePoint server, perform the initial step below.

1. Open a SharePoint Management Shell as an administrator.
2. Create the Glyma databases by executing the following command.

New-GLDatabase -DatabaseServer <DB Server Name> -WebApplicationPoolAccount <App pool account for SharePoint sites> -SearchCrawlAccount <Search content access account> -GlymaServiceApplicationPoolAccount <App pool account for Glyma Node Service Application> -MapDatabaseName <DB Name> -TransactionDatabaseName <Transaction DB Name> -SecurityDatabaseName <Security DB Name>

For example: Installing to a database server called SQL.

New-GLDatabase -DatabaseServer SQL -WebApplicationPoolAccount DOMAIN\spwebapp

-SearchCrawlAccount DOMAIN\spsearch

-GlymaServiceApplicationPoolAccount DOMAIN\spserviceapp

-MapDatabaseName GL\_map

-TransactionDatabaseName GL\_map\_transaction

-SecurityDatabaseName GL\_map\_security

Note: Take note the names of the SQL databases created in this command, as you will be needing them later in the deployment.

Note: If the above powershell command does not work, import the Glyma PowerShell modules as described in step 3

## Provision the Glyma search custom connector

The Glyma search custom connector is provisioned by:

* Registering the Glyma search custom connector on each server running the SharePoint search crawl component.
* Configuring the Search schema.
* Creating a Glyma content source.

### Registering the Glyma search custom connector

On **every** server running the SharePoint search crawl component, perform the following steps.

1. Copy the BCS model file, GlymaRepositoryModel.xml, to a folder on the server. This file defines how SharePoint interacts with the Glyma search custom connector and is loaded the first time the Glyma search custom connector is loaded. Changes to the file do not take effect until the SharePoint search service is restarted (and the Glyma search custom connector is re-loaded) on the server.

Note: This file can be stored in a shared location or copied to every server where the Glyma search custom connector is installed. The choice of location for this file affects the fault tolerance of the Glyma search custom connector. If the file is stored in a shared location and it becomes inaccessible for whatever reason, all Glyma search custom connectors will not be able to restart. If the file is stored on every server where the Glyma search custom connector is installed, each connector is only affected by the availability of its own BCS model file; however, any changes required to the file will need to be replicated to all servers.

1. Open the BCS model file in a text editor.
2. Change the SecurityConnectionString property to connect to the correct SQL server and to the Glyma security database.

<Property Name="SecurityConnectionString" Type="System.String">Server=**<Database Server Name>**;Database=**<Glyma Security Database Name>**;Integrated Security=True;</Property>

1. Find the sample LOBSystemInstance element.
2. Change the name attribute of the sample LOBSystemInstance to a meaningful name. This name will be used in the start address when defining a content source and in the URL of all nodes from this Glyma database.

<LobSystemInstance Name="Glyma">

<Properties>

<Property Name="ShowInSearchUI" Type="System.String">True</Property>

<Property Name="ConnectionString" Type="System.String">Server=**<Database Server Name>**;Database=**<Glyma Map Database Name>**;Integrated Security=True;</Property>

</Properties>

</LobSystemInstance>

Note: If you have multiple Glyma databases, you will have multiple LOBSystemInstance entries. Thus it is best to choose a name that matches the Glyma database being crawled. For example if you have a dedicated site collection for executive strategy development, and it has its own Glyma database, then LOBSystemInstance should be named something like “ExecStrategy”

Note: Take a note of the LOBSystemInstance name as you will be using it when you configure a content source in SharePoint later in this document

1. Change the ConnectionString property to connect to the required SQL Server and Glyma map database name.
2. Save the changes to the GlymaRepositoryModel.xml file.
3. In a SharePoint Management Shell running as an administrator, execute the PowerShell commands below.

$searchapp = Get-SPEnterpriseSearchServiceApplication

New-SPEnterpriseSearchCrawlCustomConnector -SearchApplication $searchapp -Name "Glyma Repository" -protocol glyma -ModelFilePath "<Model File Name>"

<Model File Name> - Full path to the BCS model file, GlymaRepositoryModel.xml, using a UNC path or local file path e.g. C:\Data\Glyma\GlymaRepositoryModel.xml.

1. Open a registry editor and go to the key:

* **For SharePoint 2010**:

[HKEY\_LOCAL\_MACHINE]\SOFTWARE\Microsoft\Office Server\14.0\Search\Setup\ProtocolHandlers.

* **For SharePoint 2013**:

[HKEY\_LOCAL\_MACHINE]\SOFTWARE\Microsoft\Office Server\15.0\Search\Setup\ProtocolHandlers.

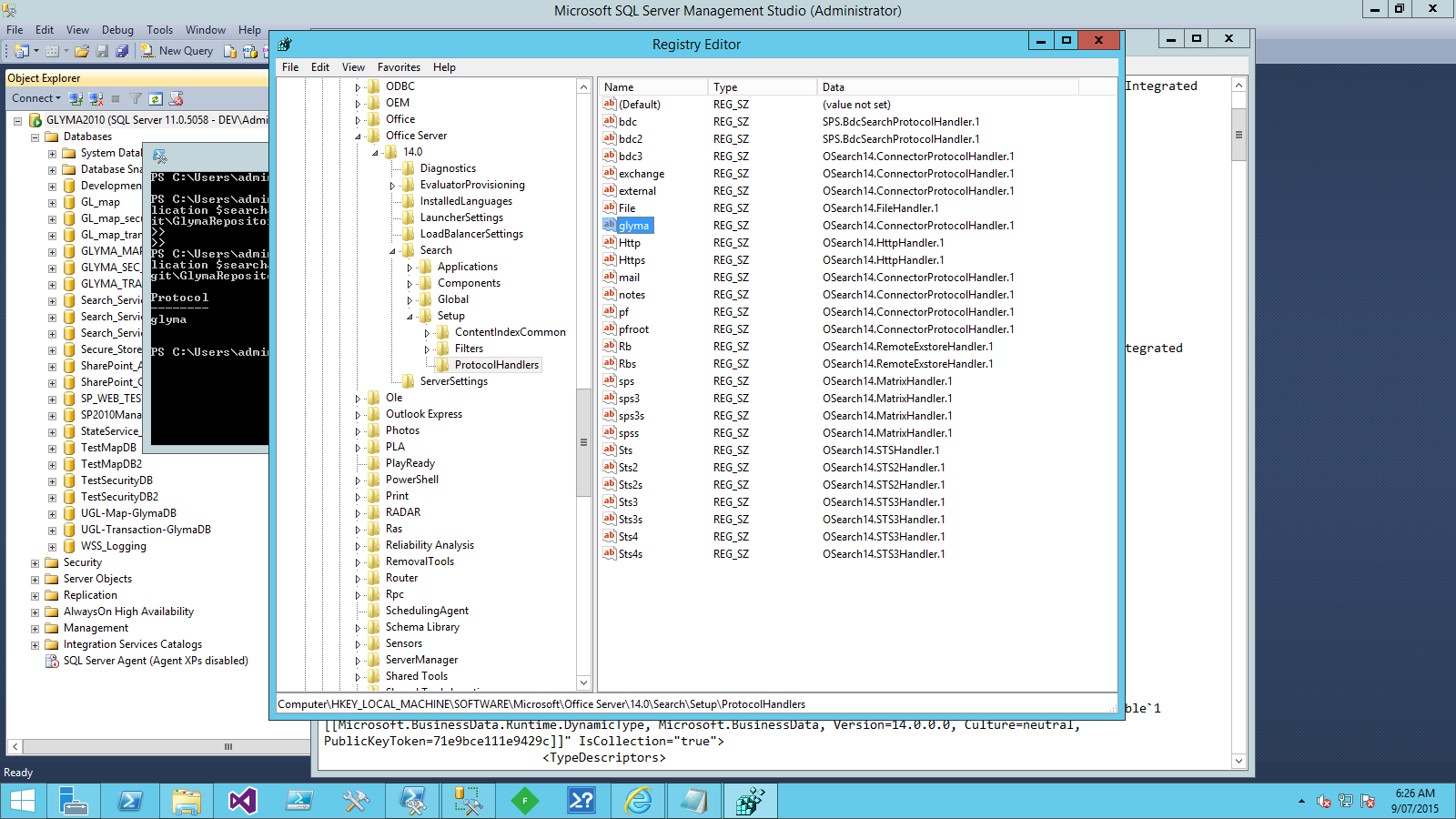
1. Add a new string value called: glyma.
2. Set the value of the string value to one of the values below.

* **For SharePoint 2010**:

OSearch14.ConnectorProtocolHandler.1.

* **For SharePoint 2013**:

OSearch15.ConnectorProtocolHandler.1.



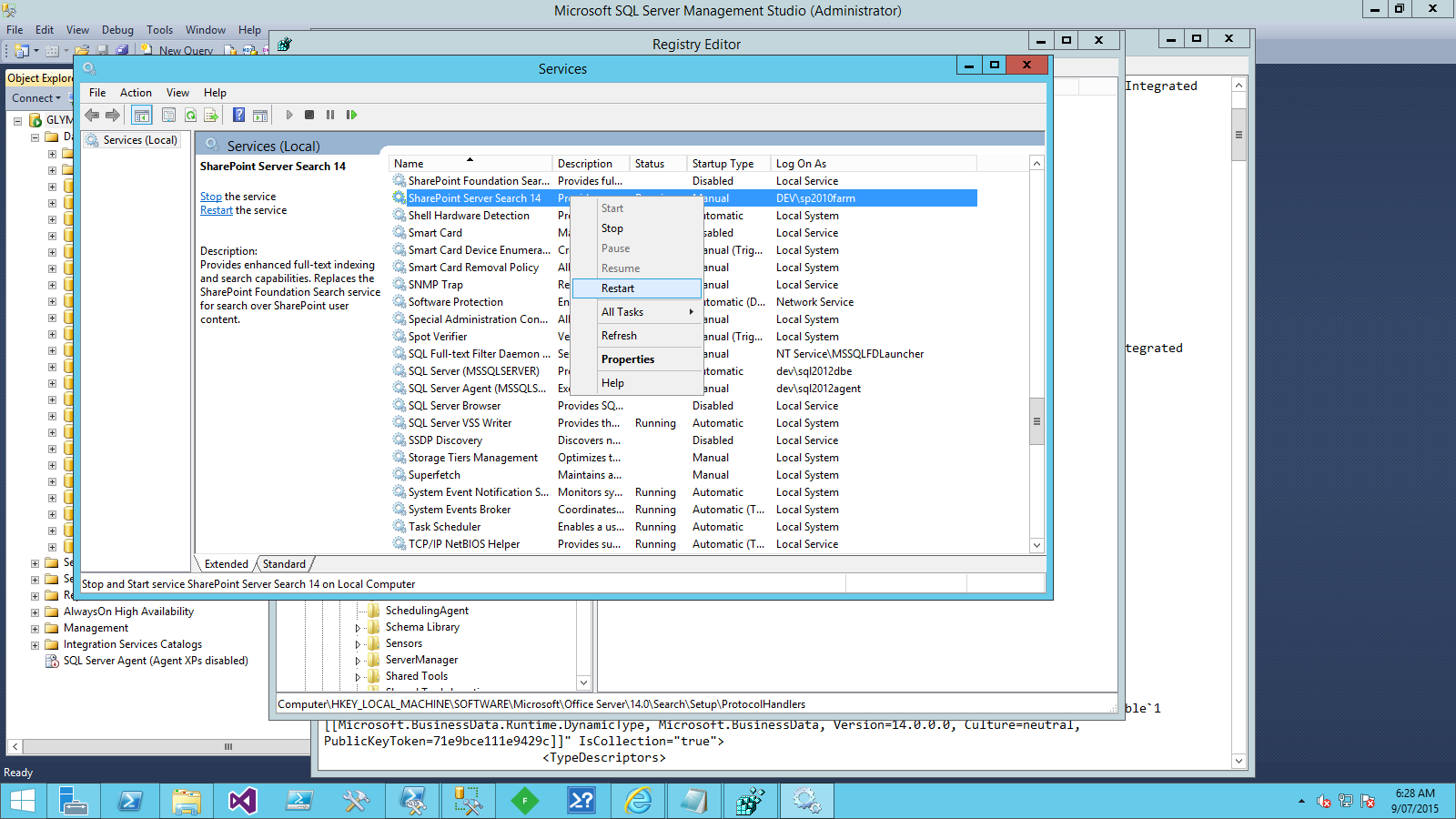
1. Restart the Windows service for SharePoint search to make the Search Service application aware of the new indexing connector.

* For SharePoint 2010:

SharePoint Server Search 14.

* For SharePoint 2013:

SharePoint Server Search 15.



1. For SharePoint 2013, ensure all Search Service application components have restarted and have returned to the running state.

### Configuring the Search schema

Glyma requires the deployment of crawled and managed properties to support a customised display of Glyma search results. These are installed by performing the steps below.

1. Copy the Glyma deployment PowerShell module files, GlymaDeployment.psm1 and GlymaDeployment.psd1, to a SharePoint WFE or application server.
2. Open the SharePoint Management shell as an administrator on the server with the Glyma deployment PowerShell module file.
3. Import the Glyma PowerShell modules by executing the commands below.

Import-Module "<Path to file>\GlymaDeployment.psd1"

1. Install the crawled properties and managed properties for Glyma by executing the command below.

Install-SPGLSearchSchema –searchAppName <Search Service Application Name>

Note: You can determine the search service application via Manage Service Applications in SharePoint Central Administration, or by executing the Get-SPEnterpriseSearchServiceApplication command and reviewing the Name property

1. Open SharePoint Central Administration.
2. In the Search Administration page, click on “Metadata Properties” and verify that the category, “Glyma Repository” exists with crawled properties for GlymaMap and GlymaNode entities, as shown in the diagram below.



Figure . Glyma crawled properties.

1. Click on the “Managed Properties” link in the toolbar to go to the “Metadata Property Mappings” page.
2. On the “Metadata Property Mappings” page, verify that the managed properties in the table below exist.

