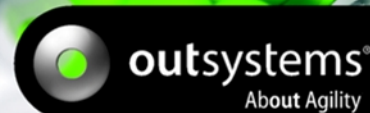


# OutSystems® Platform

## Integrating OutSystems and SharePoint Applications



The OutSystems® Platform can easily be integrated with external systems. SharePoint is one of them and it's the one we focus in this technical note.

We will describe how to integrate OutSystems and SharePoint applications both at the level of the user interface and at the level of business logic and data through web services. We will also address how to ensure security and authentication in these scenarios.

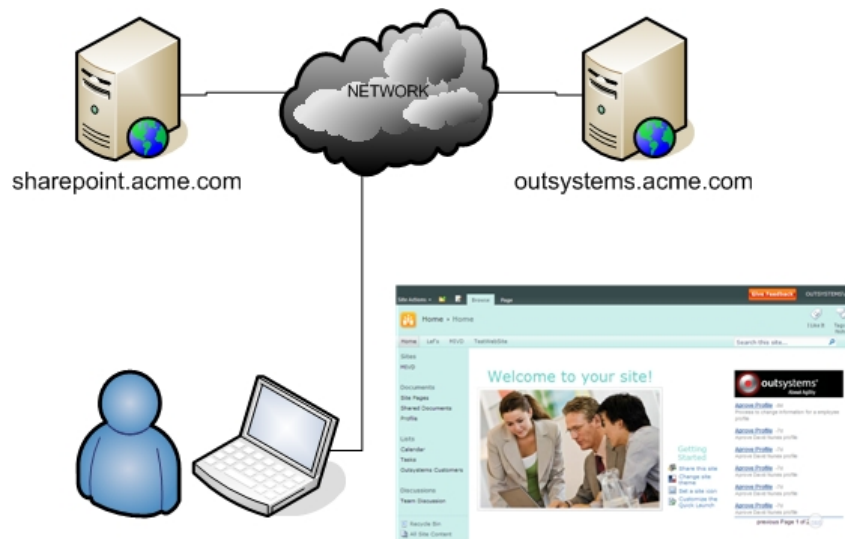
The steps described have been tested with SharePoint 2010 and the Agile Platform 5.1.

1 The Integration Scenario.....	2
2 Integrating the User Interface of OutSystems' apps in SharePoint.....	2
2.1 Requirements for UI Integration .....	2
2.2 Integrating the OutSystems Apps' User Interfaces.....	3
2.3 User Interface Authentication.....	4
2.3.1 Integrating User Authentication.....	4
2.3.2 Setting Browsers for Integrated Authentication .....	6
2.3.3 Web Services Authentication.....	6
2.4 Page Interactions between SharePoint and OutSystems.....	6
2.5 Embedded Change Technology and Embedded Process Automation.....	7
3 Integrating Business Logic and Data.....	7
3.1 Consuming OutSystems Business Logic and Data in SharePoint.....	7
3.2 Consuming SharePoint Web Services in OutSystems Applications.....	7
4 Appendixes .....	8
4.1 Configuring a Site as Local Intranet in Internet Explorer 8 .....	8
4.2 Configuring Trusted Sites in Firefox .....	9
4.3 Installing OutSystems Web Parts Package .....	10
4.4 Configuring Kerberos for SharePoint .....	14
4.4.1 Using the DelegConfig Application to Configure Kerberos .....	14

# 1 The Integration Scenario

This document revolves around a simple scenario where you have part of your intranet running under SharePoint (e.g., with your intranet's homepage and document management) and set of custom applications delivered using the OutSystems Platform (in this text a Recruitment application).

SharePoint is running in one server named *sharepoint.acme.com* and the OutSystems Platform is running in a separate server named *outsystems.acme.com*. The key characteristic here is that they share the parent domain *acme.com*. Other configurations in which the SharePoint and OutSystems share a common parent domain (e.g., *sharepoint.intranet.acme.com* and *outsystems.acme.com*) are fully supported. Adjust the instructions as needed.



Configurations where a parent domain isn't shared but the domains belongs to the same forest are supported but you will lose the page interaction described in 2.4 and will need to perform extra configurations, not covered in this document, to support [Kerberos authentication](#). Configurations where server domains are in different forests are not supported.

Running the OutSystems Platform and SharePoint from the same server is not supported.

## 2 Integrating the User Interface of OutSystems' apps in SharePoint

### 2.1 Requirements for UI Integration

Together with this document you should have downloaded `OutSystemsAndSharepoint.zip` which contains a SharePoint Solution Package with a helper SharePoint Web Part (`OSWebparts.wsp`), a helper SharePointAdapter eSpace (`SharePointAdapter.oms`) and a sample eSpace (`SPRecruitment.oms`) which will be used throughout this document.

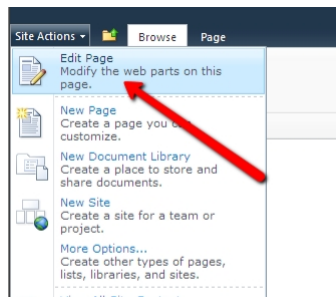
If you have not downloaded these yet you can download the zip file at <http://www.outsystems.com/NetworkSolutions/ProjectDetail.aspx?ProjectId=170>.

Before following the steps below you should install `OSWebparts.wsp` as described in [Installing OutSystems Web Parts Package](#), deploy `SharePointAdapter.oms` to your OutSystems Platform server and, optionally, deploy `SPRecruitment.oms`.

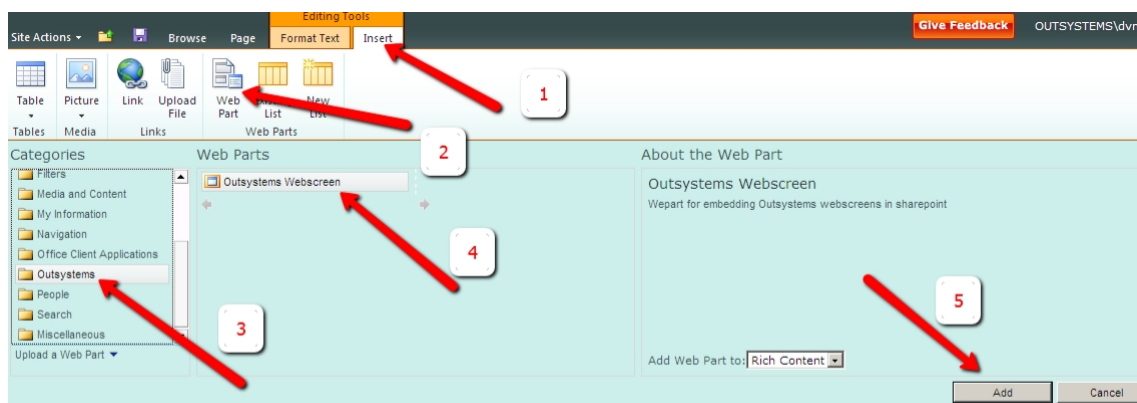
## 2.2 Integrating the OutSystems Apps' User Interfaces

To integrate your OutSystems' application user interface into a SharePoint page you should leverage the OSWebscreen web part. This web part allows you to easily embed a web page from your application as part of a SharePoint page.

