SAP BusinessObjects Integration Option for Microsoft SharePoint software Administrator Guide

- SAP BusinessObjects 4.0 Service Pack 5

2012-11-06

Copyright

2012-11-06

Contents

Chapter 1 Welcome to the Integration Option for Microsoft SharePoint software.................................5

1.1 About this Guide...5

1.1.1 History of this Document...5

1.2 Who Should Read this Guide?..5

1.3 What is the Integration Option for Microsoft SharePoint Software?...6

Chapter 2 Configuring the Integration Option for Microsoft SharePoint software.................................7

2.1 Understanding the Template Configuration File...7

2.2 Configuring the web.config Tags..7

2.3 Enabling Logging and Tracing in the Software...12

2.4 Creating Sites Enabled for Accessing SAP BusinessObjects Content Within SharePoint 13

2.4.1 Creating Sites Using the SAP BusinessObjects Site Definition Template 13

2.4.2 Creating Sites Using a SharePoint Site Template 14

2.5 Configuring Web Parts...15

2.5.1 Adding Web Parts...16

2.5.2 Connecting Web Parts...16

2.5.3 Adding IOMS-Display Search Results Web Part to a Blank Site..17

2.6 Enabling anonymous access on IIS for AnalyticalReporting..17

Chapter 3 Deploying the Software..19

3.1 Overview..19

3.2 Configuring the SAP BusinessObjects Business Intelligence platform....................................19

3.2.1 Security and Single Sign-On 19

3.2.2 User and Group Rights...26

3.2.3 Configuring Secure Socket Layer on IIS 6.0...26

3.2.4 Configuring Secure Socket Layer on IIS 7.5...28

3.2.5 Configuring ISA 2006 for Reverse Proxy...31

3.3 Configuring the Optional BI Platform Settings..34

3.3.1 Specifying a Server for Processing Reports...35

3.3.2 Specifying Parameter Settings..35

3.4 Scheduling and Scaling Recommendations..36

3.4.1 Exporting Reports...37

3.4.2 Data Source Information.....37
3.4.3 Report Rights.....37
3.4.4 Performance Improvement.....37
3.5 Crystal Report Considerations.....37

Appendix A More Information.....39

Index 41

Welcome to the Integration Option for Microsoft SharePoint software

1.1 About this Guide

This guide details configuration, deployment, and troubleshooting information for the integration Option for Microsoft SharePoint software.

1.1.1 History of this Document

The following table provides an overview of the recent history of this document:

Version	Date	Description
SAP BusinessObjects integration option for Microsoft SharePoint software 4.0, Service Pack 2	3rd August, 2011	First release of this document after XI 3.1 SP4
SAP BusinessObjects integration option for Microsoft SharePoint software 4.0, Feature Pack 3	16 March, 2012	To understand the new features of the software documented in this guide, refer to following topic: • Enabling Logging and Tracing in the Software • Enabling anonymous access on IIS for AnalyticalReporting • Configuring the web.config Tags

1.2 Who Should Read this Guide?

This guide is intended for the following audiences:

- Administrators who want to know how to configure the SAP BusinessObjects Business Intelligence (BI) platform to work with the integration option for Microsoft SharePoint software
- Portlet developers who want to know how to create customized portlets

Familiarity with the Microsoft SharePoint portal server is essential, as is a good working knowledge of both Crystal Reports and the SAP BusinessObjects BI platform.

1.3 What is the Integration Option for Microsoft SharePoint Software?

The integration option for Microsoft SharePoint software provides state-of-the-art integration of Business Intelligence content with Microsoft SharePoint portal. This software runs in your Web Browser and allows you to access the SAP BusinessObjects BI Platform content through the Microsoft SharePoint environment.

The main objective of this software is to eliminate the need for a separate platform or portal for accessing Business Intelligence data, for users of Microsoft SharePoint.

The software accomplishes the above objective in the following ways:

- It provides you with an out-of-the-box site template having the look,feel and behavior similar to that of Microsoft SharePoint. After deploying the software on your system, if you have the administrative rights, you can readily use this template to create a dedicated site for accessing the SAP BusinessObjects Business Intelligence(BI) platform content from within the Microsoft SharePoint environment.
- It gives you access to a Web Part gallery consisting of modular units of functionality called Web Parts. As a user holding administrative rights, you can configure these SAP BusinessObjects Web Parts to any site created within Microsoft SharePoint. This way, a SharePoint site can also be enabled for accessing or managing the SAP Businessobjects BI platform content based on the extent of requirements.
- It provides you with end-to-end capabilities such that you can perform all actions required to interact with the BI platform content conveniently and exhaustively while remaining within the SharePoint environment.

The different types of Business Intelligence objects include Crystal Reports documents, Web Intelligence documents, Publications, Xcelsius reports, Advanced Analysis Documents, Portable Data Format documents, Microsoft Excel spreadsheets, Microsoft Word files, program files, object packages and other reports.