**For SharePoint 2010**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Name | Type | May be deleted | Used in scopes | Optimized | Mappings |
| GlymaRepositoryName | Text | Yes | Yes | No | GlymaMap.RepositoryName(Text), GlymaNode.RepositoryName(Text) |
| GlymaDomainId | Text | Yes | Yes | No | GlymaMap.DomainId(Text), GlymaNode.DomainId(Text) |
| GlymaDomainName | Text | Yes | Yes | No | GlymaMap.DomainName(Text), GlymaNode.DomainName(Text) |
| GlymaMapId | Text | Yes | Yes | No | GlymaMap.MapId(Text), GlymaNode.MapId(Text) |
| GlymaMapName | Text | Yes | Yes | No | GlymaMap.MapName(Text), GlymaNode.MapName(Text) |
| GlymaNodeId | Text | Yes | No | No | GlymaMap.Id(Text), GlymaNode.Id(Text) |
| GlymaNodeType | Text | Yes | Yes | No | GlymaMap.NodeType(Text), GlymaNode.NodeType(Text) |
| GlymaNote | Text | Yes | No | No | GlymaMap.Note(Text), GlymaNode.Note(Text) |
| GlymaContent | Text | Yes | No | No | GlymaMap.Content(Text), GlymaNode.Content(Text) |
| GlymaParentNodes | Text | Yes | No | No | GlymaMap.ParentNodes(Text), GlymaNode.ParentNodes(Text) |
| GlymaChildNodes | Text | Yes | No | No | GlymaMap.ChildNodes(Text), GlymaNode.ChildNodes(Text) |
| GlymaDescription | Text | Yes | No | No | GlymaMap.Description(Text), GlymaNode.Description(Text) |
| GlymaDescriptionType | Text | Yes | No | No | GlymaMap.DescriptionType(Text), GlymaNode.ChildNodes(Text) |

**For SharePoint 2013**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Name | Type | Search | Query | Retrieve | Refine | Sort | Mappings |
| GlymaRepositoryName | Text | Y | Y | Y | Y | Y | GlymaMap.RepositoryName(Text), GlymaNode.RepositoryName(Text) |
| GlymaDomainId | Text | Y | Y | Y | Y | Y | GlymaMap.DomainId(Text), GlymaNode.DomainId(Text) |
| GlymaDomainName | Text | Y | Y | Y | Y | Y | GlymaMap.DomainName(Text), GlymaNode.DomainName(Text) |
| GlymaMapId | Text | Y | Y | Y | Y | Y | GlymaMap.MapId(Text), GlymaNode.MapId(Text) |
| GlymaMapName | Text | Y | Y | Y | Y | Y | GlymaMap.MapName(Text), GlymaNode.MapName(Text) |
| GlymaNodeId | Text | Y | Y | Y |  |  | GlymaMap.Id(Text), GlymaNode.Id(Text) |
| GlymaNodeType | Text | Y | Y | Y | Y | Y | GlymaMap.NodeType(Text), GlymaNode.NodeType(Text) |
| GlymaNote | Text | Y | Y | Y |  |  | GlymaMap.Note(Text), GlymaNode.Note(Text) |
| GlymaContent | Text | Y | Y | Y |  |  | GlymaMap.Content(Text), GlymaNode.Content(Text) |
| GlymaParentNodes | Text | Y | Y | Y |  |  | GlymaMap.ParentNodes(Text), GlymaNode.ParentNodes(Text) |
| GlymaChildNodes | Text | Y | Y | Y |  |  | GlymaMap.ChildNodes(Text), GlymaNode.ChildNodes(Text) |
| GlymaDescription | Text | Y | Y | Y |  |  | GlymaMap.Description(Text), GlymaNode.Description(Text) |
| GlymaDescriptionType | Text |  |  | Y |  |  | GlymaMap.DescriptionType(Text), GlymaNode.ChildNodes(Text) |

1. At this stage, you are now able to perform a crawl of Glyma content.

### Creating a Glyma content source

1. Open SharePoint Central Administration.
2. Navigate to the Search Administration page.
3. Click on the “Content Sources” link in the Quick Launch.
4. On the “Manage Content Sources” page, click on “New Content Source” link.
5. Specify the properties in the table below.

|  |  |
| --- | --- |
| **Property** | **Value** |
| Name | Enter an appropriate name. |
| Content Source Type | Custom Repository |
| Type of Repository | Glyma Repository |
| Start Addresses | glyma://<Repository Name>  <Repository Name> is the name specified in the LOBSystemInstance element in the BDC model file. |
| Crawl Schedules | Define an appropriate crawl schedule.  NOTE: Only full crawls are currently supported. |
| Content Source Priority | Normal |
| Start Full Crawl | Unchecked. |

1. At this stage, you are now ready to perform a full crawl of your Glyma content.

## Configure a SharePoint site collection for Glyma

A SharePoint site collection is configured for Glyma by associating it with a set of Gllma databases, as well as establishing a security context for the site collection.

Note: For more details on the security context concept, see the section “Glyma Security Framework” in Appendix A.

Site collection configuration is performed via the following steps.

1. Associate the SharePoint site collection with a Glyma database.
   1. Open the SharePoint Management shell as an administrator on the server with the assemblies.
   2. Associate the site collection to the Glyma databases by executing the following command:

Set-SPGLSiteAssociation –Identity <Site Collection URL> -DefaultPageUrl <URL to page that will contain the Glyma Mapping Web Part> -DatabaseServer <Server Name> -MapDatabaseName <Map DB Name> -TransactionDatabaseName <Transaction DB Name> -SecurityDatabaseName <Security DB Name>

Note: The DefaultPageUrl is likely to be in a pages library using the publishing feature. Therefore the value is likely to be: http(s)://WebAppliation/Pages/glyma.aspx or something similar

Note: The DefaultPageURL does not have to be created in advance at this point.

For Example:

Set-SPGLSiteAssociation -Identity http://samplesite -DefaultPageUrl http://samplesite/pages/glyma.aspx -DatabaseServer SQL -MapDatabaseName GL\_map -TransactionDatabaseName GL\_map\_transaction ‑SecurityDatabaseName GL\_map\_security

Note: If the above PowerShell command does not work, import the Glyma PowerShell modules by executing the following commands:

Import-Module "<Path to assembly>\Glyma.Powershell.dll"

Import-Module "<Path to assembly>\Glyma.Powershell.SharePoint.dll"

* 1. Configure a new security context for the site collection be executing the following command:

New-SPGLSecurableContext <Site Collection URL> -SecurableContextName <A Name for the Securable Context>

Note: The SecurableContextName can be any string. As a good practice, consider naming it the same as the site collection URL. Consult the section “Glyma Security Framework” in Appendix A for more detail.

* 1. Set the Glyma map database for the new security context. This allows the Glyma search custom connector to identify the site collection administrators and to grant them permissions to view search results

Set-SPGLSecurableContextDatabase -DatabaseServer <Server Name> -SecurityDatabaseName <Security DB Name> –SiteCollectionUrl <Site Collection URL> -MapDatabaseName <Map DB Name>

Note: This step assumes you have provisioned the Glyma Search connector on the SharePoint Farm.

Note: If the above PowerShell command does not work, import the Glyma PowerShell modules by executing the following commands:

Import-Module "<Path to file>\GlymaDeployment.psd1"

1. Activate the following **site collection** features:

* SharePoint Server Standard Site Collection features
* SharePoint Server Publishing Infrastructure
* Glyma Pre-requisites
* Glyma Search Pre-requisites
* Glyma Mapping Tool
* Glyma Related Content Panels Web Part
* Glyma Branding

1. Activate the following site features:

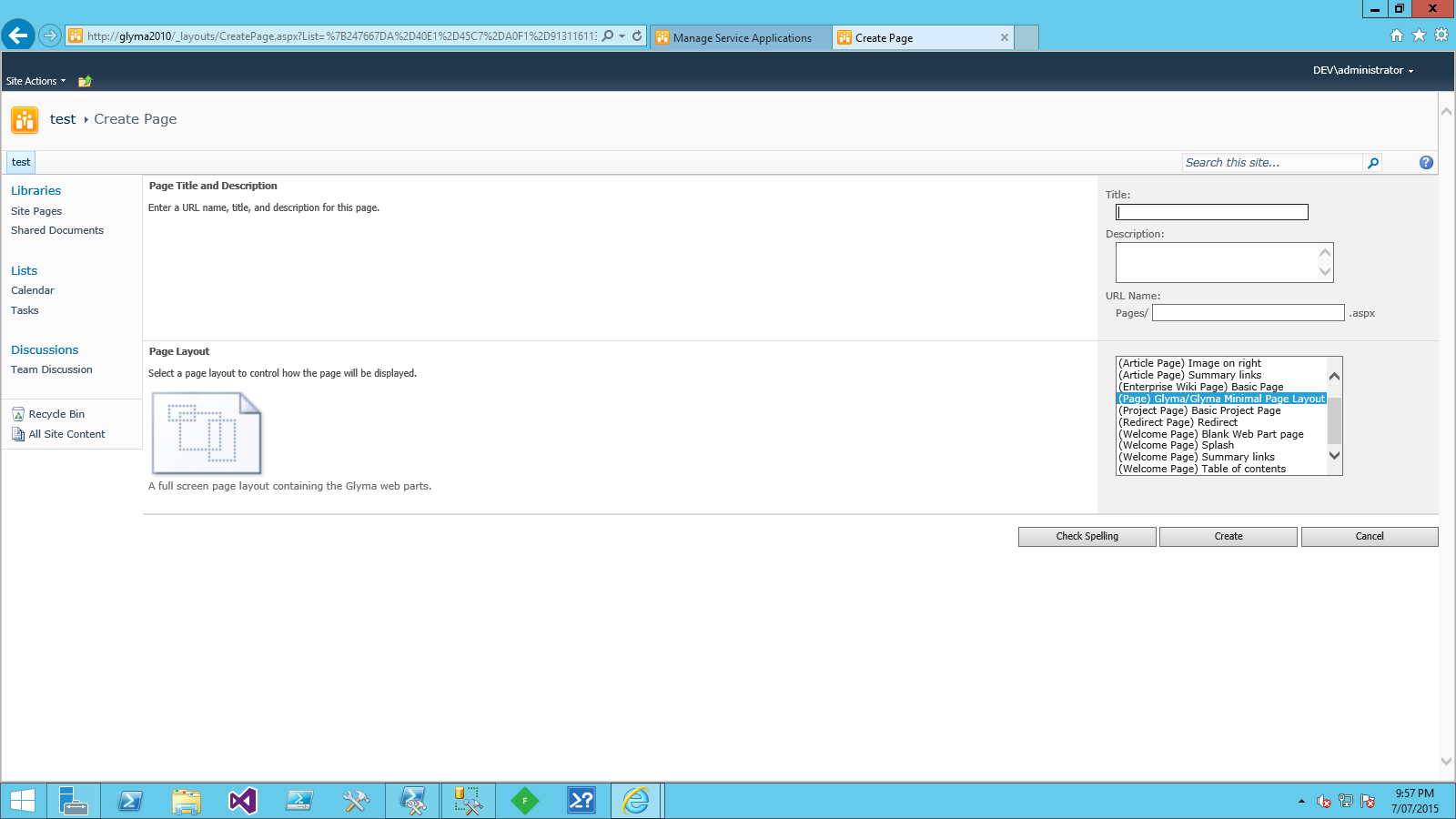
* SharePoint Server Publishing

1. Change the master page to one of the deployed Glyma master pages. The choice of master pages is described in the table below.

|  |  |
| --- | --- |
| Master Page | Description |
| glyma.master | Based on the standard SharePoint master page with additional references to JavaScript and CSS files required by Glyma. |
| glyma-yammer.master | An extension of glyma.master with additional references to JavaScript and CSS files required to support Yammer. |
| glyma-minimal.master | A highly styled master page that removes the standard SharePoint look-and-feel. |
| glyma-yammer-minimal.master | An extension of glyma-minimal.master with additional references to JavaScript and CSS files required to support Yammer. |

Alternatively, copy the CSS and JavaScript references in the Glyma master pages to your existing master page.

1. In the Pages document library, create a new web part page called, Glyma.aspx.



Note: If you choose the Glyma Minimal Page Layout, it already contains the Glyma web parts, so you can skip to step 7. This page layout can only be used with the **Glyma minimal master page**.

1. In the new Glyma.aspx page:
   1. Add the web part, Glyma Mapping Web Part, to a web zone in the main body of the page.
   2. Add the web part, Glyma Related Contents Panel, to a web part zone on the right hand side of the page.
2. Save the Glyma.aspx page and publish a major version.
3. At this stage, you are now able to open the Glyma.aspx page and use Glyma.
4. Create a sub-site for search using the Enterprise Search Center template.
5. To support the display of Glyma search results, the results page must have a reference to a jQuery library.

This can be done either by:

* including the reference in the master page used for the site; or by
* including the reference directly in the page using a Content Editor web part.

You can reference the version of the jQuery library deployed to the Style Library (under the folder: Glyma/Common) by the “Glyma Pre-requisites” site collection feature.