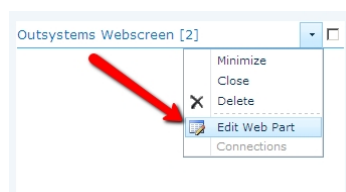
1. Edit the page in SharePoint;



2. Add the OutSystems Webscreen web part to the desired page section;



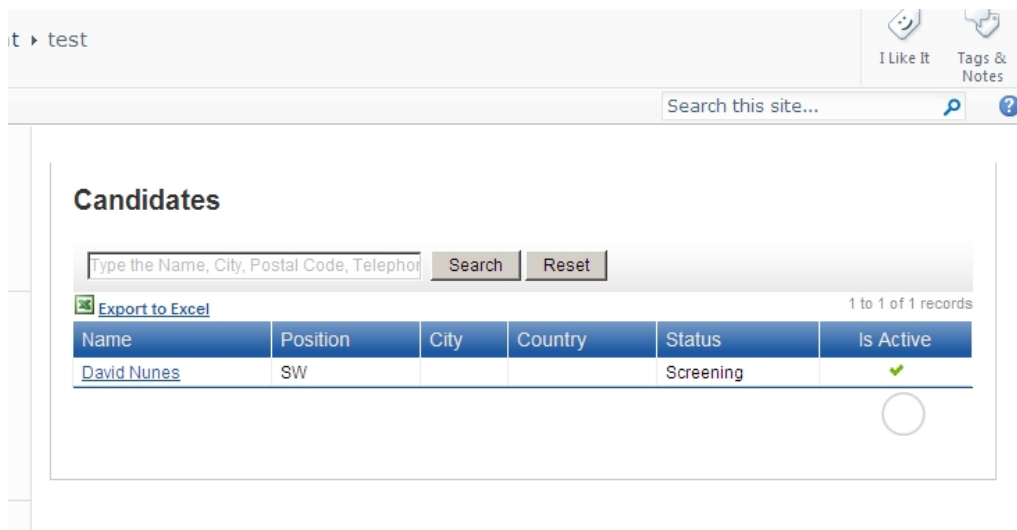
3. Edit the properties of the web part you just added;



In the OutSystems section of the web part properties, type the URL of your application's page. In the example below we are using the URL [http://outsystems.acme.com/SPRecruitment/candidate\\_list.aspx](http://outsystems.acme.com/SPRecruitment/candidate_list.aspx) which corresponds to the Candidate\_List webscreen of the eSpace SPRecruitment published on outsystems.acme.com. When finished press OK to update the web part with the new content.

You can safely leave IFrame Id and Document Domain blank. These will be properly explained later in this document.

4. Finish the page design and review the final result.



The `OsWebScreen` web part creates an `IFrame` for the OutSystems content. The `IFrame` `Id` property is available so that you may later use it if you need to write JavaScript to access and manipulate the contents of the `IFrame`. Note that, as the SharePoint and OutSystems pages come from different domains, strict restrictions on cross-domain scripting exist. Section 2.4 explains in detail how to overcome this barrier.

## 2.3 User Interface Authentication

This section focuses on how to enable a user to authenticate transparently across SharePoint and OutSystems. This allows the user to login only once and have a seamless experience across SharePoint and OutSystems pages.

As we are using an `IFrame` to embed the OutSystems' web page the browser will effectively fetch two pages, one from SharePoint and another from the OutSystems Platform, although for the user it all just seems one page. This means that the user could potentially be asked for authentication twice, one for the SharePoint page and another for the OutSystems page. The instructions below focus on how to make the OutSystems Platform determine the identity of the user transparently in case he/she has not yet signed in in the OutSystems Platform but has already done so in SharePoint.

Technology wise we will focus on NTLM and Kerberos authentication as they are the two most popular authentications methods for SharePoint.

### 2.3.1 Integrating User Authentication

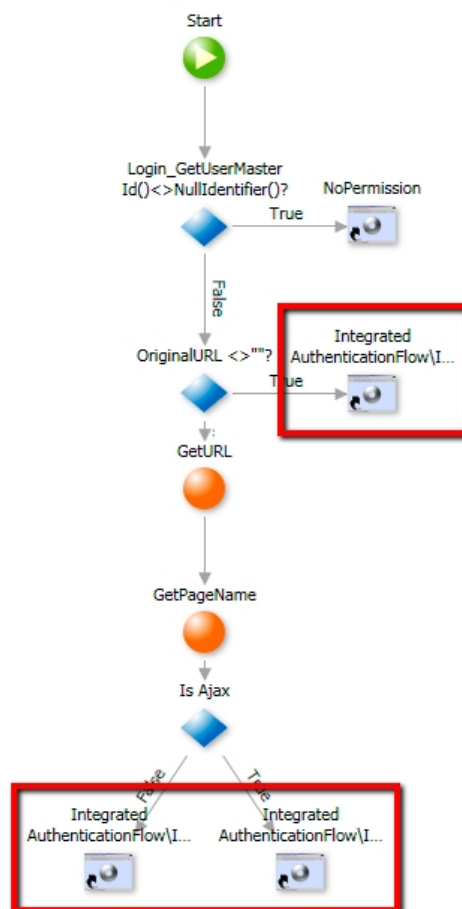
The first step to achieve a single sign on experience is to set SharePoint to use NTLM or Kerberos authentication. After this you need to perform a few small changes to the pages of the application you built with the OutSystems Platform and want to expose within SharePoint.