For more information about SAP BusinessObjects Business Intelligence (BI) Platform , refer to the *SAP BusinessObjects Business Intelligence Platform Administrator Guide*, which is included with the BI platform. For more information about Crystal Reports, see the *Crystal Reports User' Guide*, which is included with Crystal Reports.

Configuring the Integration Option for Microsoft SharePoint software

This chapter describes how to configure the integration option for Microsoft SharePoint software for specific SharePoint deployments. For more information on general administrative tasks, refer to the documentation of Microsoft Office SharePoint server (2007 or 2010 based on your deployment).

2.1 Understanding the Template Configuration File

Every time a website is created by using the SharePoint solution, SharePoint uses an XML configuration template file to generate the *web.config* file entries.

This template also specifies the SAP BusinessObjects BI platform system information that you entered during installation. Hence, if you change the system on which the BI platform Central Management Server (CMS) is located, you need to update this XML file. In particular, you need to update the value for the **BusinessObjects Enterprise Central Management Server** key to ensure that the value matches the name of the CMS.

During installation, the integration option for Microsoft SharePoint software installation program updates the `web.config` file that is located in the standard root space of the SharePoint web server `(..\InetPub\wwwroot\wss\VirtualDirectories\<portnumber>)`. The installation program also creates a backup of the original `web.config` file, known as "`backup web.config`".This file is stored in the installation directory.

By default the SharePoint site is hosted on Port 80 and web.config file is located in the path `(C:\inetpub\wwwroot\wss\VirtualDirectories\80)`.

Note:
The `web.config` file for Microsoft SharePoint 2007 and SharePoint 2010 are maintained separately on the individual servers but the tags added by the integration option software during installation are almost common to both.

2.2 Configuring the web.config Tags

As an administrator, you can configure some specific tags in the `web.config` file to define behaviour of features provided by the integration option software.

These configurable tags are mentioned below:

Document Viewer

```
 <!-- Voyager viewer Url %id%, %type%, %lang% and %token% are substitution variables -->
<add key="BusinessObjects Enterprise SharePoint InfoView Voyager Viewer Url" value="http//<IP address of the
 CMS>/BOE/BI/OpenDocument/opendoc/openDocument.jsp?sIDType=CUID&amp;iDocID=%id%&amp;token=%to
ken%&amp;lang=%lang%" />

<!-- Document viewer Url %id%, %type%, %lang% and %token% are substitution variables -->
<add key="BusinessObjects Enterprise SharePoint InfoView Document Viewer Url" value="/_layouts/OpenDocu
ment/opendoc/openDocument.aspx?sKind=%type%&amp;sIDType=CUID&amp;iDocID=%id%&amp;token=%token%&amp;lang=%lang%"
 />

<add key="boe.trustguard.enable" value="true" /> </appSettings>
```

Crystal Viewer

```
<CrystalReports>
<add key="path.dhtmlViewer" value="/crystalreportviewers" />
</CrystalReports>
```