**For SharePoint 2010**

1. In the search sub-site, go to the Pages library and edit the page: results.aspx.
   1. Update the Refiner web part configuration.

|  |  |
| --- | --- |
| Property | Value |
| Filter Category Definition | Add the filter categories:  <Category Title="Node Type" Description="The type of node" Type="Microsoft.Office.Server.Search.WebControls.ManagedPropertyFilterGenerator" MetadataThreshold="2" NumberOfFiltersToDisplay="6" MaxNumberOfFilters="0" SortBy="Name" SortDirection="Ascending" SortByForMoreFilters="Name" SortDirectionForMoreFilters="Ascending" ShowMoreLink="True" MappedProperty="GlymaNodeType" MoreLinkText="show more" LessLinkText="show fewer"/>  <Category Title="Project" Description="The name of the project" Type="Microsoft.Office.Server.Search.WebControls.ManagedPropertyFilterGenerator" MetadataThreshold="2" NumberOfFiltersToDisplay="5" MaxNumberOfFilters="0" SortBy="Name" SortDirection="Ascending" SortByForMoreFilters="Name" SortDirectionForMoreFilters="Ascending" ShowMoreLink="True" MappedProperty="GlymaDomainName" MoreLinkText="show more" LessLinkText="show fewer"/>  <Category Title="Map" Description="The name of the map" Type="Microsoft.Office.Server.Search.WebControls.ManagedPropertyFilterGenerator" MetadataThreshold="2" NumberOfFiltersToDisplay="10" MaxNumberOfFilters="0" SortBy="Name" SortDirection="Ascending" SortByForMoreFilters="Name" SortDirectionForMoreFilters="Ascending" ShowMoreLink="True" MappedProperty="GlymaMapName" MoreLinkText="show more" LessLinkText="show fewer"/> |
| Accuracy Index | 500 |
| Number of Characters to Display | 25 |
| Use Default Configuration | Unchecked. |

* 1. Update the Search Core Results web part.

|  |  |
| --- | --- |
| Property | Value |
| Display Properties > Use Location Visualization | Unchecked |
| Display Properties > Fetched Properties | <Columns><Column Name="WorkId"/><Column Name="Rank"/><Column Name="Title"/><Column Name="Author"/><Column Name="Size"/><Column Name="Path"/><Column Name="Description"/><Column Name="Write"/><Column Name="SiteName"/><Column Name="CollapsingStatus"/><Column Name="HitHighlightedSummary"/><Column Name="HitHighlightedProperties"/><Column Name="ContentClass"/><Column Name="IsDocument"/><Column Name="PictureThumbnailURL"/><Column Name="PopularSocialTags"/><Column Name="PictureWidth"/><Column Name="PictureHeight"/><Column Name="DatePictureTaken"/><Column Name="ServerRedirectedURL"/><Column Name="GlymaRepositoryName"/><Column Name="GlymaDomainName"/><Column Name="GlymaDomainId"/><Column Name="GlymaMapName"/><Column Name="GlymaMapId"/><Column Name="GlymaNodeId"/><Column Name="GlymaNodeType"/><Column Name="GlymaNote"/><Column Name="GlymaContent"/><Column Name="GlymaParentNodes"/><Column Name="GlymaChildNodes"/></Columns> |
| Result Query Options > Enable Search Term Stemming | Checked |
| Miscellaneous > XSL Link | <Server relative URL to the GlymaSearchResults.xslt file>  For example:  /sites/SiteX/Style Library/Glyma/Search/Xsl/GlymaSearchResults.xslt. |

* 1. If a reference to the jQuery library is not included in the master page, add a hidden Content Editor web part with the following HTML content.

<script type="text/javascript" src="<Site collection path>/Style Library/Glyma/Common/jquery-1.10.2.min.js"></script>

1. Save the page, results.aspx, and ensure that it is published.
2. Configure the site collection search settings using the details below.

|  |  |
| --- | --- |
| Property | Value |
| Site Collection Search Center | <Server relative URL to Pages library in search site>  For example:  /sites/SiteX/search/pages |
| Site Collection Search Dropdown Mode | Show scopes dropdown |
| Site Collection Search Results Page | <Server relative URL to results page in search site>  /sites/SiteX/search/pages/results.aspx |

1. If the site collection is using a managed path e.g. http://ServerName/sites/SiteX:
   1. Go to the Style Library in the top-level site.
   2. Navigate to the folder: Glyma/Search/Xsl.
   3. Open the file: GlymaSearchResultsSiteSpecific.xslt.
   4. Modify the entry below to specify the server relative URL of the site collection.

<xsl:variable name="siteCollectionServerRelativeUrl" select="'<Site Collection Server Relative URL>'" />

For example, with a site collection at http://ServerName/sites/SiteX, the following entry is required.

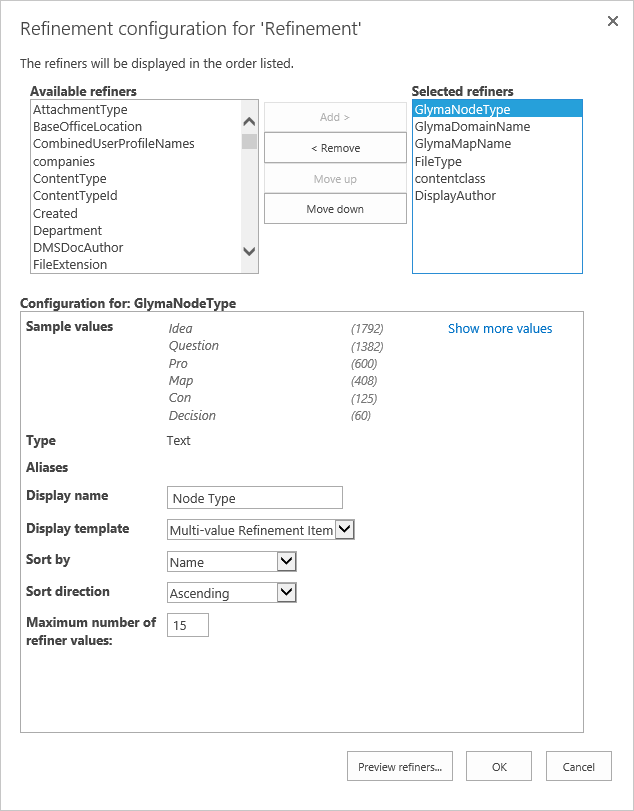
<xsl:variable name="siteCollectionServerRelativeUrl" select="'/sites/SiteX'" />

Note: The value must not have a trailing ‘/’ character.

**For SharePoint 2013**

1. In the search sub-site, go to the Pages library and edit the page: results.aspx.
2. Update the Refiner web part configuration.

|  |  |
| --- | --- |
| Refiner | Settings |
| GlymaNodeType | Display Name: Node Type  Display Template: Multi-value refinement item  Sort By: Name  Sort Direction: Ascending  Maximum number of refiner values: 15 |
| GlymaDomainName | Display Name: Project  Display Template: Refinement Item  Sort By: Name  Sort Direction: Ascending  Maximum number of refiner values: 15 |
| GlymaMapName | Display Name: Map  Display Template: Refinement Item  Sort By: Name  Sort Direction: Ascending  Maximum number of refiner values: 15 |

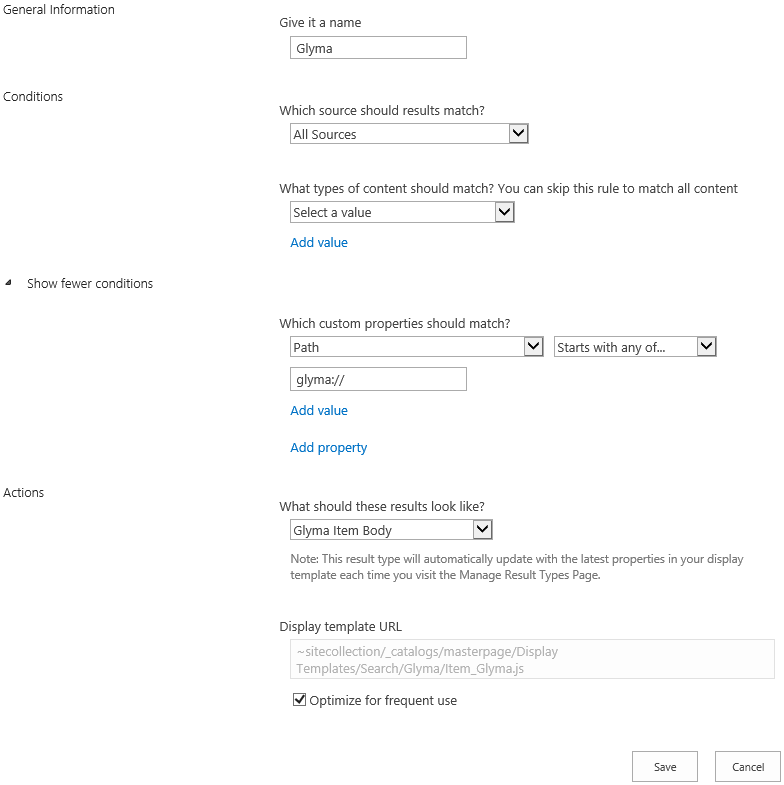


1. If a reference to the jQuery library is not included in the master page, add a hidden Content Editor web part with the following HTML content.

<script type="text/javascript" src="<Site collection path>/Style Library/Glyma/Common/jquery-1.10.2.min.js"></script>

1. Save the page, results.aspx, and ensure that it is published.
2. Create a new search result type for the site collection using the details below.

|  |  |
| --- | --- |
| Property | Value |
| General Information > Name | Glyma |
| Conditions | Path + Starts with any of… + glyma:// |
| Actions | Glyma Item Body  Optimize for frequent use |



1. Configure the site collection search settings using the details below.

|  |  |
| --- | --- |
| Property | Value |
| Enter a Search Centre URL | <Server relative URL to Pages library in search site>  For example:  /sites/SiteX/search/pages |
| Which search results page should queries be sent to? | Send queries to a custom results page URL |
| Results page URL | {SearchCenterURL}/results.aspx |

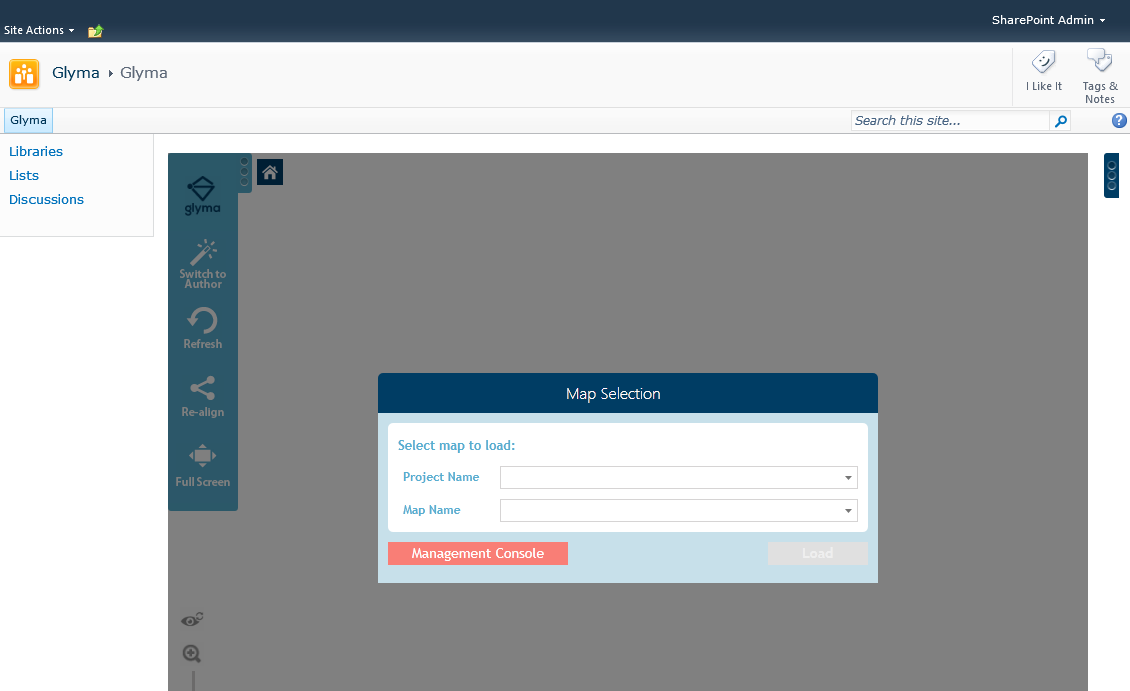
At this stage, you are now able to submit search queries and have Glyma search results displayed correctly (once you’ve created content and performed a full crawl).

## Verify the deployment

To test your Glyma deployment, perform the steps below.

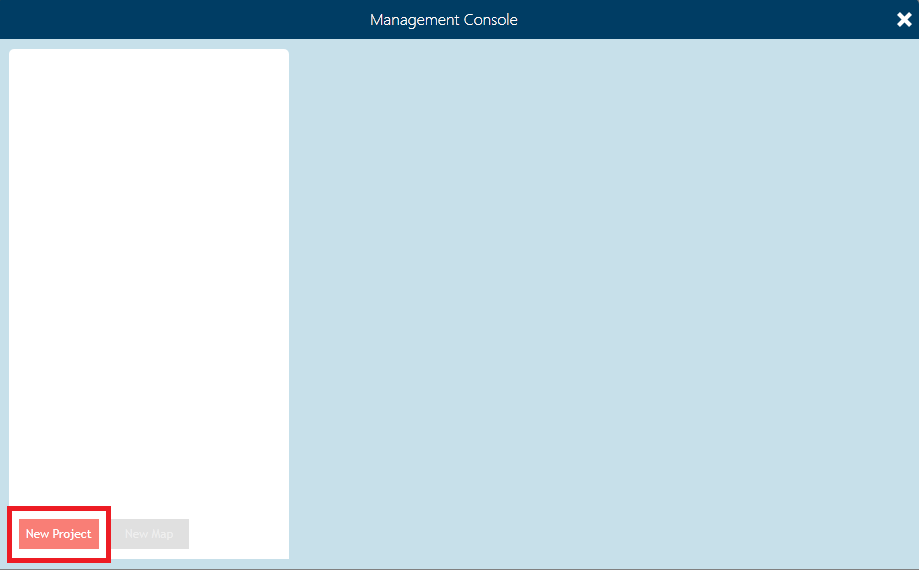
Open the Glyma.aspx page created in “Configure a SharePoint site collection for Glyma”.

1. The Glyma Mapping web part should display a “Map Selection” dialog box as shown in the diagram below.

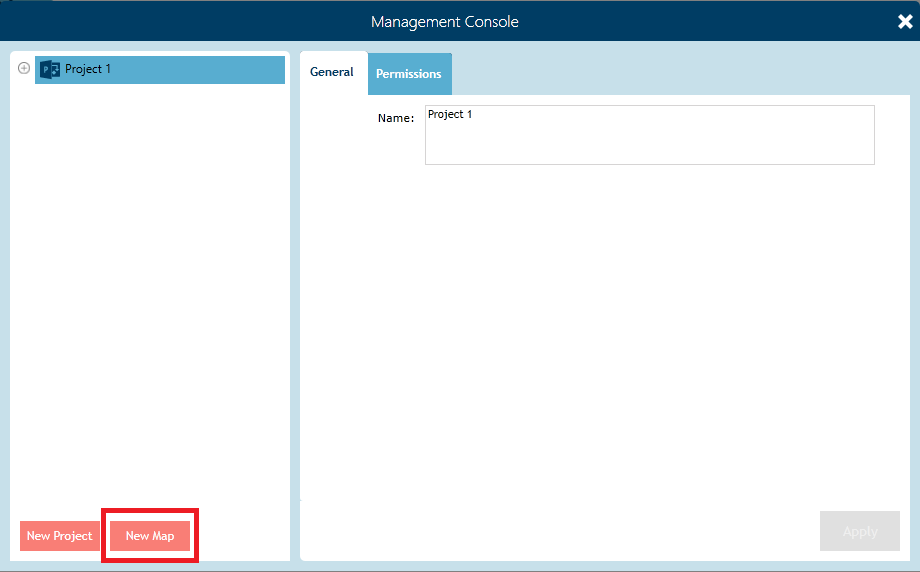


If the “Map Selection” dialog box is not displayed, please refer to the topic “Map Selection dialog box is not displayed in Glyma Mapping web part” in the “Troubleshooting” section of this document.