1. Set Integrated Authentication to Yes in the web screen or web flow you want to expose in SharePoint

Web Screen Properties	
Name	TaskList_Ajax
Description	...
Public	No
HTTP Security	...
Integrated Authentication	Yes
Is Frequent Destination	No
Title	...
Cache in Minutes	...
Advanced	
Style Sheet	...
JavaScript	...
Permissions	
Anonymous	<input type="checkbox"/>
Registered	<input checked="" type="checkbox"/>
Extended Properties	
Name 1	...
Value 1	...

2. Handle exceptions for unregistered users that reach your web screen. To make this easier we provide in the SharePointAdapter eSpace the `IntegratedAuthenticationScreen` which has a set of adjustments for a smoother integration with SharePoint. For exception handling itself we will use the OutSystems Platform's ability to have a single exception flow that manages all unhandled exceptions for a given eSpace. We will assume in the instructions you haven't changed the flow which is generated by default.

- a. Use Add/Remove References in your eSpace so that it includes a reference to the `IntegratedAuthenticationScreen` from the `SharePointAdapter` eSpace;
- b. In the Preparation action of the `ScreenFlows\Exceptions\UnregisteredHandler` web screen change the Destination elements that originally linked to the local `Login` web screen so that they now link to the `IntegratedAuthenticationScreen`;



- c. Check that the Exceptions Web Flow of the eSpace is set to the `Exceptions` web flow – this will be the Web Flow that will handle any unhandled exception raised in the eSpace.

### 2.3.2 Setting Browsers for Integrated Authentication

Internet browsers behave differently regarding integrated authentication, as follows:

**Internet Explorer 7+:** by default it will automatically use the operating system's credentials as long as it considers the site as an intranet site. See how to [configure a site as Local Intranet in Internet Explorer](#);

**Firefox 1.9+:** requires sites to be trusted to pass on operation system's credentials. See how to [configure trusted sites in Firefox](#);

**Chrome 6.0+:** by default it will automatically use the operating system's credentials as long as it considers the site as an intranet site. See how to [configure a site as Local Intranet](#);

### 2.3.3 Web Services Authentication

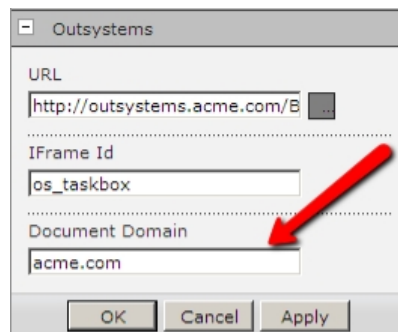
Web Services with integrated authentication (see further ahead in this document) are also supported but require OutSystems and SharePoint servers have to be configured for Kerberos authentication and delegation. More detailed instructions on how to configure Kerberos can be found [later in this document](#).

## 2.4 Page Interactions between SharePoint and OutSystems

For security reasons all major browsers enforce the [Same-Origin Policy](#) which specifies that a page from `site1.com` should not have access to or change the properties of a page from `site2.com`. This means that, for our integration scenario to be successful, an additional measure needs to be taken so that both SharePoint pages and OutSystems pages behave as if they belonged to the same domain.

The way to achieve this is explicitly setting in each page the [document domain](#) that the browser should consider. In this case we will set pages served both by `sharepoint.intranet.acme.com` and by `outsystems.acme.com` to identify themselves as belonging to the `acme.com` parent domain.

**SharePoint:** set the parent domain in the Document Domain property of the OSWebScreen web part.



**OutSystems:** Add the `EmbedScreenSharepoint` web block from the `SharepointAdapter` eSpace to the specific OutSystems web screens that are being embedded in SharePoint and set the parent domain in the `documentDomain` argument.

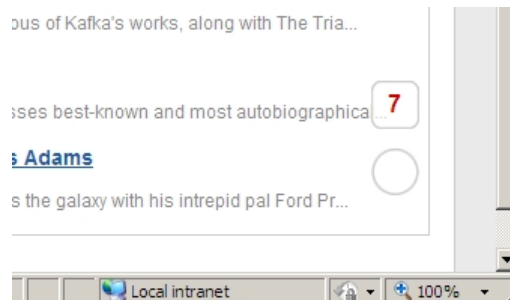


With this, both SharePoint's pages and OutSystems' web screens have their document domain elevated to a common parent domain and can now interact with each other. A positive side effect of this is that the `IFrame` defined in the `OSWebScreen` web part will now resize itself according to the size of its content.

A negative side effect is that, changing the page domains in the OutSystems environment will prevent Ajax calls from working when using Firefox. Everything works properly with Internet Explorer 7.0+ and Chrome 2.0+.

## 2.5 Embedded Change Technology and Embedded Process Automation

OutSystems' [Embedded Change Technology](#) (ECT) and [Embedded Process Automation](#) (EPA) both work by overlaying themselves to the displayed page.



Typically you do not want these to appear in the inner page when it is being embedded within another page. This is not an issue for EPA as it automatically disables itself when the page which would contain it is inside an IFrame.

As for ECT you can disable it in one of two ways:

1. If your eSpace is only used to be embedded within SharePoint, you should disable ECT for that eSpace altogether. You can easily do that in Enterprise Manager.
2. If only specific screens are embedded in SharePoint and you only want to remove ECT from these, you can add to the Preparation action of each screen a call to the `RemoveScreenFeedback` which you can find in the `ECT_Controller` extension.

## 3 Integrating Business Logic and Data

### 3.1 Consuming OutSystems Business Logic and Data in SharePoint

The best way to reuse business logic and data maintained by OutSystems applications within SharePoint is through web services. [Web services are easily built in the OutSystems Platform](#) and you can then consume them in SharePoint custom web parts you code or with Business Connectivity Services.

To ensure security and authentication Web Services with integrated authentication are also supported. Note that before you can consume a web service both OutSystems and SharePoint servers have to be configured for Kerberos authentication and delegation. Detailed instructions on how to configure Kerberos can be found [later in this document](#).

Once Kerberos authentication and delegation have been setup the web services created with the OutSystems Platform are ready to be consumed like any other authenticated web service.