Infoview App Settings

```
<InfoViewAppSettings>
<!-- ==================== -->
<!-- Customizable options -->
<!-- You can specify the default CMS machine name here -->
<!-- Put your CMS name inside <param-value> "/> -->
<!-- eg. -->
<!-- <add key="cms.default</param-name> -->
<!--CrystalMS"/> -->
<add key="cms.default" value="localhost" />
<!-- Choose whether to let the user change the CMS name -->
<!-- If it isn't shown the default System from above will be used -->
<add key="cms.visible" value="false" /
<!-- You can specify the default Authentication types here -->
<!-- secEnterprise, secLDAP, secWinAD, secSAPR3 -->
<add key="authentication.default" value="secEnterprise" />
<!-- Choose whether to let the user change the authentication type -->
<!-- If it isn't shown the default authentication type from above will be used. If you make it true, you
would get the authentication field as a dropdown in the CMS logon screen of your BusinessObjects site -->
<add key="authentication.visible" value="false" />
<!-- The default home page -->
<add key="homepage.default" value="/listing/Home.aspx" />
<!-- If the locale preference is disabled (only english languages will be used/allowed) -->
<add key="disable.locale.preference" value="false" />
<!-- Set to false to disable Siteminder single sign on. -->
<add key="siteminder.enabled" value="false" />
<!-- You can specify the siteminder Authentication type here -->
<!-- secLDAP, secWinAD -->
<add key="siteminder.authentication" value="secLDAP" />
<!-- Set to true to enable other single sign on. -->
<add key="vintela.enabled" value="false" />
<add key="sso.enabled" value="false" />
<!-- Set to false to disable logon with token. -->

<add key="logontoken.enabled" value="true" />
<!-- For turning persistent cookies on/off for the logon page. Defaults to true if this is not present
-->
<add key="persistentcookies.enabled" value="true" />
<!--
Trusted authentication: set how to retrieve userID
set to "REMOTE_USER" for HttpServletRequest.getRemoteUser()
set to "HTTP_HEADER" for HTTP header
set to "QUERY_STRING" for URL query string
set to "COOKIE" for cookie
set to "WEB_SESSION" for web session
set to "USER_PRINCIPAL" for user principal
set to "VINTELA" for Vintela integration
reset to empty to disable trusted authentication
-->
<add key="trusted.auth.user.retrieval"
value="" />
<!--
```

```
Trusted authentication: set Header/URL parameter/Cookie/Session variable name to retrieve username
No need to set for REMOTE_USER or USER_PRINCIPAL.
-->

<add key="trusted.auth.user.param" value="" />
<!--
Trusted authentication: session variable name
to retrieve the shared secret;
Leave empty if shared secret is not passed from web session
-->

<add key="trusted.auth.shared.secret" value="" />
<!--
Configurable logon service
These 2 configurations allow one to customize the location of the logon service
config.logon.service.context: the service context path. e.g. /InfoViewApp
config.logon.service.url: the service url without context path. e.g. /logon/logon.do
-->

<add key="config.logon.service.context" value="" />
<add key="config.logon.service.url" value="" />
<!--
Configurable timeout service
These 2 configurations allow one to customize the location of the timeout service
config.timeout.service.context: the service context path. e.g. /InfoViewApp
config.timeout.service.url: the service url without context path. e.g. /logon/logon.do
-->

<add key="config.timeout.service.context" value="" />
<add key="config.timeout.service.url" value="" />
<!--
cms.clusters: comma separated list of cluster names
Each cluster in the above list requires its own parameter:
param-name = cms.clusters.<clustername> (without the @)
param-value = comma separated list of cms servers

note: Each param-name must match case with the corresponding value in cms.clusters.

note2: No port needs to be given for a server.
If none is given, then the default port 6400 is assumed.

Alternatively, these parameters may be put in a file called "clusters.properties" which should
be placed in the WEB-INF/classes directory. The parameters in this file should be stored
in the normal .properties format, i.e. one "<name>=<value> pair per line. If this file
exists, the settings in web.xml will be ignored
entirely.
-->

<!-- EXAMPLE:
<add key="cms.clusters" value="@samplecluster, @samplecluster2,
@samplecluster3"/>
<add key="cms.clusters.samplecluster" value="cmsone:6400, cmstwo"/>
<add key="cms.clusters.samplecluster2" value="cms3, cms4, cms5"/>
<add key="cms.clusters.samplecluster3" value="aps05"/>
-->
<!-- Sample equivalent clusters.properties file:
cms.clusters=@samplecluster, @samplecluster2, @samplecluster3
cms.clusters.samplecluster=cmsone:6400, cmstwo
cms.clusters.samplecluster2=cms3, cms4, cms5
cms.clusters.samplecluster3=aps05
-->

<!-- proxy.contextpaths: comma separated list of proxies -->
<!-- EXAMPLE:
<add key="proxy.contextpaths" value="/Infoview"/>
OR
<add key="proxy.contextpaths" value="/Marketing,/Sales/infoview,/HR"/>
-->
<add key="proxy.contextpaths" value=""/>
<!-- Default window properties when viewing a document in a new window. -->
<!-- Does not override the window properties defined in the plugin files. -->
<add key="window.properties.default"
value="fullscreen=yes,location=no,scrollbars=yes,menubars=no,toolbars=no,resizable=yes"
/>
<!-- location to pick up help files
-->
<add key="customized.help.location" value="" />
<!-- Shared Destination From Field -->
<!-- Enables or Disables the From field when scheduling a object to a destination.
When the value is set to false the From field will not be rendered and the system
will first attempt to get the email value from the report default, if report default
```

```
is not available it will attempt to get the value from the email address on user