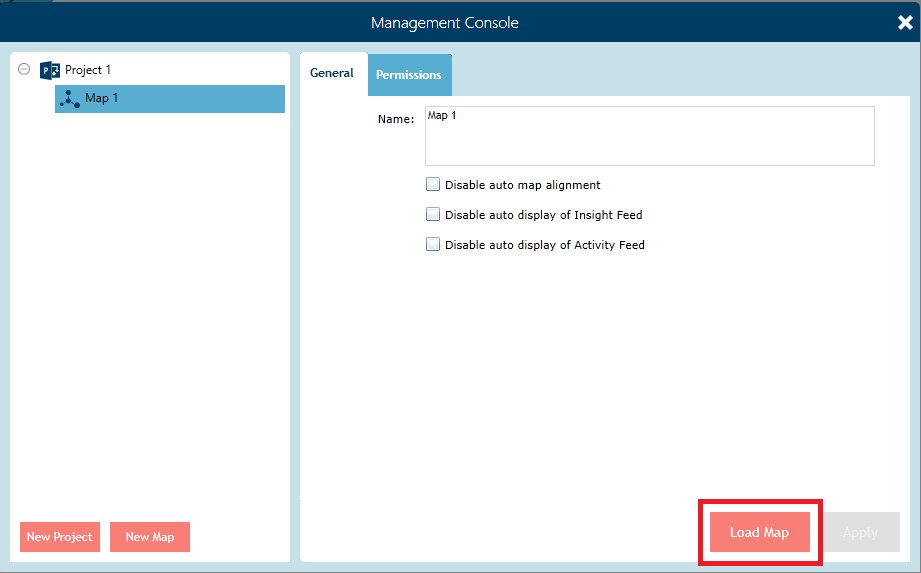
1. In the “Map Selection” dialog box, click on the Management Console button.
2. In the “Management Console”, create a new project by clicking on the “New Project” button.



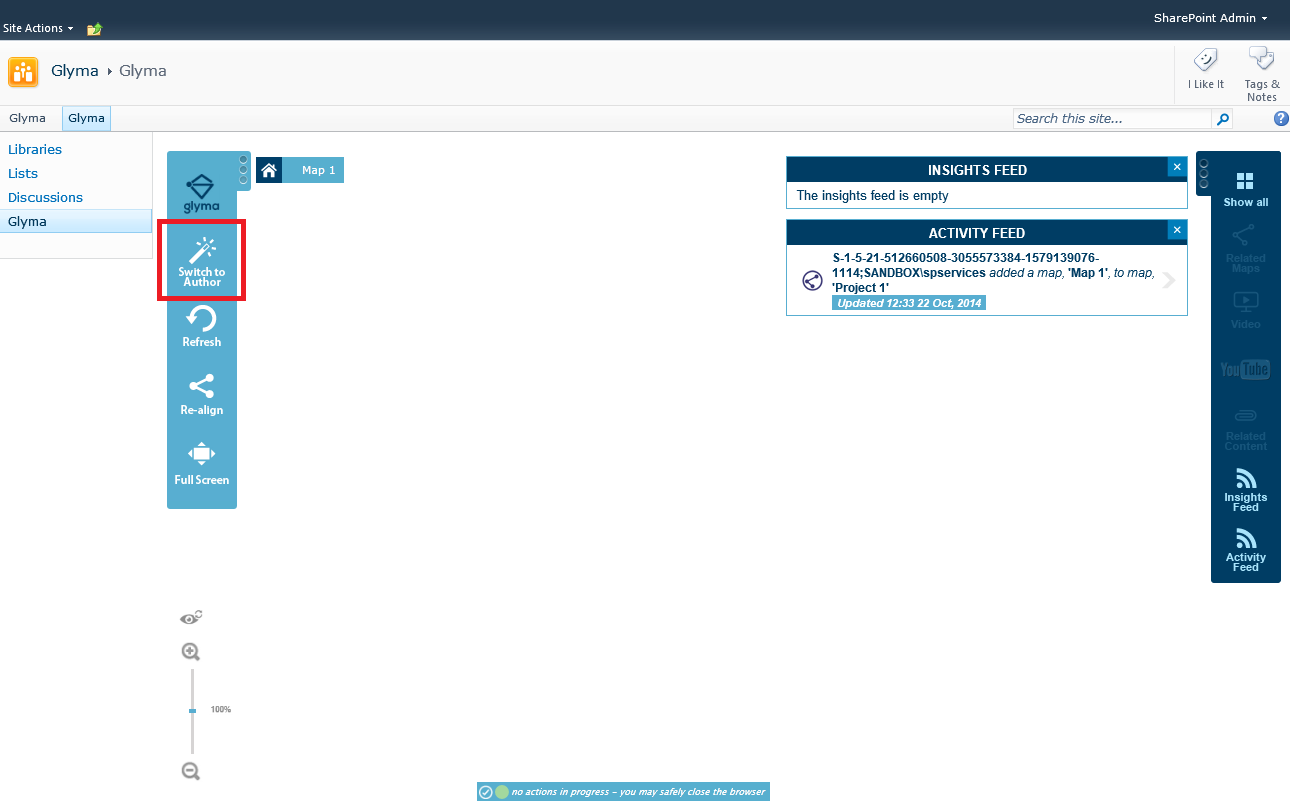
1. Select the new project and create a new map by clicking on the “New Map” button.



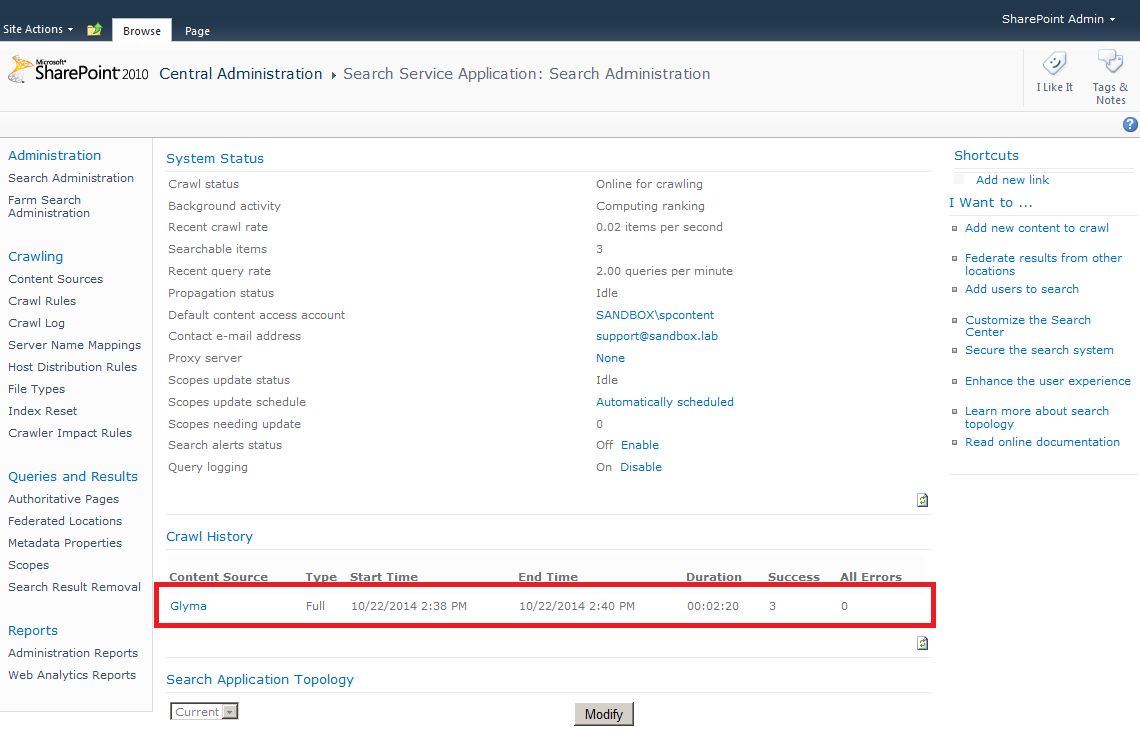
1. Select the new map and click the “Load Map” button to load the map.



1. The new map will be loaded and displayed. On the new map click the “Switch to Author” button and start adding nodes to the map.



1. At this stage, you have successfully confirmed Glyma’s authoring functionality. The next step is to confirm Glyma’s search functionality.
2. Open SharePoint Central Administration.
3. Navigate to the Search Administration page.
4. Click on the “Content Sources” link in the Quick Launch.
5. On the “Manage Content Sources” page, click on the Glyma content source and start a full crawl.
6. Open the Search Administration page and monitor the status of the crawl in the Crawl History section of the page. A successful crawl will have no errors reported.



1. Once a successful crawl has been completed, perform a search in the site collection. This should display all Glyma nodes that match the search criteria that you have permission to view.

# Scripted Deployment Process

Glyma currently supports a partial scripted deployment using details from a XML configuration file. The remainder of the deployment must be completed manually. The partial scripted deployment performs the steps below.

* Deploys the Glyma SharePoint solutions.
* Provisions the Glyma node service application.
* Configures the Search schema.
* Creates the Glyma databases.
* Associates a SharePoint site collection with the Glyma databases.

The scripted deployment process for Glyma is described below. You must have the SQL Server SMO installed to perform this process.

1. Execute the scripted deployment.
2. Restart the Glyma Node Services.
3. Provision the Glyma search custom connector.
4. Create a Glyma search content source.
5. Configure a SharePoint site collection for Glyma.
6. Confirm the deployment.

## Execute the scripted deployment

1. Copy the deployment files to a SharePoint WFE or an application server that has SQL SMO installed.

The PowerShell related deployment files include.

* Glyma.Powershell.dll
* Glyma.Powershell.SharePoint.dll
* GlymaDeployment.psm1
* GlymaDeployment.psd1
* GlymaDeploymentConfiguration.xml

The SharePoint solutions include:

* Glyma.NodeServiceApp.wsp
* Glyma.NodeServiceInstaller.wsp
* Glyma.LargeFileUpload.wsp
* Glyma.SharePoint.Common.wsp
* GlymaMappingTool.wsp
* GlymaRelatedContentPanelsWebPart.wsp
* Glyma.SharePoint.Search.wsp
* Glyma.SharePoint.Search.UI.wsp

1. Open the GlymaDeploymentConfiguration.xml file and specify the required settings.

Note: All settings in this file must have a valid value for the deployment environment.

1. Open a SharePoint Management Shell as an administrator.
2. Import the Glyma PowerShell modules by executing the commands below.

Import-Module "<Path to assembly>\Glyma.Powershell.dll"

Import-Module "<Path to assembly>\Glyma.Powershell.SharePoint.dll"

Import-Module "<Path to file>\GlymaDeployment.psd1"

1. Execute the scripted deployment by executing the command below.

Install-Glyma –configFilePath “<Path to GlymaDeploymentConfig.xml file>”

If you wish to log the scripted deployment, execute the command below.

Install-Glyma -configFilePath “<Path to GlymaDeploymentConfig.xml file>” -Verbose \*> "<Path to log file>"

1. Veriy that all Glyma SharePoint solutions have been deployed.

## Restart the Glyma Node Services

Please refer to steps 8 & 9 provided in “Provision the Glyma Node Service application” in the section “Manual Deployment Process”.

## Provision the Glyma search custom connector

Please refer to steps 1- 6 provided in “Registering the Glyma search custom connector” in the section “Manual Deployment Process”.

On **every** server running the SharePoint search crawl component, perform the following steps.

1. Copy the deployment files below to each server running the crawl component.

* GlymaDeployment.psm1
* GlymaDeployment.psd1
* GlymaDeploymentConfiguration.xml

1. Open a SharePoint Management Shell as an administrator.
2. Import the Glyma PowerShell modules by executing the commands below.

Import-Module "<Path to assembly>\Glyma.Powershell.dll"

Import-Module "<Path to assembly>\Glyma.Powershell.SharePoint.dll"

Import-Module "<Path to file>\GlymaDeployment.psd1"

1. Execute the scripted deployment by executing the command below.

Install-GlymaSearchCustomConnector –configFilePath “<Path to GlymaDeploymentConfig.xml file>”

Note: You don’t need to perform the steps described in “Configuring the Search schema” because the scripted deployment performs them.

## Creating a Glyma content source

Please refer to the steps provided in “Creating a Glyma content source” in the section “Manual Deployment Process”.

## Configure a SharePoint site collection for Glyma

Please refer to the steps provided in “Configure a SharePoint site collection for Glyma” in the section “Manual Deployment Process”.

Note: You don’t need to perform the first step of associating the SharePoint site collection with a Glyma database because the scripted deployment performs this.

## Verify the deployment

Please refer to the steps provided in “Verify the deployment” in the section “Manual Deployment Process”.

# Manual Rollback Process

Glyma is removed using the steps below.

1. Revert the configuration of the site collection.
2. De-activate features in the site collection.
3. Remove the files deployed to the site collection.
4. Remove the Glyma Node Service application.
5. Remove the Glyma search custom connector.
6. Remove the Glyma SharePoint solutions.
7. Remove the Glyma databases.

## Revert the configuration of the site collection

1. In the search sub-site, go to the Pages library and edit the page: results.aspx.
   1. Remove the changes made to the Refiner web part.
   2. Remove the changes made to the Search Core Results web part.
2. In the top-level site, change the master page to a non-Glyma master page.