### 3.2 Consuming SharePoint Web Services in OutSystems Applications

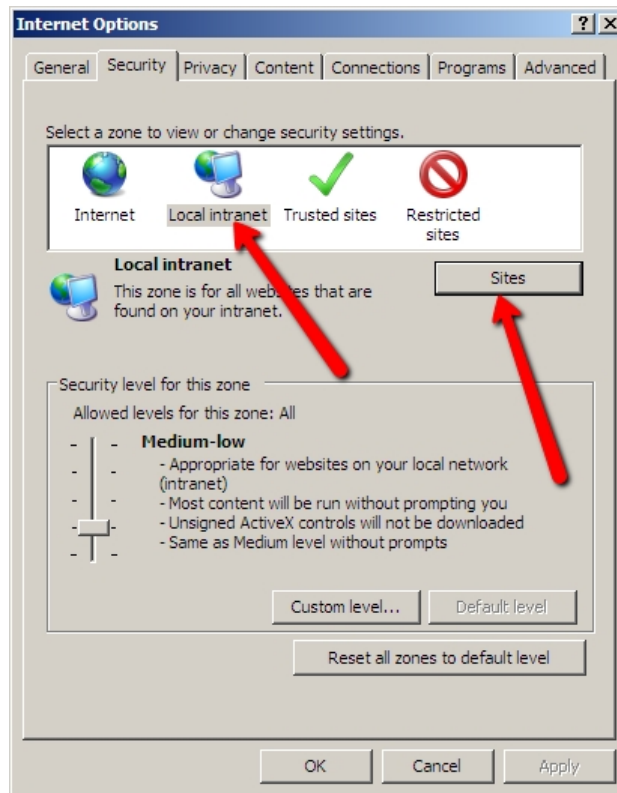
Web Services exposed from SharePoint can be consumed by OutSystems applications [as normal](#).

Microsoft provides a list of the web services SharePoint 2010 exposes, including detailed descriptions, which can be found at <http://msdn.microsoft.com/en-us/library/ee705814.aspx>.

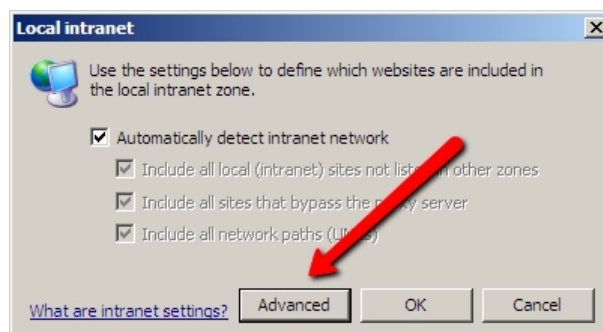
## 4 Appendixes

### 4.1 Configuring a Site as Local Intranet in Internet Explorer 8

1. Go to the Tools menu and choose Internet Options
2. Switch to the Security tab choose Local Intranet and click on the Sites button

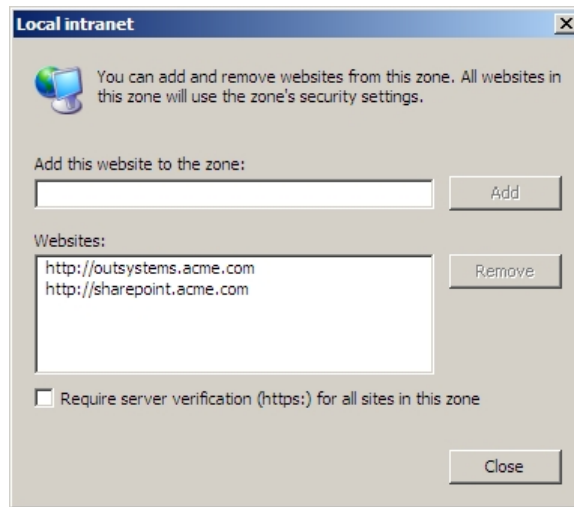


3. Click on the Advanced button





4. Add the address of the sites to be considered as local intranet; wildcards are accepted e.g.: \*.acme.com



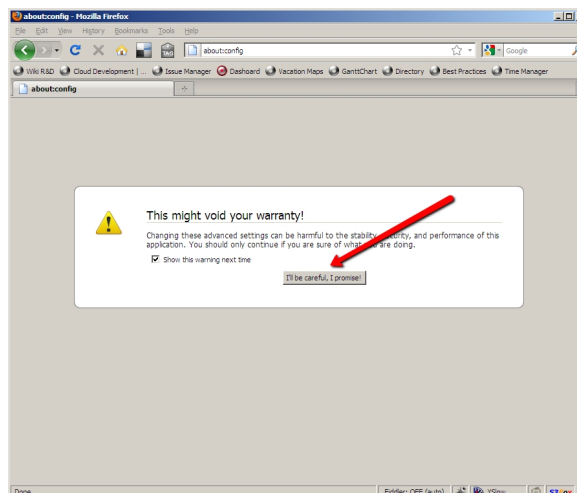
5. Now confirm and close all opened windows.
6. Open the site in Internet Explorer 8 and check that it is a local intranet on the status bar, at the bottom of the browser.



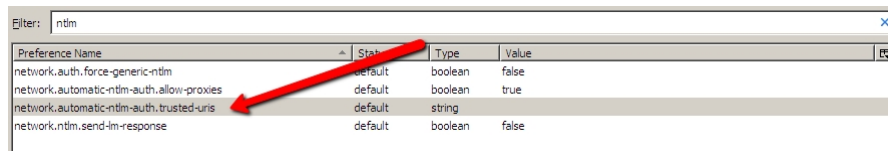
7. For an enterprise wide deployment Microsoft provides instructions on how to deploy customized versions of Internet Explorer 8 can be found at <http://technet.microsoft.com/en-us/library/cc985339.aspx>.

## 4.2 Configuring Trusted Sites in Firefox

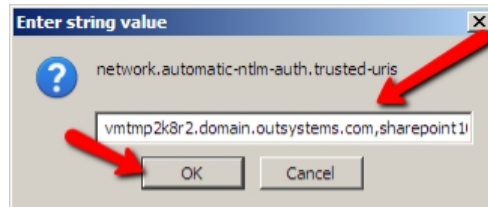
1. Launch Firefox and type `about:config` in the URL. For the most recent Firefox versions a confirmation is required.