profile of the logged on user and lastly if the user profile email address in not
available it will use the job server default.
-->
<add key="SMTPFrom" value="true" />
<!-- application name -->
<add key="app.name" value="BusinessObjects InfoView" />
<add key="app.name.short" value="InfoView"
/>
<add key="app.name.greeting" value="BusinessObjects" />
<add key="app.supportmygroups" value="false"/>
<add key="app.supportlocreports" value="false" />
<add key="app.ondemandlink" value="http://information.ondemand.com/istore/" />

<add key="app.ondemand.toolbar.button.enabled" value="false" />
<add key="app.ondemand.textlink.enabled" value="true" />
<!-- threshold at which the tree list control will not display all the nodes -->
<!-- instead, a too many children message will be printed -->
<add key="max.tree.children.threshold" value="200" />
<!-- URLs -->
<add key="url.exit" value="" />
<add key="url.error" value="common/error.aspx" />
<!-- Content : ALL schema and non-schema (global) file resources. -->
<!-- Resolution: Resource path resolves to <schemaPath>/<resourcePathAndFileName>.
-->

<!-- Prefixes : - Values prefixed with the
value given by schema.prefix are resolved to the current schema
-->
<!-- - Values prefixed with the value given
by schema.global.prefix are resolved as non-schema (global) items
-->
<!-- - NONE indicates no prefix
-->
<!-- - If these 2 prefixes are the same
(including both NONE) you essentially have NO global items.
-->
<!-- - If neither prefix is matched, item is "schema". -->
<!-- - The prefix is not part of the file spec. -->
<!-- Note : Only the default schema is now in use. -->
<!-- Schemas -->
<add key="schema.global.prefix" value="NONE" />
<add key="schema.prefix" value="*" />

<!-- context-relative paths -->
<add key="schema.global" value="/res/general" />
<add key="schema.default" value="/res/schema.blue" />
<!-- File resources -->
<add key="img.obj.default" value="ce_generic_object.gif" />
<add key="img.list.heading.separator" value="separator_grey_title_bar.gif" />
<add key="img.list.plus" value="collapse.gif" />
<add key="img.list.minus" value="expand.gif" />
<add key="img.banner.left" value="*IV_left_topbanner.gif" />
<add key="img.banner.right" value="*IV_right_topbanner.gif" />
<add key="img.banner.logo" value="*login_banner_center.gif" />

<!-- Sorting Arrows -->
<add key="img.sort.arrowdown" value="sort_desc.gif" />
<add key="img.sort.arrowup" value="sort_asc.gif" />

<!-- Panel gradient & buttons -->
<add key="img.panel.titlebar" value="*panel_title_bar_fill.gif" />
<add key="img.panel.footerbar" value="*panel_footer_bar_fill.gif" />
<add key="img.panel.new.window" value="*new_window.gif" />
<add key="img.panel.new.window.hover" value="*new_window_hover.gif" />
<add key="img.panel.arrowdown" value="*arrow_down.gif" />
<add key="img.panel.arrowdown.hover" value="*arrow_down_hover.gif" />
<add key="img.panel.arrowleft" value="*arrow_left.gif" />
<add key="img.panel.arrowleft.hover" value="*arrow_left_hover.gif" />
<add key="img.panel.arrowright" value="*arrow_right.gif" />
<add key="img.panel.arrowright.hover" value="*arrow_right_hover.gif" />

<add key="img.panel.arrowup" value="*arrow_up.gif" />
<add key="img.panel.arrowup.hover" value="*arrow_up_hover.gif" />
<add key="img.panel.close" value="*close_panel.gif" />
<add key="img.panel.close.hover" value="*close_panel_hover.gif" />
<add key="img.panel.maximize" value="*maximize.gif" />
<add key="img.panel.maximize.hover" value="*maximize_hover.gif" />
<add key="img.panel.minimize" value="*minimize.gif" />
<add key="img.panel.minimize.hover" value="*minimize_hover.gif" />
<add key="img.panel.restore" value="*restore_down.gif" />
```

```
<add key="img.panel.restore.hover" value="*restore_down_hover.gif" />
<add key="img.panel.tearoff" value="*tear_off.gif" />
<add key="img.panel.tearoff.hover" value="*tear_off_hover.gif" />

<!-- Toolbar (22x22) images -->
<add key="img.toolbar.calendar" value="toolbar/calendar.gif" />
<add key="img.toolbar.home" value="toolbar/home.gif" />
<add key="img.toolbar.refresh" value="toolbar/refresh.gif" />

<!-- Error (32x32) image -->
<add key="img.error" value="infoview_error.gif" />

<!-- InfoView homepage icons -->
<add key="img.home.myinfoview" value="MyInfoView.gif" />
<add key="img.home.favefolder" value="favfolder.gif" />
<add key="img.home.folder" value="folder.gif" />
<add key="img.home.help" value="help.gif" />
<add key="img.home.inbox" value="inbox.gif" />

<add key="img.home.preferences" value="preferences_infoview.gif" />
<add key="img.home.ondemand" value="ondemand.gif" />

<!-- JSTL Configuration -->
<add key="localizationContext" value="com.businessobjects.infoview.ApplicationResources"
/>

<!-- Clustering:
true - SessionCleanupListener will expire an Enterprise Session.
false - SessionCleanupListener will logoff an Enterprise Session.
-->
<add key="distributable" value="true" />
<!-- Uncomment the following context-param if you are using multi-byte characters with WebLogic
and you are not using CrystalUTF8InputActionServlet as the action servlet. Please
note that for this to work your application will need to send data to and receive data from the
client browser in UTF8. -->

<!--
<add key="weblogic.httpd.inputCharset./*"
value="utf-8"/>
-->

<add key="path.rightFrame" value="1" />
</InfoViewAppSettings>
<InfoViewAppActionMapping>
<add key="logon" value="/logon/logon.aspx" />
<add key="logonForm" value="/logon/logon.aspx" />
<add key="logonService" value="/logon/logon.aspx" />
<add key="timeout" value="/logon/logon.aspx" />

<add key="logoff" value="/logon/logoff.aspx" />
<add key="main" value="/listing/main.aspx" />
<add key="appService" value="/common/appService.aspx" />
<add key="help" value="/help/helpredir.aspx" />
</InfoViewAppActionMapping>
</configuration>
```