## De-activate features in the site collection

1. De-activate the following site collection features:

* Glyma Mapping Tool
* Glyma Related Content Panels Web Part
* Glyma Branding
* Glyma Search Pre-requisites
* Glyma Pre-requisites

## Remove the files deployed to the site collection.

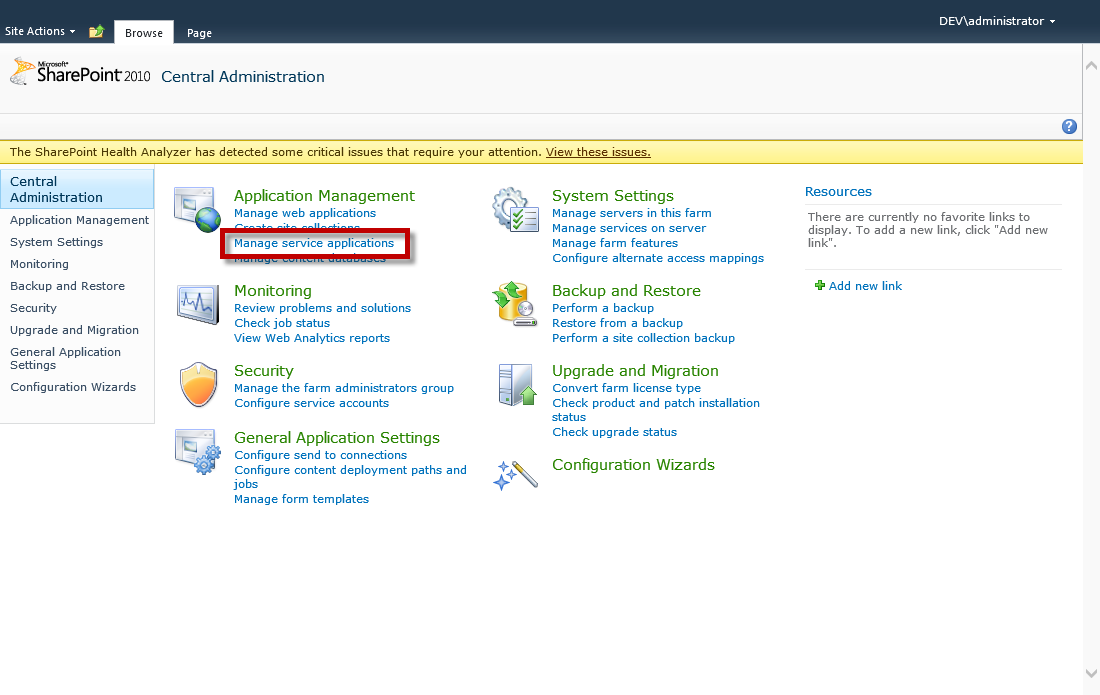
In the top-level site, perform the steps below.

1. Go to the Pages document library and delete the file, Glyma.aspx.
2. Go to the Style Library and delete the folder: “Glyma”.
3. Go to the Master Page Gallery and delete the folder: “Glyma”.

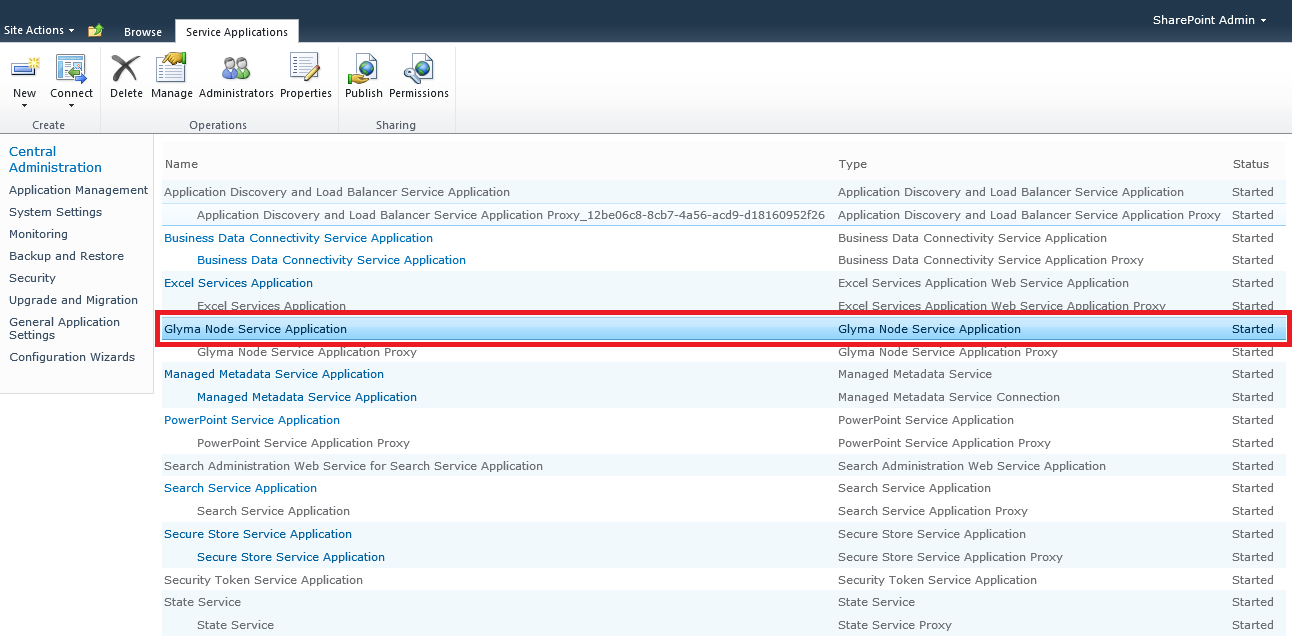
## Remove the Glyma Node Service application

Go to the Central Administration site and perform the following steps to remove the Glyma Node Service Application.

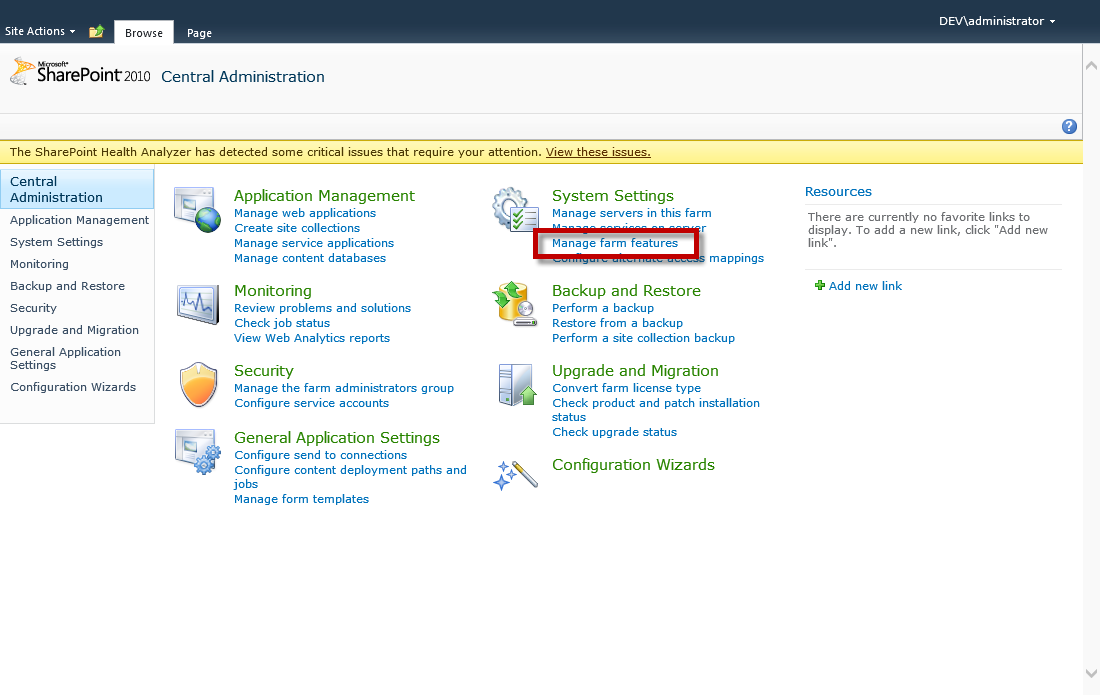
1. On the main Central Administration page, go to “Manage service application” under “Application Management”.



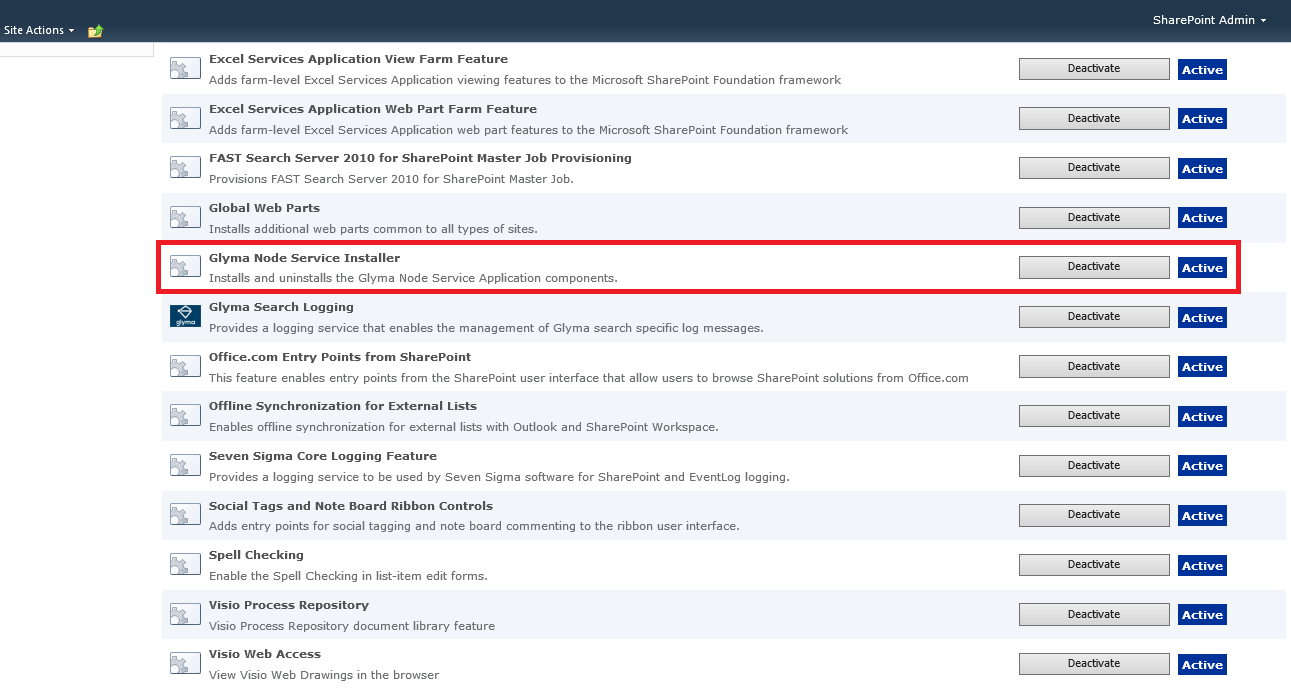
1. Select the Glyma Node Service Application and click the Delete button in the ribbon.



1. On the main Central Administration page, go to “Manage farm features” under “System Settings”.

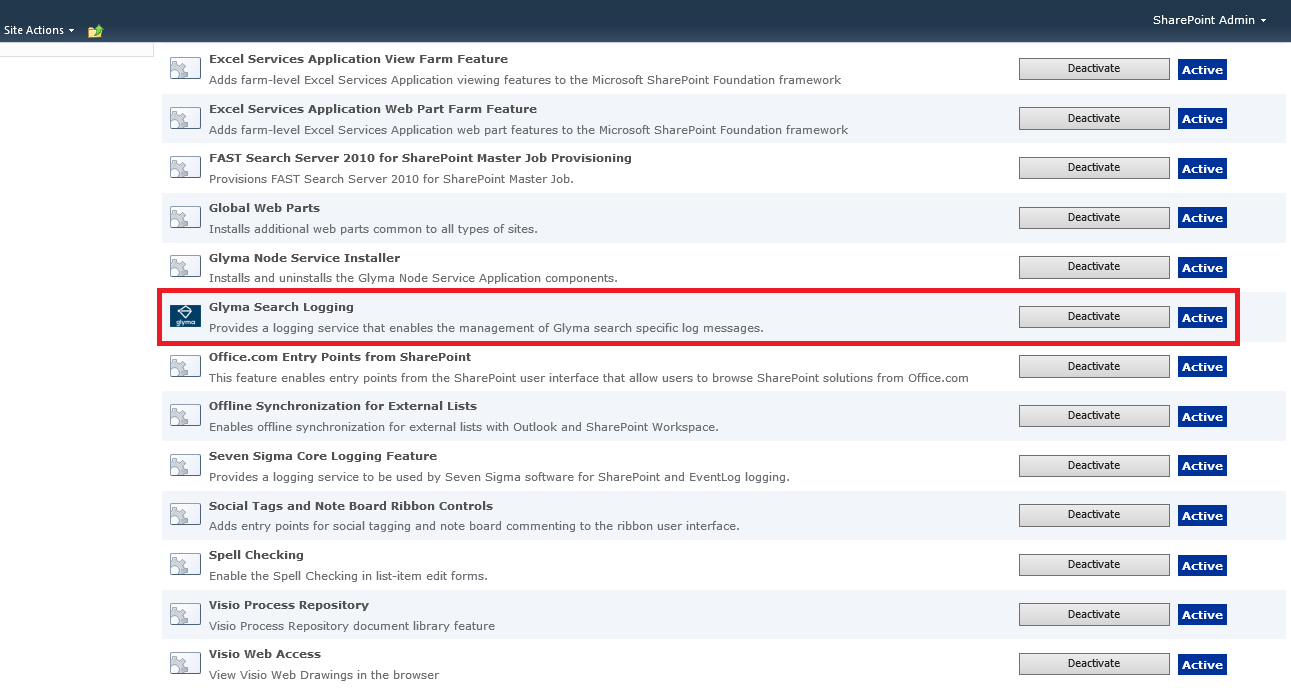


1. De-activate the “Glyma Node Service Installer” feature.



## Remove the Glyma search custom connector

1. Open SharePoint Central Administration.
2. Navigate to the Search Administration page.
3. Click on the “Content Sources” link in the Quick Launch.
4. On the “Manage Content Sources” page, remove the Glyma content source.
5. De-active the Glyma Search Logging feature.