2. Type `ntlm` on the filter and double click on `network.automatic-ntlm-auth.trusted-uris`.



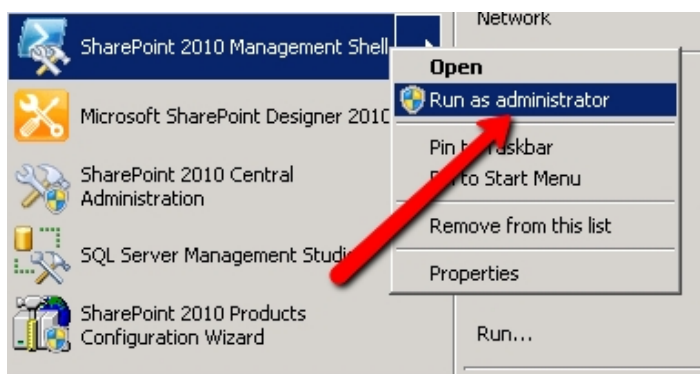
- Enter the host names of the servers that should be trusted for authentication – separated by commas.



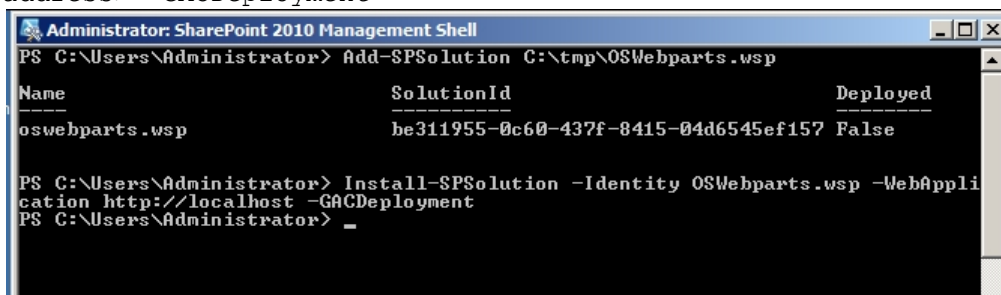
- For an enterprise wide deployment Mozilla provides instructions on how to deploy customized versions of Firefox can be found at [https://wiki.mozilla.org/Deployment:Deploying\\_Firefox](https://wiki.mozilla.org/Deployment:Deploying_Firefox).

### 4.3 Installing OutSystems Web Parts Package

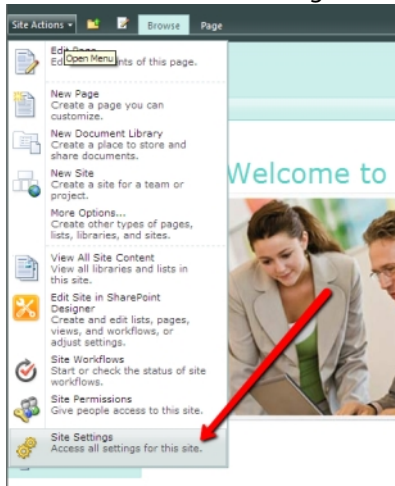
- Get the Web Parts package from <http://www.outsystems.com/NetworkSolutions/ProjectDetail.aspx?ProjectId=170>.



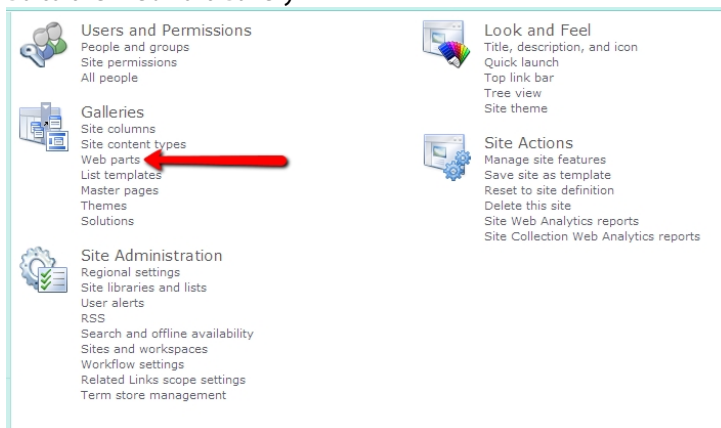
- Open SharePoint 2010 Management Shell as administrator
- Type `Add-SPSolution <path>\OSWebparts.wsp`
- Type `Install-SpSolution -Identity OSWebparts.wsp -WebApplication <app address> -GACDeployment`



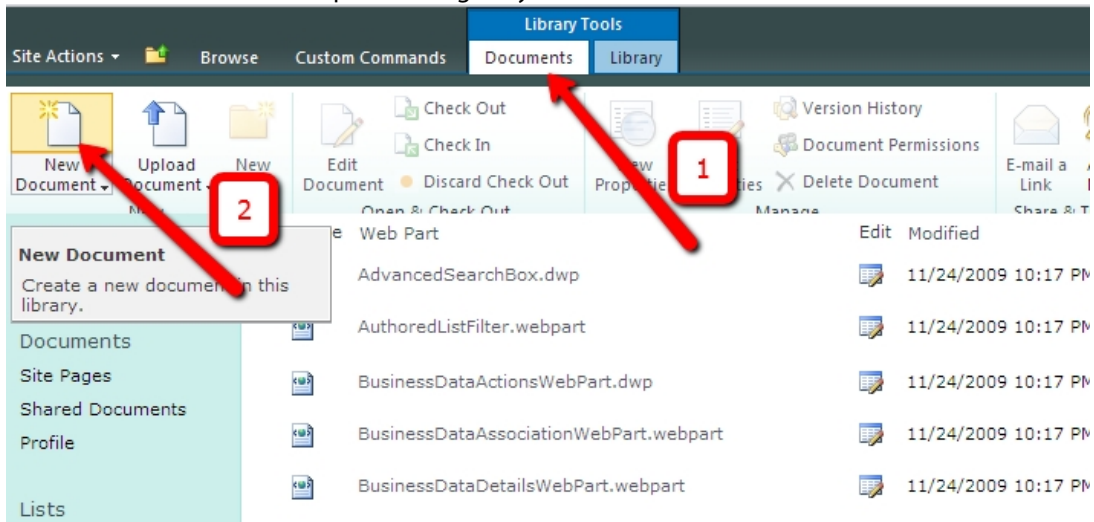
5. Go to SharePoint Site Settings



6. Go to the Web Part Gallery



7. Add the OsWebscreen web part to the gallery



**New Web Parts**

**Populate Gallery** 4

☐ Overwrite if file already exists?