Exclusions

There are certain object types in the BI platform (BOE) repository that are not supported by the integration option for Microsoft SharePoint software. However, once users logon to SharePoint and connect to the CMS, all object types may appear on their sites. If you do not want the unsupported object types to appear on the BusinessObjects site, update the following tag in the web.config file:

```
 <add key="BusinessObjects Enterprise Object Exclusions" value="<exc_Obj1>,<exc_Obj2>,<exc_Obj3>" />
```

where {exc_Obj1, exc_Obj2...} are the objects you want to exclude. For example,

```
 <add key="BusinessObjects Enterprise Object Exclusions" value="MON.Probe,DFS.Parameters,PlatformSearchSchedul
ing,Analytic" />
```

2.3 Enabling Logging and Tracing in the Software

To enable logging and tracing for security and monitoring reasons, you need to perform certain configuration settings by making updates to the `web.config` file.

Perform the following steps:

1. Add the following tag and attribute values in the `<configSections>` of web.config:

```
<section name="log4net" type="log4net.Config.Log4NetConfigurationSectionHandler, log4net, Version=1.2.10.0,
 Culture=neutral, PublicKeyToken=692fbea5521e1304"/>
```

2. Add the following tag and attributes in the `<appSettings>` of web.config.

```
<add key="bobj.logging" value="True"/>
<add key="bobj.logging.log4net.override" value="[Physical path]\\Logs\\[FileName].xml"/>
```

3. Create an XML file with the same name as the one that you have specified in `FileName` above. Add the below content in this file:

```
<?xml version="1.0" encoding="utf-8" ?>
<log4net>
<!---   For log -->
  <root>
   <appender name="LogAppender" type="log4net.Appender.FileAppender" >
     <file value="E:\Logs\iPointLog.log"/> <!-- You can specify any path here but the container Folder
name for the log file has to be Logs -->
       <layout type="log4net.Layout.PatternLayout">
         <conversionPattern value="%date[%thread] %-5level %logger %class - %m%n" />
       </layout>
   </appender>
   <level value="FATAL"/>
   <level value="WARN"/>
   <appender-ref ref="LogAppender"/>
  </root>
<!-- End for log -->
</log4net>
```

Note:

1. For a developer trace file, the *`value`* attribute of `<level>` tag can have the following possible values:
   - INFO
   - DEBUG
   - ERROR
2. For an admin log file, the *`value`* attribute of `<level>` tag can have the following possible values:
   - FATAL
   - WARN
3. If you want the *`value`* attribute of `<level>` tag to have all possible values (including those for the developer trace and admin log), then you can set `<level value="ALL"/>`. If you want only specific values for the attribute, then you can add them individually as illustrated in the above example.
4. As of now, the logging feature is only implemented in the “Universal Repository Explorer”(URE) of the software. (URE is a custom control that is used in implementing certain views of the "User actions" web page of an SAP BusinessObjects site).

Essentially, this means that logging will occur only when you perform certain actions, such as setting scheduling options for an object (for example **Enterprise Recipients**, **Dynamic Recipients** for a publication), viewing **History** of an object, assigning **Categories** to an object, sending an object to Inbox etc.). All these actions involve the URE in different views of the "User actions" web page.

Logging will be implemented for all the Web Parts in future.

2.4 Creating Sites Enabled for Accessing SAP BusinessObjects Content Within SharePoint

Based on your requirement, you can create additional SharePoint sites that have access to the SAP BusinessObjects Business Intelligence(BI) platform content. You can do so in one of the following ways:

- By creating a site using any of the SharePoint templates and adding the BusinessObjects Web Parts to the sites pages.
- By creating a site using the SAP BusinessObjects Site Definition template that directly enables you to access and manage the BI platform data.