On **every** server running the SharePoint search crawl component, perform the following steps.

1. In a SharePoint Management Shell running as an administrator, execute the PowerShell commands below.

$searchapp = Get-SPEnterpriseSearchServiceApplication

Get-SPEnterpriseSearchCrawlCustomConnector -SearchApplication $searchapp -protocol glyma | Remove-SPEnterpriseSearchCrawlCustomConnector -SearchApplication $searchapp

1. Open a registry editor and go to the key:

* **For SharePoint 2010**:

[HKEY\_LOCAL\_MACHINE]\ SOFTWARE\Microsoft\Office Server\14.0\Search\Setup\ProtocolHandlers.

* **For SharePoint 2013**:

[HKEY\_LOCAL\_MACHINE]\ SOFTWARE\Microsoft\Office Server\15.0\Search\Setup\ProtocolHandlers.

1. Remove the string value called: glyma.
2. Restart the Windows service for SharePoint search to make the Search Service application aware of the changes.

* **For SharePoint 2010**:

SharePoint Server Search 14.

* **For SharePoint 2013**:

SharePoint Server Search 15.

1. Remove the BCS model file, GlymaRepositoryModel.xml.

## Remove the Glyma SharePoint solutions

1. Open SharePoint Central Administration.
2. Click the System Settings link in the Quick Launch.
3. Click on the Manage farm solutions link.
4. For each Glyma SharePoint solution:
   1. Click on the link for the SharePoint solution.
   2. Retract the SharePoint solution.
   3. When the SharePoint solution has been successfully retracted and has a status of “Not Deployed”, click on the link for the SharePoint solution.
   4. Remove the SharePoint solution.

## Remove the Glyma databases

1. Open SQL Server Management Studio.
2. Delete the Glyma databases.

# Scripted Rollback Process

Glyma currently supports a partial scripted rollback using details from a XML configuration file. The remainder of the rollback must be completed manually. The partial scripted deployment performs the steps below.

* Removes the Glyma related search schema
* Removes the Glyma Node Service application
* Removes the Glyma SharePoint solutions.

The scripted deployment process for Glyma is described below. Execute the scripted deployment.

1. Revert the configuration of the site collection.
2. De-activate features in the site collection.
3. Remove the files deployed to the site collection.
4. Execute the scripted rollback.
5. Remove the Glyma search custom connector.
6. Remove the Glyma databases.

## Revert the configuration of the site collection

Please refer to the steps provided in “Revert the configuration of the site collection” in the section “Manual Rollback Process”.

## De-activate features in the site collection

Please refer to the steps provided in “De-activate features in the site collection” in the section “Manual Rollback Process”.

## Remove the files deployed to the site collection.

Please refer to the steps provided in “Remove the files deployed to the site collection.” in the section “Manual Rollback Process”.

## Executed the scripted rollback

1. Copy the deployment files to a SharePoint WFE or an application server that has SQL SMO installed.

The PowerShell related deployment files include.

* Glyma.Powershell.dll
* Glyma.Powershell.SharePoint.dll
* GlymaDeployment.psm1
* GlymaDeployment.psd1
* GlymaDeploymentConfiguration.xml

1. Open the GlymaDeploymentConfiguration.xml file and ensure the deployment settings are correct.

Note: All settings in this file must have a valid value for the deployment environment.

1. Open a SharePoint Management Shell as an administrator.
2. Import the Glyma PowerShell modules by executing the commands below.

Import-Module "<Path to assembly>\Glyma.Powershell.dll"

Import-Module "<Path to assembly>\Glyma.Powershell.SharePoint.dll"

Import-Module "<Path to file>\GlymaDeployment.psd1"

1. Execute the scripted rollback by executing the command below.

Uninstall-Glyma –configFilePath “<Path to GlymaDeploymentConfig.xml file>”

If you wish to log the scripted rollback, execute the command below.

Uninstall-Glyma -configFilePath "“<Path to GlymaDeploymentConfig.xml file>" -Verbose \*> "“<Path to log file>"

1. Veriy that all Glyma SharePoint solutions have been removed.

## Remove the Glyma search custom connector

On **every** server running the SharePoint search crawl component, perform the following steps.

1. Copy the deployment files below to each server running the crawl component.

* GlymaDeployment.psm1
* GlymaDeployment.psd1
* GlymaDeploymentConfiguration.xml

1. Open a SharePoint Management Shell as an administrator.
2. Import the Glyma PowerShell modules by executing the commands below.

Import-Module "<Path to assembly>\Glyma.Powershell.dll"

Import-Module "<Path to assembly>\Glyma.Powershell.SharePoint.dll"

Import-Module "<Path to file>\GlymaDeployment.psd1"

1. Execute the scripted deployment by executing the command below.

Uninstall-GlymaSearchCustomConnector –configFilePath “<Path to GlymaDeploymentConfig.xml file>”

## Remove the Glyma databases

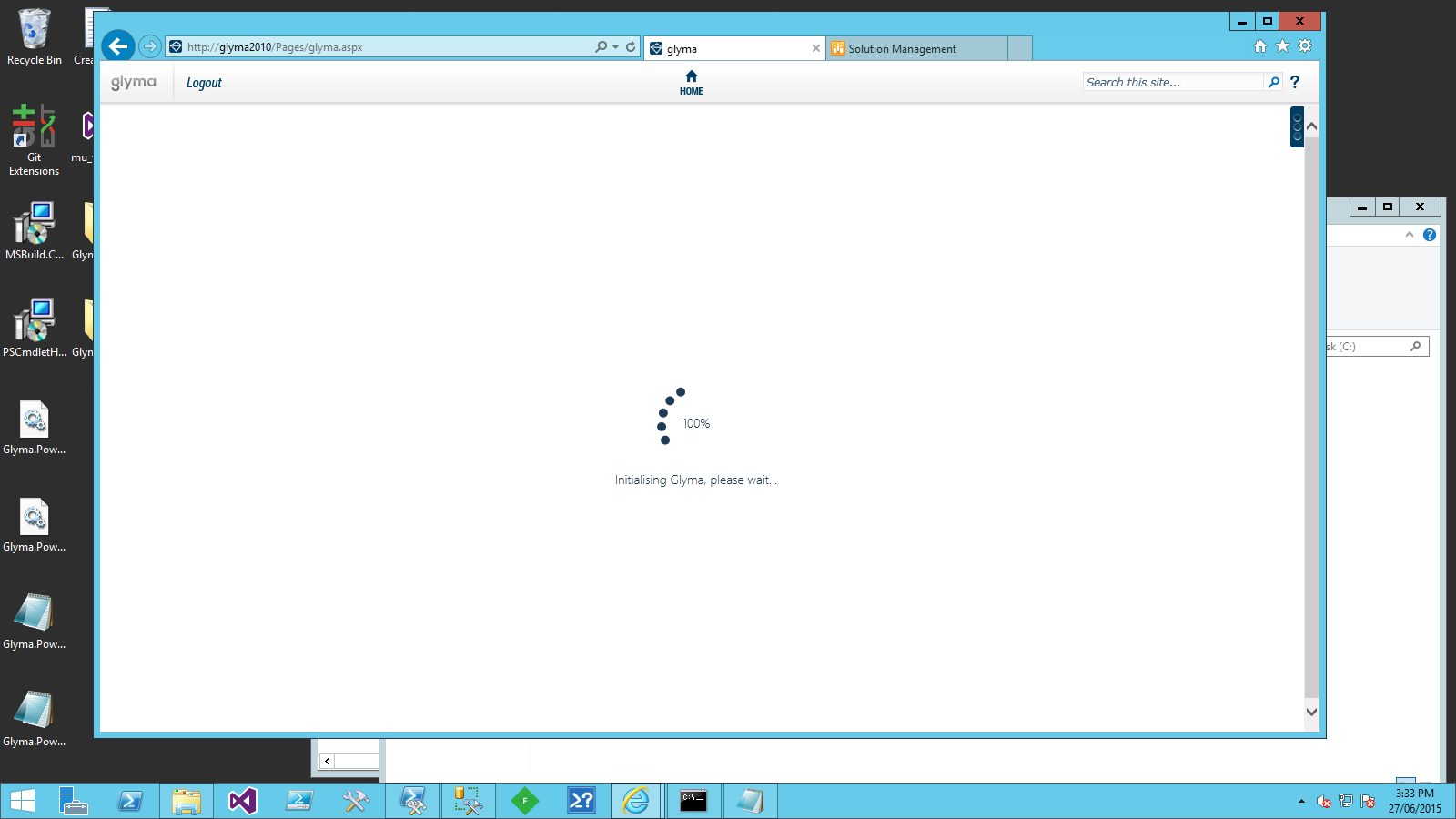
Please refer to the steps provided in “Remove the files deployed to the site collection.” in the section “Manual Rollback Process”.

# Troubleshooting

This section describes possible issues that you may encounter when deploying Glyma and how they can be resolved.

## Map Selection dialog box is not displayed in Glyma Mapping web part

In this scenario, you have successfully deployed all Glyma site collection features and created a page with the Glyma mapping tool web parts. However the map selection screen does not load and the initialisation icon remains on the page.



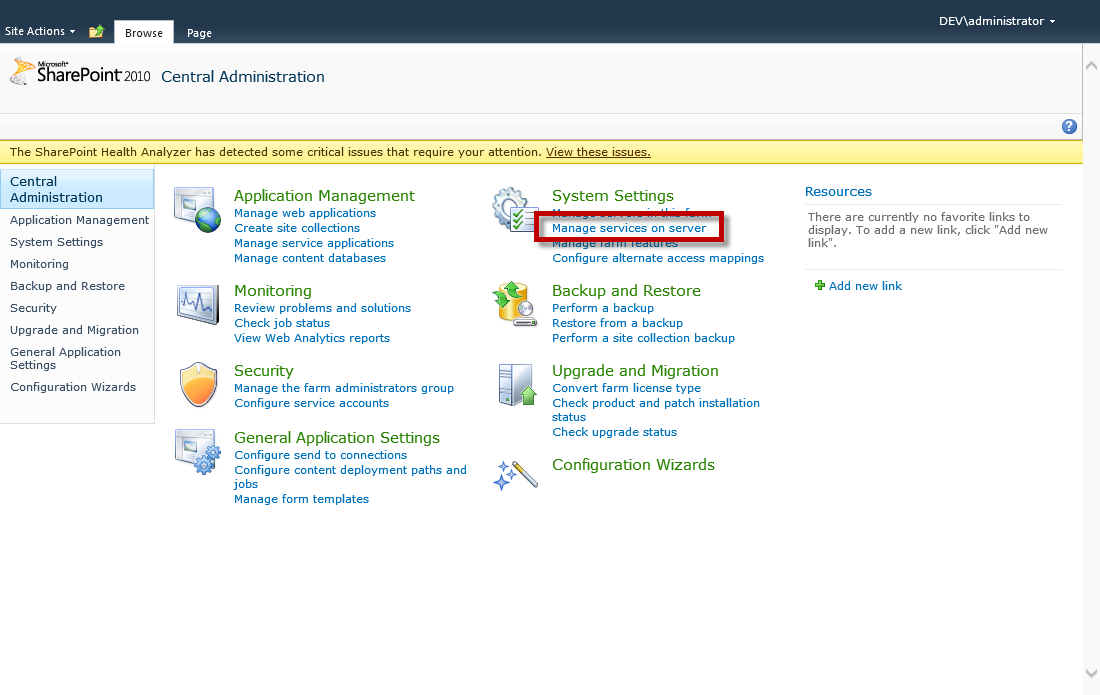
This issue can occur when either:

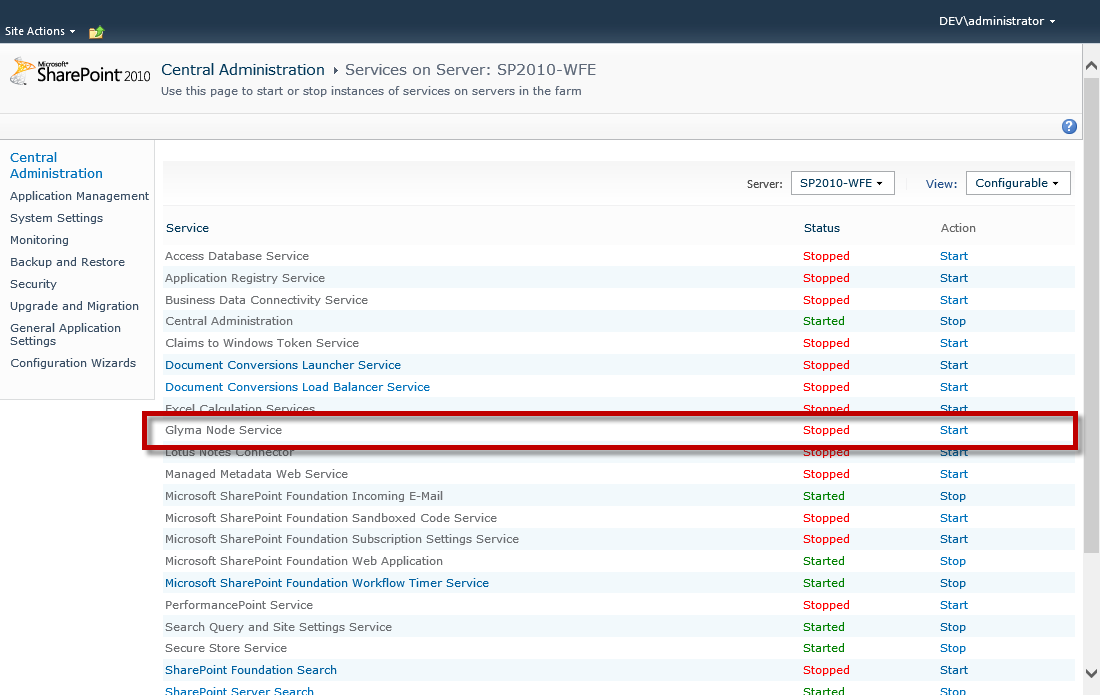
* The Glyma Mapping web part is unable to communicate with the Glyma Node Service application
* The connectivity of a Site Collection to Glyma databases is misconfigured