☐ Web Part Type Name 3

☒ Cum.Outsystems.Webparts.OsWebscreen














☐ Microsoft.Office.Excel.WebUI.ExcelWebRenderer

File Name

.webpart

.webpart

## 8. Edit the web part

	MSPictureLibrarySlideshow.webpart		11/24/2009 10:17 PM	OUTSYSTEMS\pvo	Conte
	MSSimpleForm.dwp		11/24/2009 10:17 PM	OUTSYSTEMS\pvo	Conte
	MSUserDocs.dwp		11/24/2009 10:17 PM	OUTSYSTEMS\pvo	Docur
	MSUserTasks.dwp		11/24/2009 10:17 PM	OUTSYSTEMS\pvo	People
	MSXml.dwp		11/24/2009 10:17 PM	OUTSYSTEMS\pvo	Conte
	OlapFilter.dwp		11/24/2009 10:17 PM	OUTSYSTEMS\pvo	Filters
<input type="checkbox"/>	OsWebscreen.webpart <span style="color: green;">NEW</span>		9/28/2010 4:57 PM	OUTSYSTEMS\pvo	

1 - 30

## 9. Fill in the web part category

Web Part Gallery - OsWebscreen.webpart

**Edit**

Save Cancel Paste Copy Delete Export View Xml Manage Permissions

Commit Clipboard Actions

Name \*  .webpart

Title

Description

Group  Specify your own value:

Recommendation Settings

☐ Filters

☐ Dashboard

☐ My Site

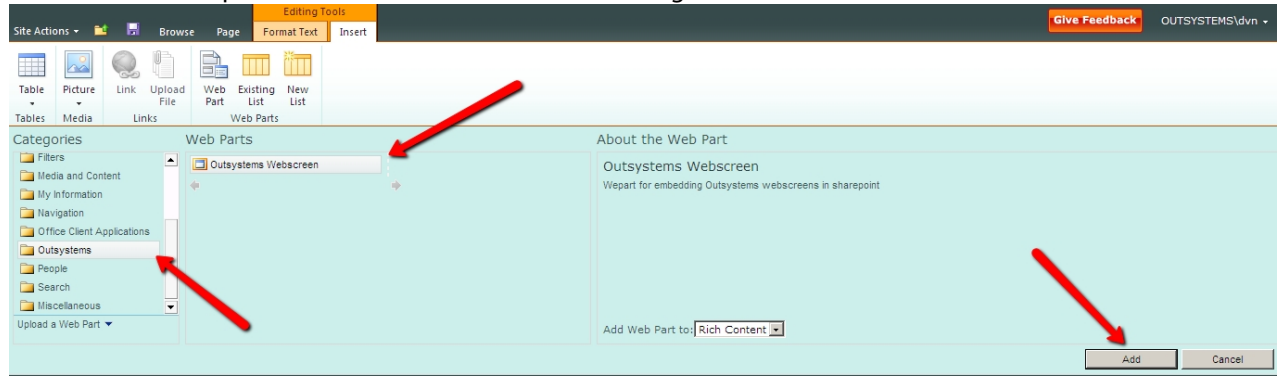
☐ Specify your own value:

Please specify site template names separated by ";#". Your web part will appear in "Recommended web parts" category when a user tries to add a web part to any web part pages within sites using site templates mentioned here. Otherwise, for page level recommendations of web parts, you can include a tag here and then add that same tag to "Recommended" property on the web part adder control on the page in question.

Created at 9/28/2010 4:57 PM by OUTSYSTEMS\pvo  
Last modified at 9/28/2010 4:57 PM by OUTSYSTEMS\pvo

**Save** **Cancel**

10. OsWebscreen web part should now be available on the design tools.



## 4.4 Configuring Kerberos for SharePoint

Microsoft has a detailed white paper on how to configure Kerberos authentication and delegation for SharePoint 2010 which you can review at <http://blogs.technet.com/b/tothesharepoint/archive/2010/07/22/whitepaper-configuring-kerberos-authentication-for-sharepoint-2010-and-sql-server-2008-r2-products.aspx>.

Alternatively, you can leverage a tool called DelegConfig written by [Brian Murphy-Booth](#) that guides you, step by step, on setting up Kerberos for SharePoint. This ASP.NET application examines a SharePoint server for Kerberos authentication and delegation issues and produces a detailed report with the missing configurations and instructions on how they can be addressed. You can download this application at <http://blogs.iis.net/brian-murphy-booth/archive/2009/04/22/delegconfig-v2-beta.aspx>. The installation instructions are packaged with the download.

### 4.4.1 Using the DelegConfig Application to Configure Kerberos

After installing the DelegConfig application, open it in an Internet browser, and start the Kerberos configuration Wizard.

[\[Report\]](#) [\[Wizard\]](#) [\[SetSPN\]](#) [\[SetDelegation\]](#) [\[Tests\]](#)

## Introduction

**DON'T RUSH!!!** You are not so smart that you should skip over reading the following. I like to skip over documentation just as much as the next person. But for your own benefit please read this information (usage tips and features). If you are not aware of everything this tool can do, you will add unnecessary confusion and work to your already frustrating experience of getting Kerberos and Delegation to function properly.

## Usage Tips

- **READ what the report tells you** - If I had a penny for every time somebody asked me what the report ALREADY SAYS I would be rich. Okay, maybe not rich, but I'd have a lot of pennies.
- **Start by using the [report](#) locally from the web server** - You should still use the same URL that you plan on using remotely. However, certain types of authentication problems will occur only if your connection is using Kerberos and there is something misconfigured. Using this tool from a browser instance local to the server will avoid those types of problems since in most cases local requests use NTLM.
- **Next, use the [report](#) from a remote client** - One important check that is performed is whether or not your browser has actually connected to the web service using Kerberos. If you always make your requests from the web server itself, you will likely always see a "Negotiate with NTLM" connection with a red "x" next to it (and red icons usually bother people). A second important piece of information revolves around name resolution of the *client*. If your requests are always from the server, how can we see what the client thinks?
- **Lastly, click any "Fix This" buttons locally from the server** - There will be "Fix This" buttons that appear that will allow you to make the exact changes that you need to get things working. But just like any other web application, this application is at the mercy of the whole double-hop concept. The most relevant types of changes this tool can make are Trust settings and ServicePrincipalName settings which are both stored in Active Directory. If you try to make changes to these settings (i.e. you click the fixThis buttons) from a remote browser instance it will likely fail because of the failed double-hop from browser-to-WebServer then webServer-to-ActiveDirectory.