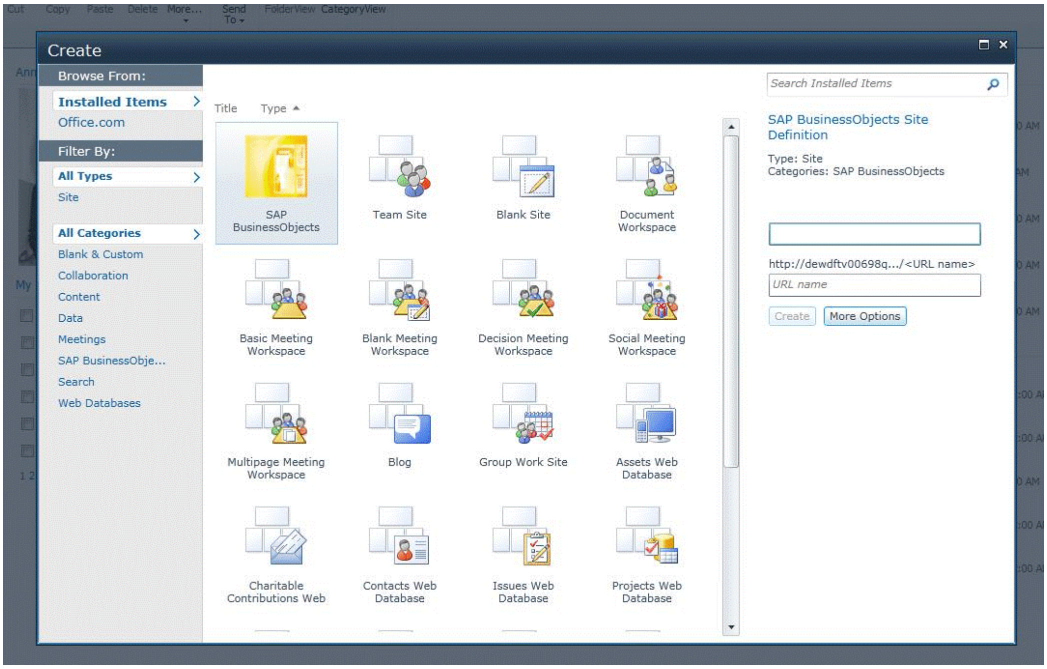
2.4.1 Creating Sites Using the SAP BusinessObjects Site Definition Template

The integration option provides you with an out-of-the-box solution that enables you to create a ready to use site.This solution is the SAP BusinessObjects Site Definition template. The structure and capabilities of this template are such that you can carry out all basic activities required for viewing, managing and interacting with the SAP BusinessObjects content from within the SharePoint environment.This template consists of the following Web Parts:

- IOMS-Advertisement
- IOMS-Content Explorer
- IOMS-Recent Searches
- IOMS-Recently Viewed
- IOMS-Display Search Results

These Web Parts are essential to work conveniently with objects in the SAP BusinessObjects BI platform from within the SharePoint system. The connection between the Web Parts is already established.

The “SAP BusinessObjects Site Definition” template appears within the `SAP BusinessObjects` category of site templates when you create a new site within SharePoint. After selecting this template, you can specify a URL for your unique site in the same way as you do for other SharePoint sites:



Type: Site
Categories: SAP BusinessObjects

Note:
The above image is a screenshot from the SharePoint 2010 platform. In SharePoint 2007, the interface is slightly different. However, the concept remains the same.

Note:
- To know more about the features provided by the SAP BusinessObjects Site Definition Template, read the *SAP BusinessObjects integration option for Microsoft SharePoint software Getting Started Guide*.
- Based on your requirements, you can also add the Viewer Web Parts provided by the integration option software, to the site created using the above mentioned template. To do so, you can refer to the Configuring Web Parts section of this guide.

2.4.2 Creating Sites Using a SharePoint Site Template

You can create sites on SharePoint portal using any of the various templates provided by Microsoft SharePoint, and thereafter add the SAP BusinessObjects Web Parts to it.

However, to be able to work with the Business Intelligence platform content through these Web Parts, you also need to activate certain site features explicitly. These are the SAP BusinessObjects site features provided by the integration option for Microsoft SharePoint software.

2.4.2.1 Activating the BusinessObjects Features of a Site

To activate the BusinessObjects features of your site, perform the following steps:

1. On the Home page of the site, access **Site Actions>Site Settings>Site Features**. On the Site Features page, you will see a couple of BusinessObjects features.
2. Click the **Active** button against the feature you want to activate. To deactive the feature, click **Deactivate** . The following table summarizes the site features and their purpose:

Feature	Significance
"SAP BusinessObjects Logon "	Activate this feature to connect to the Central Management Server(CMS). This feature is mandatory to activate as you need to connect to the CMS for working with the BI platform content.
"SAP BusinessObjects Log Off"	Activate this feature to log off from the CMS. This disconnects you from access to the BI platform content.
"SAP BusinessObjects Platform Action Pages"	Activate this feature to perform various actions on the reports or objects like setting object properties, scheduling, viewing history, assigning a category, sending etc.
"SAP BusinessObjects Preferences Settings"	Enable this feature to be able to set preferences like password, timezone and locale, date and time settings, Web Intelligence and Crystal Report preferences etc.

Having activated the mandatory and chosen features, you can now access and work with the BI platform content through the Web Parts added to your SharePoint site.

Note:
These features are already activated if you use the out-of-the-box solution called SAP BusinessObjects Site Definition template provided by the integration option, to create your site in SharePoint.

2.5 Configuring Web Parts

This section describes how to add various Web Parts to a SharePoint site page and connect them to the "IOMS-Content Explorer" Web Part.

2.5.1 Adding Web Parts

You can modify the appearance and functionality of a web page in the SharePoint system by adding Web Parts.