### The Glyma Mapping web part is unable to communicate with the Glyma Node Service application

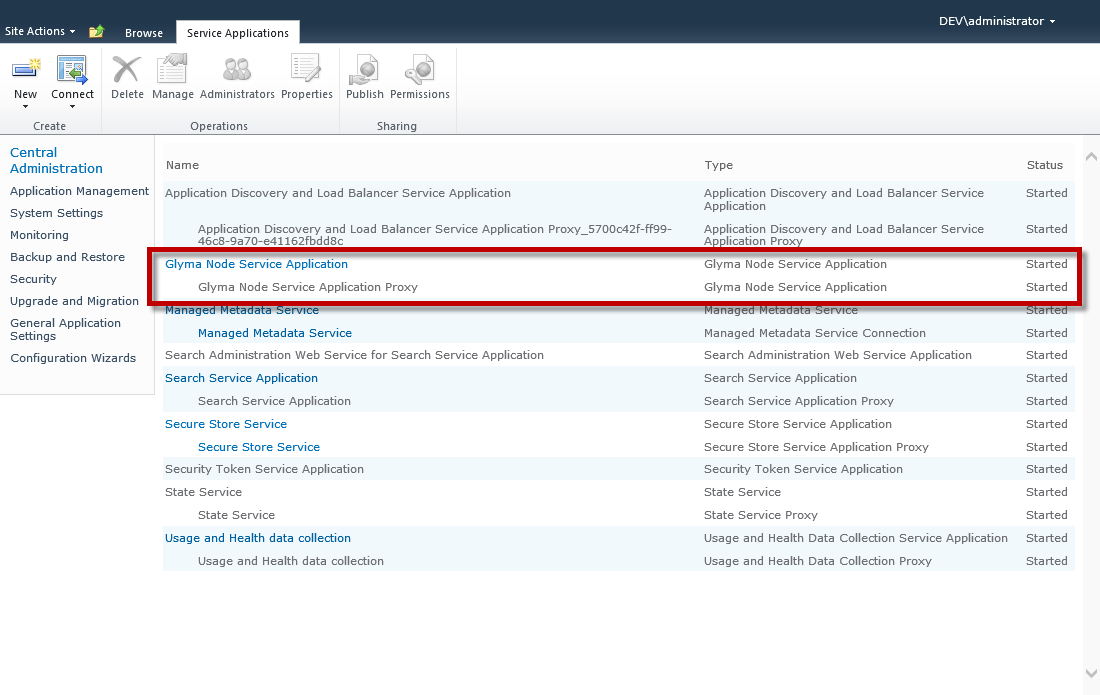
To resolve this issue, perform the steps below.

1. Confirm the Glyma Node Service is running.
   1. Open SharePoint Central Administration and go to “Manage services on server” under “System Settings”.



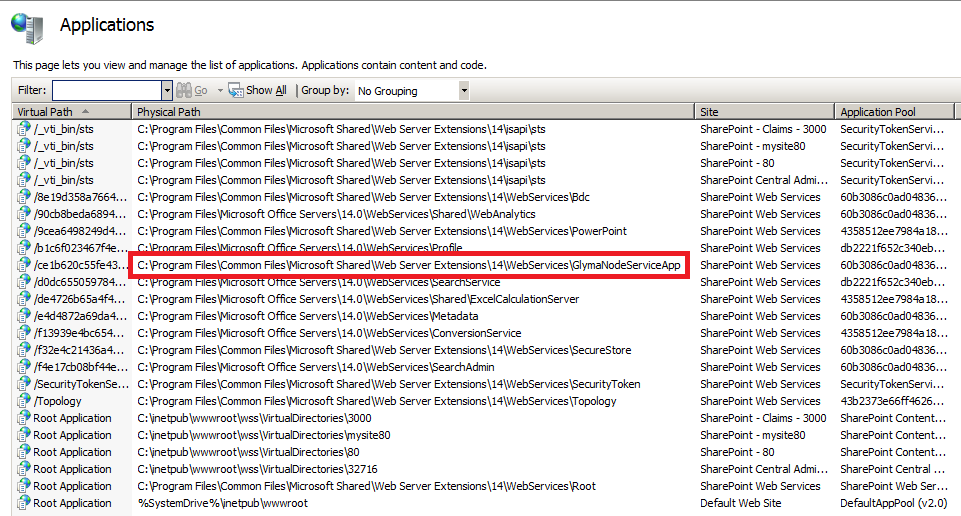
* 1. Ensure the “Glyma Node Service” is started.

1. Confirm the Glyma Node Service application has been provisioned.
   1. Open SharePoint Central Administration and go to “Manage service application” under “Application Management”.
   2. On the “Manage Service Applications page”, ensure the Glyma Node Service application is listed.



If the service application doesn’t exist, perform the steps in “Provision the Glyma Node Service application”.

* 1. On each server that has the Glyma Node Service application running, open IIS Manager and view all the applications. Ensure the application for the Glyma Node Service application exists.



If the application doesn’t exist, restart the Glyma Node and verify that the restart has created the application in IIS Manager.

### The connectivity of a Site Collection to Glyma databases is misconfigured

When Glyma is installed to a site collection, PowerShell is used to create the Glyma databases and then associate them to the site collection. Care must be taken because a small typo can cause connectivity problems.

To resolve this issue, perform the steps below.

1. Confirm that Glyma databases have been configured for the site collection.
   1. Open the SharePoint Management shell as an administrator.
   2. Create a connection to the site collection by executing the following commands:

$site = Get-SPSite <site collection URL>

$web = $site.OpenWeb()

* 1. List the properties of the site collection and look for properties that start with “glyma”. Take note of all of the databaseserver and databasename entries. Confirm the database server entry is correct.

$web.Properties”

Name Value

---- -----

glyma.securitydatabasename GL\_map\_security

glyma.transactiondatabasename GL\_map\_transaction

glyma.databaseserver SQL

glyma.databasename GL\_map

glyma.rolesdefined true

glyma.transactiondatabasese... SQL

glyma.defaultpage http://glyma2010/pages/glyma.aspx

glyma.securablecontextid 1

glyma.securitydatabaseserver SQL

Note: If the properties are not listed, the Set-SPGLSiteAssociation command has not been run to create the association. Skip to step e.

* 1. Open SQL Server Management Studio and connect to the Database server. Confirm the database names match the names from the output of step c. If there is a mismatch, move to step e.
  2. If there is a mismatch, rerun the Set-SPGLSiteAssociation command as specified in the section titled: Associate the SharePoint site collection with a Glyma database.

### The Glyma database permissions are misconfigured

When Glyma is installed to a site collection, PowerShell is used to create the Glyma databases. These databases are accessed by three different Glyma components:

* The application pool account for the Glyma node service application
* The application pool account for the web applications Glyma is deployed to
* The SharePoint search crawler account.

When the Glyma databases are provisioned, permissions are set for each of the above accounts. If the application pool accounts are changed, or were incorrectly applied, permissions will have to be assigned through SQL Server Management Studio.

Assign the correct application pool account DBO permission on the affected Glyma databases.

### The Glyma Security Context has not been set

Glyma integrates and augments with the Out-of-the-Box SharePoint framework so that pre-existing SharePoint and Active Directory groups can be leveraged in administering access to Glyma Projects and Glyma Maps. Just like SharePoint Site Collections act as a logical boundary for SharePoint Security Groups and Users, Glyma has a logical boundary referred to as a “Securable Context” which currently exists at the same boundary as a Site Collection. In the future the configurability of a Glyma Securable Context will expand so that it can exist across Site Collection boundaries if appropriately configured by an administrator.

This requires that each site collection have a security context created. To create this security context refer to section: “Configure a Sharepoint site collection for Glyma”.

### The Glyma node service application has not been provisioned

If the Glyma node service application has not been provisioned or is not started, the Silverlight client cannot connect to the Glyma databases. Confirm that the service has been provisioned and started as per section: “Provision the Glyma Node Service application” in this manual:

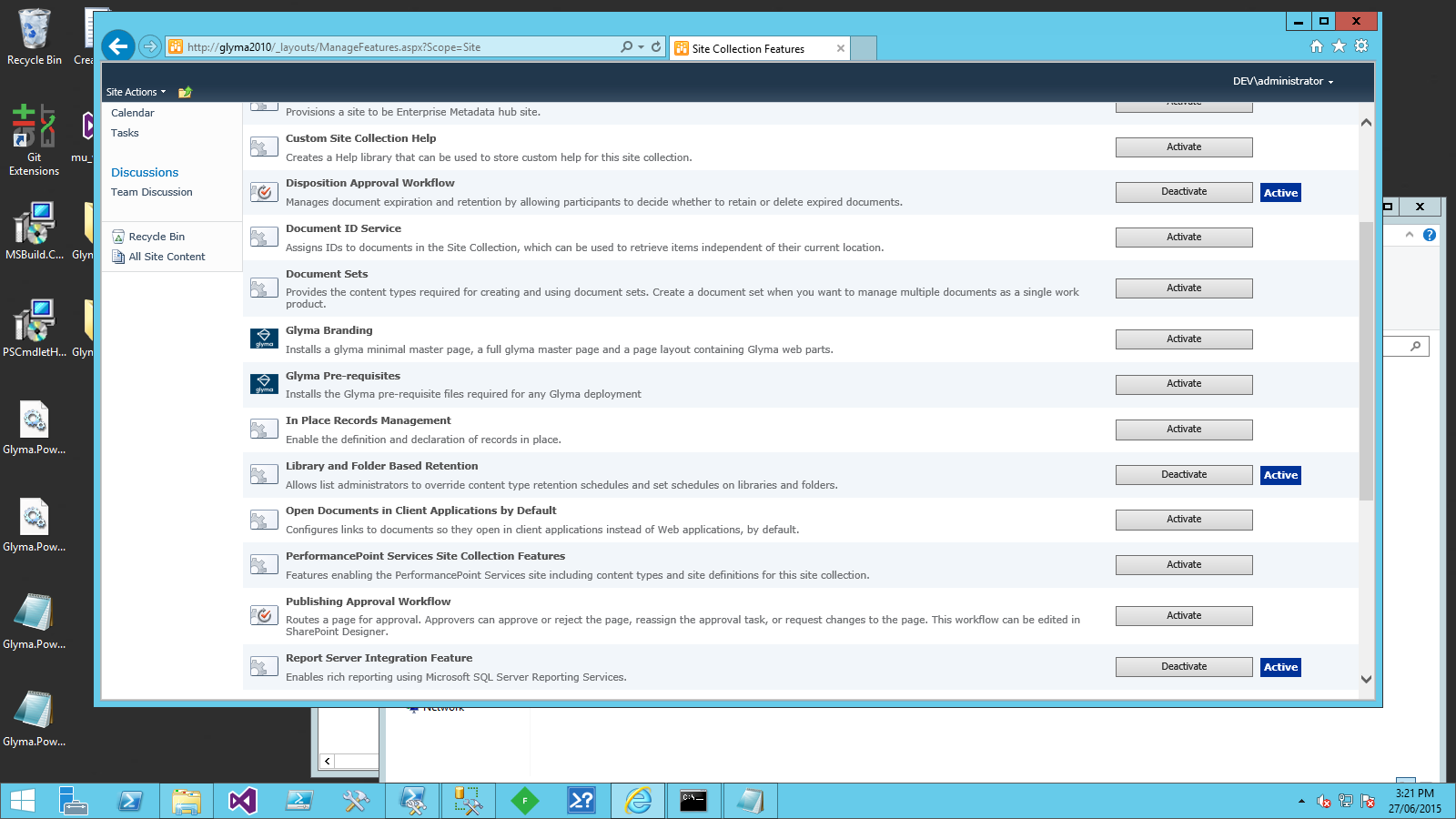
Note: If you have removed the Glyma node service solution file as part of an upgrade, you will need to reprovision it.

## Unable to see the Export Tab in the Glyma Management Console

If the export tab is missing from the Glyma management console, it is most likely that the Glyma Export Timer Job feature has not been active on the web application. To resolve, follow the steps outlined in the section “Activate the Glyma Export Timer Job feature”

## Missing Glyma features in the site collection

There are five Glyma site collection features that need to be activated to use Glyma, however you see two features available to be activated as shown below.



Some Glyma farm solutions are deployed to a particular web application. These are typically those that need to add safe control entries for the included web parts and controls to the web.config file. For example:

* Glymamappingtool.wsp
* GlymaRelatedContentPanelWebPart.wsp

To resolve this issue, perform the steps below.

1. Confirm Glyma farm solutions have been deployed to the web application as specified in section “Deploy Glyma SharePoint Solutions to SharePoint Farm”.

# Appendix A: Glyma Architecture

The purpose of this section is to provide an overview of the components that make up Glyma and how those components interact. The intention is to provide system administrators and developers with enough background information so that they are able to troubleshoot and provide helpful feedback to the Glyma support team in the event of a support incident.

## Glyma System Architectural Concepts and Overview

The following sections provide details on the interactions that the Glyma components have with each other and with SharePoint.

### Glyma Solution and Feature Architecture

“Figure 1 - SharePoint Solution and Feature Architecture” depicts the different SharePoint Solutions that are required to install a working Glyma system on top of SharePoint and where they are deployed into the SharePoint topology. The diagram also outlines the features each solution is responsible for deploying and their dependencies.