## Pages

- /Set/SPNs.aspx - Allows adding and removing of ServicePrincipalNames
- /Set/Delegation.aspx - Allows changing Trust for Delegation settings.
- /Set/Providers.aspx - Allows correcting of inadequate NTAuthenticationProviders settings.
- /Report.aspx - Gives a picture of what is right and what is wrong.
- /Wizard.aspx - A set of wizard steps that supports adding more tiers to /Report.aspx.
- /Test.aspx - Allows double-hop tests for webServer-to-Sql or webServer-to-File server or webServer-to-webServer


The following steps illustrate the setting up of Kerberos for SharePoint using the DelegConfig application. Although this is a specific example for a specific scenario, it may be used as basis to set up your situation only by changing the responses in order to match your infrastructure scenario.

1. A short welcome message is displayed before the setup of Kerberos authentication and delegation parameters;

## Kerberos & Delegation Configuration Wizard

To continue, click Next.

Welcome to the Kerberos and Delegation Configuration wizard. This wizard will assist you in configuring what is needed to allow successful multi-hop Kerberos authentication for Nth tier applications.

 Back Next Cancel

2. Confirm that the SharePoint server is the right one;

## Current Environment

Is the Front-End service that you are configuring running in the **SharePoint - 80** application pool with a host name of **vmsharepoint10.domain.outsystems.com**?

If appropriate, clicking Yes will pre-configure the next few steps of the wizard.

 Yes

 Back Next Cancel


3. Define the access name to the server that is hosting SharePoint;

## Host Name


What host name is currently used to connect to your **HTTP** server?

A host name is the NetBIOS or Fully Qualified name that is used to connect to a network resource. The use of an IP address by clients as the host name is not recommended for use with Kerberos.

Examples: <http://www.company.com> websvr01  
<http://intranet:82> <https://PayRoll>

 \\FileServer\Public sqlNodeA.corpnet.local\Com  
olapsrv02 192.168.0.156

Host Name:

 Back Next Cancel




4. Set whether the SharePoint server is load balanced or not;

## Load Balanced

Choose whether **vmsharepoint10.domain.outsystems.com** is load balanced or not.

When configuring **ServicePrincipalName** and/or **Trust for delegation** settings, it is important to understand whether a service is load balanced or not when deciding which account to configure these settings against.

- ☒ Not Applicable  
☐ Load Balanced  
☐ Clustered

 Back Next Cancel


5. For the Kernel Mode choose 'Use AppPool Credentials' option because kernel mode authentication is not supported by SharePoint 2010 products;

## Kernel Mode

Is the **useKernelMode** feature enabled on your **vmsharepoint10.domain.outsystems.com** server?

By default, IIS 7.0 on Windows Server 2008 or Vista with SP1 or higher handles Kerberos in kernel mode. This makes setting ServicePrincipalNames on the application pool service account unnecessary. Instead they should be set on the computer account of the IIS server.

- ☐ Use Kernel Mode  
☒ Use AppPool Credentials

 Back Next Cancel


6. The Port Number and Instance Name settings do not apply to HTTP services for the SharePoint server, so skip forward;

## Port Number or Instance Name

Enter the port number or instance name being used to connect to the **HTTP** service running on **vmsharepoint10.domain.outsystems.com**.

Typically a client Kerberos application chooses whether to include a port number or instance name when constructing a ServicePrincipalName (SPN). For most client types, however, this information may not be used.

Not Applicable

 Back Next Cancel



7. Set the account that is configured on the SharePoint application pool;

## Service Account Name

Enter the account name that is running the HTTP service running on **vmsharepoint10.domain.outsystems.com**.

All the various Kerberos settings for a particular service need to be applied to the user/account that handles authentication for that service. For something like IIS this is the account running the W3WP.exe process. For something like SQL this is the account running the SQLSERVER.EXE process.

☐ Preconfigured **NETWORK SERVICE**

☒ Configured **OUTSYSTEMS\MOSSApp**

☐ Kernel Mode Authentication

8. Configure SharePoint to delegate credentials to another server;

## Trust for Delegation

Does the HTTP service running on **vmsharepoint10.domain.outsystems.com** need to delegate ("pass") credentials to another server?

Many people refer to "delegation" as the right to pass a user's credentials on to another service. Delegation is actually the right to "act on behalf of" that other entity even when that entity's password is not known.

☒ Yes

☐ No

9. Choose the type of delegation trust: the first option is easier to configure but less secure. Choose the option that better suits your needs;

## Delegation Type

Choose the type of trust you would like to grant to **OUTSYSTEMS\MOSSApp**

The most secure option is 'Trust this account for delegation to specified services only (Use Kerberos only)'. But there are different ways to delegate credentials based on your business requirements and application limitations.

☒ Trust this account for delegation to any service (Kerberos only)

☐ Trust this account for delegation to specified services only

☐ Use Kerberos only

☐ Use any authentication protocol

10. Set the delegation to use the HTTP service (OutSystems server);

## Service Type of Back-End (2nd tier)

Choose the service type `vmsharepoint10.domain.outsystems.com` is connecting to.

A "service type" describes what type of Windows service a client will be authenticating against.

HTTP (Hyper Text Transfer Protocol)

Back Next Cancel

11. Set OutSystems server(s) to have no load balancing;

## Load Balanced

Choose whether `vmtmp2k8r2.domain.outsystems.com` is load balanced or not.

When configuring **ServicePrincipalName** and/or **Trust for delegation** settings, it is important to understand whether a service is load balanced or not when deciding which account to configure these settings against.

☒ Not Applicable  
☐ Load Balanced  
☐ Clustered

Back Next Cancel

12. There are known issues on Kernel mode authentication with Windows 2008 R2, therefore choosing 'Use AppPool Credentials' is recommended;

## Kernel Mode

Is the **useKernelMode** feature enabled on your `vmtmp2k8r2.domain.outsystems.com` server?

By default, IIS 7.0 on Windows Server 2008 or Vista with SP1 or higher handles Kerberos in kernel mode. This makes setting **ServicePrincipalNames** on the application pool service account unnecessary. Instead they should be set on the computer account of the IIS server.

☐ Use Kernel Mode  
☒ Use AppPool Credentials

Back Next Cancel


13. The Port Number and Instance Name settings do not apply to HTTP services for the OutSystems server, so skip forward;

## Port Number or Instance Name

Enter the port number or instance name being used to connect to the **HTTP** service running on **vmtmp2k8r2.domain.outsystems.com**.