To add a Web Part, complete the following steps:

1. Open the web browser and navigate to the page in the SharePoint portal where you want to add the Web Part.

   Select **Edit Page** from the **Site Actions** drop-down list. The page reloads in the Edit mode.

2. Click **Add a Web Part**.

   The "Add Web Parts -- Web Page Dialog" window appears.

3. From the list of galleries, select the predefined Web Part that you want to add, and click **Add**.

   The Web Part is added to the SharePoint portal.

   Note:
   The Web Parts provided by the integration option can be found within the SAP BusinessObjects section of the "Add Web Parts -- Web Page Dialog".

2.5.2 Connecting Web Parts

When you configure SAP BusinessObjects Web Parts on any page of a SharePoint site, you might need to connect them with other Web Parts to conveniently view and interact with Business Intelligence(BI) platform data.

To connect any Web Part to the "IOMS-Content Explorer", complete the following steps:

Note:
You can connect to Web Parts only in the “Edit” mode.

1. In the "IOMS-Content Explorer" Web Part, click **edit**.
2. Select **Connections > Send RepositoryExplorer To**.

   All the Web Parts that have been added to the SharePoint page get listed.

3. Click the Web Part you want to connect to the "IOMS-Content Explorer" Web Part.

   The selected Web Part is connected to the "IOMS-Content Explorer" Web Part.

   For example, you can connect various Viewer Web Parts like IOMS-Xcelsius Viewer, IOMS-Crystal Report Viewer, IOMS-Analytical Report Viewer to the IOMS-Content Explorer Web Part.

2.5.3 Adding "IOMS-Display Search Results" Web Part to a Blank Site

To view the SAP BusinessObjects content search results and the SharePoint search results in a site created using the blank site template provided by SharePoint, you need to perform the following steps:

1. Create a site page. For example, Bobjsrch.aspx.
2. Add "IOMS-Display Search Results" and “Microsoft Search Core Results” Web Parts to this new page of your site.
3. Go to **Site Actions** > **SiteSettings** and then in "Site Collection Administration" section of page, click on **Search settings**.

   The **<Site Collection Search Results Page>** text field appears in the page which opens.
4. Enter the string “/SitePages/Bobjsrch.aspx” in this field.
5. Perform search on this page or any page of the site and you are successfully routed to the new page(Bobjsrch.aspx in this example), displaying all the search results retrieved from the BusinessObjects and SharePoint repositories based on your Query term.

Only after performig the above steps, you can carry out successful search in a SharePoint site of blank template.

2.6 Enabling anonymous access on IIS for AnalyticalReporting

To create or edit a Web Intelligence document from the Microsoft SharePoint portal, you need to enable the anonymous access on Internet Information Services (IIS) for AnalyticalReporting.

1. Go to **Start** > **Control Panel** > **Administrative Tools** > **IIS Manager** or in the command prompt, type inetmgr to open IIS manager.
2. Navigate to **Sites** > **SharePoint Site <port>** > **_layouts** > **AnalyticalReporting**.
3. In Features view, double-click **Authentication**.
4. In the Authentication page, select **Anonymous Authentication**.
5. In Actions pane, click **Enable**.

Deploying the Software

3.1 Overview

This chapter describes how to configure the SAP BusinessObjects Business Intelligence(BI) Platform to work with the integration option for Microsoft SharePoint software. It also discusses recommendations for scheduling reports and setting properties to improve the effectiveness of reports for users. To perform these activities, you must be familiar with administering and using the BI platform.

For more information about the BI platform, see the *SAP BusinessObjects Business Intelligence Platform Administrator' Guide*.

3.2 Configuring the SAP BusinessObjects Business Intelligence platform

When you first install the integration option for Microsoft SharePoint, you must configure or update certain settings within the SAP BusinessObjects BI platform to optimize your deployment.

3.2.1 Security and Single Sign-On

The integration option supports the following authentication modes with the BI platform deployment:

- Enterprise
- LDAP
- Windows AD

Automatic Sign-On is enabled when you set the value of “sso.enabled” flag as “true” in the template configuration (`web.config`) file:

```
<add key="sso.enabled" value="true" />
```

Note:
The template configuration file is found in the following locations:

- `C:\Inetpub\wwwroot\wss\VirtualDirectories\80`
- `C:\Program Files(x86)\SAP BusinessObjects\ SAP BusinessObjects Enterprise XI 4.0\ SharepointApp\InfoViewApp`

After installing integration option, you must ensure that the BI platform security settings are correct. Otherwise, users may encounter the following error message when they attempt to access the application:

```
"Unable to access the BusinessObjects Enterprise infrastructure at servername
to username. The infrastructure may not be accessible, or you have not been
granted access using automatic sign-on with authenticationmode. Contact your
reporting administrator for further details on availability."
```

If you are using LDAP or AD authentication, ensure the following:

- The LDAP or AD deployment is set up properly.
- The portal user names match the aliases in the authentication system.