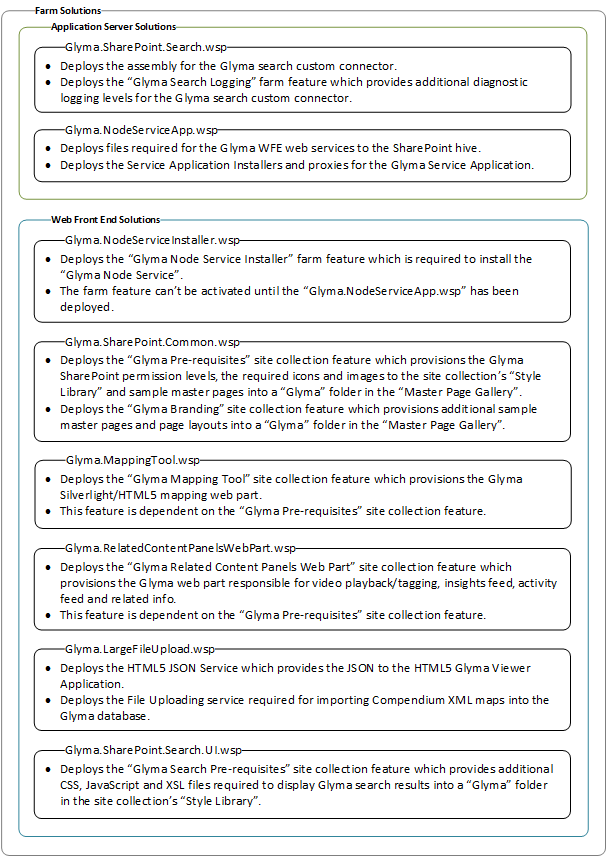


Figure - SharePoint Solution and Feature Architecture

### Glyma System Operations

“Figure 2 - Glyma Component Interactions” depicts how the Glyma components interact with each other. The directional arrows indicate the flow of data. Currently this is bidirectional for all cases except the HTML 5 viewer as the current version of Glyma is read-only. Additionally, where an arrow is located, it is possible to use tools such as PowerShell, Fiddler, etc. to monitor and troubleshoot issues that may be encountered by users.

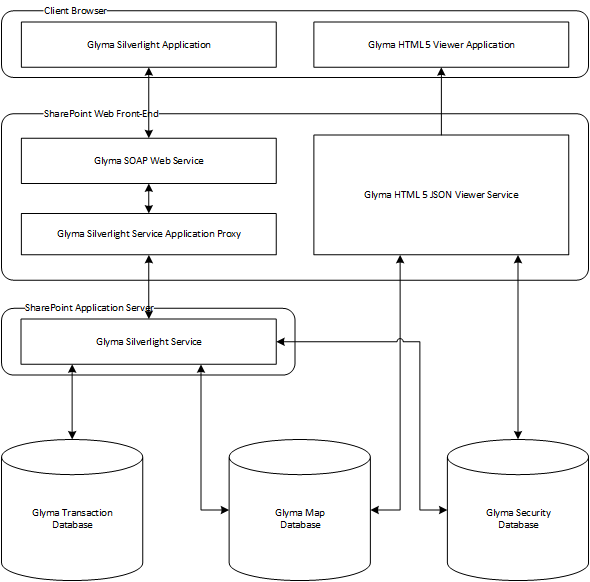


Figure - Glyma Component Interactions

### Glyma Security Framework

Glyma integrates and augments with the Out-of-the-Box SharePoint framework so that pre-existing SharePoint and Active Directory groups can be leveraged in administering access to Glyma Projects and Glyma Maps. Just like SharePoint Site Collections act as a logical boundary for SharePoint Security Groups and Users, Glyma has a logical boundary referred to as a “Securable Context” which currently exists at the same boundary as a Site Collection. In the future the configurability of a Glyma Securable Context will expand so that it can exist across Site Collection boundaries if appropriately configured by an administrator.

All SharePoint groups and users that are located within the boundary of the Securable Context (currently limited to the boundary of a Site Collection) can be used to administer security for Glyma Projects and Glyma Maps. By applying one of the permission levels listed in “Table 1” to a SharePoint group/user, that group/user will now be visible within Glyma’s permissions management screen.

|  |  |
| --- | --- |
| Permission Level Name | Level of accessibility rights within Glyma |
| Glyma Map Reader | Only has read access to the Glyma Projects and Glyma Map for which they have been allocated. |
| Glyma Map Author | Has all the same rights as a Glyma Map Reader on Glyma Projects and Glyma Maps they have been allocated.  Additionally they have create and update access to Glyma Maps they are allocated and Glyma Maps they create. |
| Glyma Map Manager | Has all the same rights as a Glyma Map Author on Glyma Projects and Glyma Maps they have been allocated.  Additionally they can delete Glyma Maps they are allocated. |
| Glyma Project Manager | Has all the same rights as a Glyma Map Manager on Glyma Projects and Glyma Maps they have been allocated.  Additionally they can create, update, and delete Glyma Projects that they are allocated. |
| SharePoint Site Collection Administrator | Has complete access and control over all Glyma Projects and Glyma Maps. |

“Figure 3 - Glyma Permissions Management Dialog” shows an illustration of the Glyma permissions screen. **N.B.** Only SharePoint Site Collection Administrators have access to the permissions management screen through the Glyma Silverlight Application web part.

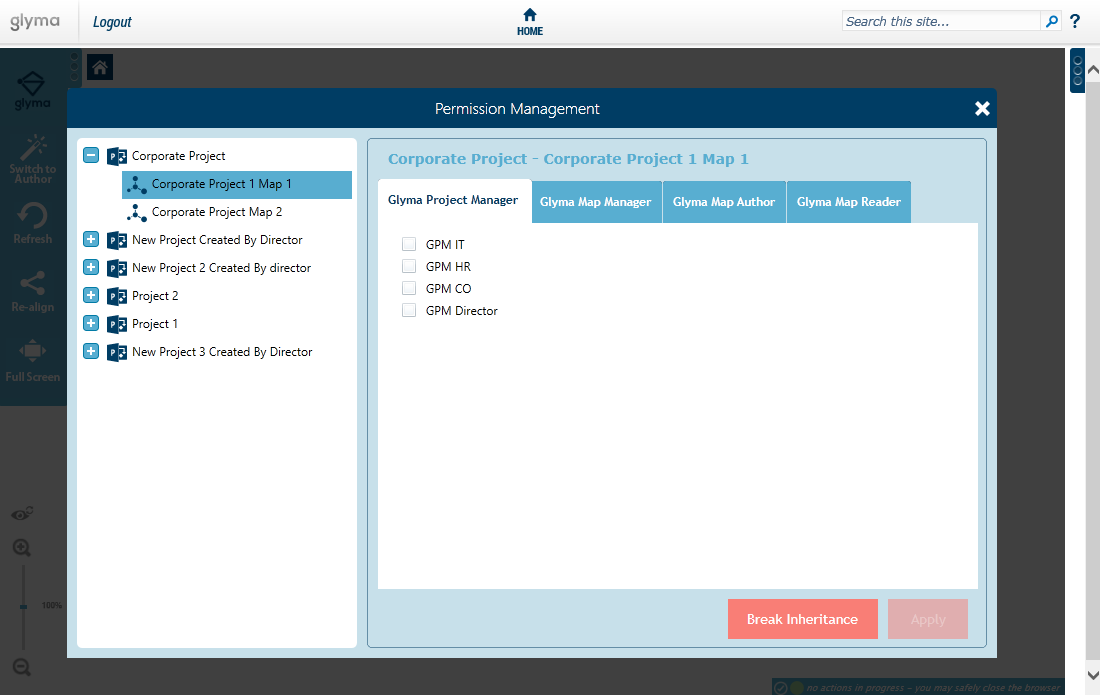


Figure - Glyma Permissions Management Dialog

## Client-side Glyma Components

The components in this section are for consumption by end-user browsers to access maps in Glyma.

### Glyma Silverlight Application

This application connects to the Glyma SOAP web service. By default the browser will attempt to load this application first. If the Silverlight 5 browser plugin is not installed on the browser, then the preview Glyma HTML 5 Viewer Application will be loaded.

#### Prerequisites

* jQuery 1.10.2 (deployed at ~sitecollection/Style Library/Glyma/Common/jquery-1.10.2.min.js)
* jQuery UI (~sitecollection/Style Library/Glyma/Common/jquery-ui.js)
* GlymaRedirector.js (~sitecollection/Style Library/Glyma/Common/GlymaRedirector.js)
* xml2json.js (~sitecollection/Style Library/Glyma/Common/xml2json.js)
* Silverlight.js (~sitecollection/Style Library/Glyma/Common/Silverlight.js)
* SilverlightErrorHandler.js (~sitecollection/Style Library/Glyma/Common/SilverlightErrorHandler.js)

#### Optional Prerequisites

* To use Yammer you will need to embed the YammerEmbedAPI available at https://assets.yammer.com/assets/platform\_embed.js

### Glyma HTML 5 Viewer Application

This application connects to the HTML 5 JSON service and delivers a read-only experience of Glyma maps to end users. The browser will attempt to load this if the Silverlight 5 browser plugin is not installed. For this to operate correctly, the user must run a browser that supports HTML 5 and the HTML Canvas element.

#### Prerequisites

* jQuery 1.10.2 (deployed at ~sitecollection/Style Library/Glyma/Common/jquery-1.10.2.min.js)
* jQuery UI (~sitecollection/Style Library/Glyma/Common/jquery-ui.js)
* GlymaRedirector.js (~sitecollection/Style Library/Glyma/Common/GlymaRedirector.js)
* xml2json.js (~sitecollection/Style Library/Glyma/Common/xml2json.js)
* Silverlight.js (~sitecollection/Style Library/Glyma/Common/Silverlight.js)
* SilverlightErrorHandler.js (~sitecollection/Style Library/Glyma/Common/SilverlightErrorHandler.js)

#### Optional Prerequisites

* To use Yammer you will need to embed the YammerEmbedAPI available at <https://assets.yammer.com/assets/platform_embed.js>

### Glyma Pre-Requisites

These are all the images and CSS styles required by the Glyma Silverlight and HTML 5 applications. These are all located within the Style Library of a site collection under a folder named: Glyma. (~sitecollection/Style Library/Glyma)

## SharePoint Web Front End Server Glyma Components

The components in this section are the server side endpoints that reside on the SharePoint web front end servers and act as intermediary services to the Glyma Node Service Application and Glyma Databases.

### Glyma HTML 5 JSON Viewer Service

This component serves the Glyma HTML 5 Application with the JSON required to render read only Glyma maps. This service reads directly from the Map Database and Security Database. Failure to access either of these databases will result in a loss of service.

### Glyma SOAP Web Service

This component serves the Glyma Silverlight Application with the SOAP end points required to render and build maps. This web service provides a web front end interface for browser clients to be able to interact with the Glyma Service Application, which performs all the actual processing of requests.

## SharePoint Application Server Glyma Components

These components are the server endpoints that handle and deliver content from the requests made by end-user browsers.

### Glyma Node Service

The Glyma Node Service handles all requests made by clients access Glyma through the Silverlight clients. This service interacts directly with the Map Database, Transaction Database, and Security Database. Failure to access any of these databases will result in a loss of service.

### Glyma Databases

Glyma requires 3 separate databases to operate. Each fulfils a distinct storage role and thus their importance in a disaster recovery scenario differ. The role of each database, and their importance, are detailed in the following sections.

#### Map Database

The Map Database contains all the content created by end users. Deletion or corruption of this database will result in losing end user content. As a result, in a disaster recovery scenario, if this database is not recoverable then it can be difficult to recover the lost content.

#### Transaction Database

The Transaction Database contains the transactions made by all end users in creating the content located in the Map Database. In a disaster recover scenario, if the Map Database is lost, then **most** of the content is recoverable using this database although some content will still be lost.

#### Security Database

The Security Database contains the security information for the Glyma Projects and Glyma Maps in the Glyma Map Database. Losing this database will not result in any loss of end user content but will require recreation of security contexts and user permissions for Glyma Projects and Glyma Maps.

### Glyma Search Custom Connector

Glyma integrates with SharePoint search using the SharePoint search connector framework. The Glyma search custom connector is a BCS indexing connector that provides the interface between SharePoint search and Glyma, and controls how Glyma content is crawled and the metadata that is provided. For further details on the SharePoint search connector framework, please refer to the MSDN article “Search connector framework in SharePoint 2013” (<http://msdn.microsoft.com/en-us/library/office/ee556429(v=office.15).aspx)>.

The Glyma search custom connector currently only supports full crawls.

#### BDC Model File

As a BCS indexing connector, the Glyma search custom connector requires a BCS model file that defines the details for crawling Glyma content. For Glyma, the BCS model file is called, GlymaRepositoryModel.xml.

The BCS model file is only read when the Glyma search custom connector is first loaded by the SharePoint search crawl component. Changes to the file do not take effect until the SharePoint search service is restarted on the server hosting the SharePoint search crawl component.

The BCS model file can be stored in a shared location or copied to every server where the Glyma search custom connector is installed. The choice of location for this file affects the fault tolerance of the Glyma search custom connector. If the file is stored in a shared location and it becomes inaccessible for whatever reason, all Glyma search custom connectors will not be able to restart. If the file is stored on every server where the Glyma search custom connector is installed, each connector is only affected by the availability of its own BCS model file; however, any changes required to the file will need to be replicated to all servers where the Glyma search custom connector is installed.

#### Security Trimming

The Glyma search custom connector currently supports security trimming in SharePoint environments that use Windows authentication. When Glyma content is crawled, access control lists (ACL’s) are created using the permission settings for the Glyma project and/or Glyma root map and the site collection’s administrators.

The creation of ACL’s during the crawl process provides the best query performance; however, a consequence of this is that SharePoint groups or users that have been recently granted permissions to Glyma content will not see search results until the Glyma content has been re-crawled.

#### Tuning the Crawler for Glyma

The Glyma search custom connector provides a number of configurable properties in the BCS model file that can be used to tune the crawl. These settings are described in the table below.

|  |  |
| --- | --- |
| Property | Description |
| SecurityConnectionString | Defines the connection string to the security database. |
| EnableNodeAclCache | Specifies whether ACL’s are cached for projects and root maps. |
| NodeAclType | Specifies the type of ACL to create for security trimming.  Currently, the only allowed value is: Windows, which specifies ACL’s are created for Windows authentication. |
| NodeAclCacheDuration | Specifies the duration (in seconds) that an ACL’s remains in the cache. |
| NodeAclCacheAutoExpirePeriod | Specifies the period (in seconds) between the automatic removal of expired ACL’s from the cache. |
| NodeAclTaskWaitDuration | Specifies a time-out value (in seconds) for the creation of an ACL. |
| ExcludeSimpleQuestions | Filters out Glyma question nodes that consist of only one or two words from the crawl. |
| ExcludeSpecifiedQuestions | Filters out user-specified Glyma question nodes from the crawl. Multiple questions can be separated using a semi-colon.  For example: Specified User Question 1?;Specified User Question 2? |
| IncludeParents | Specifies that the immediate parents of a Glyma node is retrieved during a crawl. |
| IncludeChildren | Specifies that the immediate children of a Glyma node is retrieved during a crawl. |