Typically a client Kerberos application chooses whether to include a port number or instance name when constructing a ServicePrincipalName (SPN). For most client types, however, this information may not be used.

Not Applicable

 Back Next Cancel



14. Indicate the user account configured on the OutSystems application pool;

## Service Account Name

Enter the account name that is running the **HTTP** service running on **vmtmp2k8r2.domain.outsystems.com**.

All the various Kerberos settings for a particular service need to be applied to the user/account that handles authentication for that service. For something like IIS this is the account running the W3WP.exe process. For something like SQL this is the account running the SQLSERVER.EXE process.

☐ Preconfigured NETWORK SERVICE  
☒ Configured OUTSYSTEMS\OSApp  
☐ Kernel Mode Authentication

  
 Back Next Cancel



15. OutSystems servers usually don't need to delegate credentials to other servers, so choose No and finish up the wizard.

## Trust for Delegation





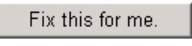




Does the **HTTP** service running on **vmtmp2k8r2.domain.outsystems.com** need to delegate ("pass") credentials to another server?

Many people refer to "delegation" as the right to pass a user's credentials on to another service. Delegation is actually the right to "act on behalf of" that other entity even when that entity's password is not known.








☐ Yes  
☒ No

  
 Back Finished Cancel

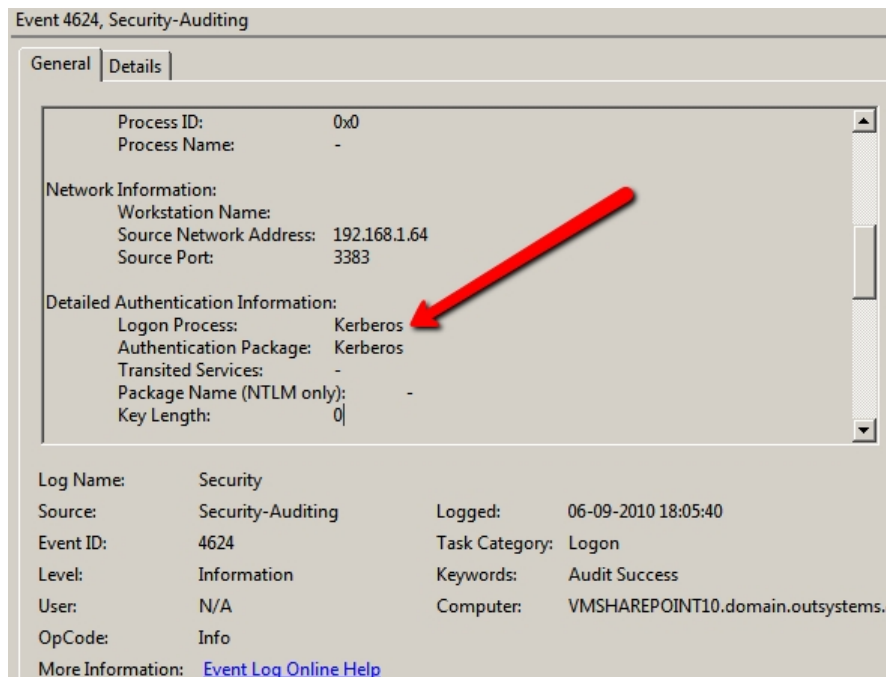
After finishing the wizard a report like the one below will be presented and each item that is not valid has a detailed explanation on how to correct it.

'vmsharepoint10.domain.outsystems.com'		
	Is Domain Account?	Service account <b>OUTSYSTEMS\dvn</b> is a valid domain account. ▶  Concepts
	Has Valid SPN?	<p>No usable ServicePrincipalName of <b>HTTP/VMSHAREPOINT10.domain.outsystems.com</b> could be found in Active Directory for the <b>OUTSYSTEMS\dvn</b> account.</p> <p>▼  What needs to change?</p> <ul style="list-style-type: none"> <li>Use SetSPN to add these missing entries:</li> </ul> <pre>setspn.exe -A HTTP/VMSHAREPOINT10.domain.outsystems.com OUTSYSTEMS\dvn</pre> <p>Or </p> <p>▼  More Information</p> <ul style="list-style-type: none"> <li>Existing SPN's for <b>OUTSYSTEMS\dvn</b>:</li> </ul> <p>There are no ServicePrincipalNames set on this account.</p> <p>▼  Concepts</p> <ul style="list-style-type: none"> <li>Domain computers are granted two ServicePrincipalNames of type "HOST" by default when they are joined to the domain. Domain users are not granted any ServicePrincipalNames because their unique identifying name is generally a UniversalPrincipalName. The "HOST" type provides Kerberos support for core services of Windows therefore encompasses all of the various service types that come included with Windows. You should <b>NEVER</b> manually add or remove an SPN with a "HOST" service type to any account. Doing so will have adverse effects to Kerberos when connecting to that computer.</li> <li>Due to the intended purpose of an SPN (unique name used to identify a specific account) they cannot be assigned to multiple accounts at one time. An SPN (Service Principal Name) is much like a UPN (Universal Principal Name). UPN's are unique names for identifying a domain user account whereas SPN's are unique names that usually identify a domain computer account. An example of a UPN would be "myAlias@microsoft.com" instead of the standard "MICROSOFT\myAlias". Having a given SPN assigned (duplicated) to multiple accounts would cause identification problems in the same exact way assigning the same username to multiple people would cause identification problems.</li> </ul>
	Has Duplicate SPN?	There are no duplicate SPN's. ▶  More Information

Multiple iterations might be required until you reach the correct Kerberos configuration.

Overall Status		
	Is Domain Account?	End user <b>OUTSYSTEMS\dvn</b> is a valid domain account. ▶  Concepts
	Authentication Method?	You have connected from your browser to IIS using <b>Kerberos</b> authentication. ▶  Concepts
	Impersonation Level?	TokenImpersonationLevel: <b>Delegation</b> ▶  More Information
	Will Delegation Succeed?	The current configuration is correct for Delegating credentials with Kerberos.

After all configurations have been correctly set, open the Event Viewer in the Security section for the SharePoint server and for the OutSystems server, and check that both are using Kerberos.



For any further troubleshooting please refer to the Microsoft's <http://blogs.technet.com/b/tothesharepoint/archive/2010/07/22/whitepaper-configuring-kerberos-authentication-for-sharepoint-2010-and-sql-server-2008-r2-products.aspx>.