For information on how to enable and configure CMC for the different authenticaton types, see the *SAP BusinessObjects Business Intelligence Platform Administrator' Guide*.

3.2.1.1 Configuring the Software for Windows AD Kerberos Authentication

To configure the integration option for Microsoft SharePoint software for Windows AD Kerberos authentication, perform the following steps:

1. Configure the SharePoint portal with Windows AD authentications. You can refer to the documentation of Microsoft SharePoint for this.
2. In SharePoint software, Create new web application, and select **Classic Mode Authentication**.
3. In Authentication provider section, select **Negotiate (Kerberos)**.
4. Configure Windows AD Kerberos authentications for the SAP BusinessObjects Business Intelligence platform (Enterprise). For this, refer to the "Authentication" section of the *SAP BusinessObjects Business Intelligence(BI) platform Administrator Guide*.
5. To verify if the Windows AD authentication is configured successfully on the BI platform, logon to the BI Launchpad using the credentials of a Windows AD authorized user.
6. In Windows AD domain controller for SharePoint server and Client machines, select **Trust this computer for delegation to any service (Kerberos only)** .
7. In SharePoint server open IIS manager.
8. In IIS manager select the site on which integration software is installed and deselect **Enable Kernel Mode Authentication**. For example, go to **SharePoint site** > **Authentication** > **Windows Authentication** > **Advanced Settings**. In **Advanced Settings** , deselect **Enable Kernel Mode Authentication**.
9. Set the value of the `authentication.visible` flag to “true” in the following files of the integration option for Microsoft SharePoint software:
   a. The InfoView app at `C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\Web Content\SharepointApp\InfoViewApp`

10. To verify if Windows AD Kerberos authentication has been configured correctly for the integration option for Microsoft SharePoint software, logon to integration option using the credentials of a Windows AD authorized user.
11. In the Client Browser trusted site, Add SharePoint Fully Qualified Domain Name URL. For example, If the browser is Internet Explorer, go to**Internet Options** > **Security** > **Trusted Site Zone** > **Sites**.
12. Select SharePoint FQDN, and Click **Add**.
13. For more information regarding SharePoint software configuration troubleshooting see *http://blogs.technet.com/b/mbiswas/archive/2009/07/10/configure-kerberos-authentication-office-sharepoint-server.aspx*

3.2.1.2 Configuring the Software for Windows AD Kerberos SSO (Single Sign On)

To configure the integration option for Microsoft SharePoint for Windows AD single sign on (SSO), perform the following steps:

1. Make sure that a Windows AD user is able to logon to the integration option for Microsoft SharePoint software.
2. Enable SSO (Single Sign On) in the Central Managment Console. For understanding how to do so, refer to the "Authentication" section of the *SAP BusinessObjects Business Intelligence(BI) platform Administrator Guide*.
3. Set the value of the `sso.enabled` flag to “true”, `authentication.default` to “secWinAD” and “identity impersonate” flag to “true” in the following files of the integration option for Microsoft SharePoint software:
   a. The InfoViewapp at `C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\Web Content\SharepointApp\InfoViewApp`
   b. The SharePoint platform services at `C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\Web Content\SharepointApp\PlatformServices`
   c. The OpenDocument file at `C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\Web Content\SharepointApp\OpenDocument`
4. Restart the IIS server.
5. Logon to the client machine with the credentials of a Windows AD authorized user.
6. If the browser is Internet Explorer, go to**Internet Options** > **Security** > **Custom Level** > **User Authentication** > **Logon** and select the *`Automatic logon with current user name & password`* option.
7. From the client, access the URL of the machine hosting the integration option for Microsoft SharePoint software. The user should be able to login to the software automatically using his Windows AD account credentials.

Note:
If the SSO logon fails, take the following steps for troubleshooting:

- Clear the browser cookies, launch a new browser window and access the URL of the machine having the integration option software deployed on it.

- Refer to the CMS (Central Management Server) logs.
- Make sure that the Windows AD authentication types of SharePoint & the SAP BusinessObjects BI platform (Enterprise) are the same (AD Kerberos).
- For more information regarding SharePoint software configuration troubleshooting see *http://blogs.technet.com/b/mbiswas/archive/2009/07/10/configure-kerberos-authentication-office-sharepoint-server.aspx*

3.2.1.3 Configuring the Software for Windows AD NTLM Authentication

To configure the integration option for Microsoft SharePoint software for Windows AD NTLM authentication, perform the following steps:

1. Configure the SharePoint portal with Windows AD authentications. You can refer to the documentation of Microsoft SharePoint for this.
2. In SharePoint software, Create new web application, and select **Classic Mode Authentication**.
3. In Authentication provider section, select **NTLM**.
4. Configure Windows AD NTLM authentications for the SAP BusinessObjects Business Intelligence platform (Enterprise). For this, refer to the "Authentication" section of the *SAP BusinessObjects Business Intelligence(BI) platform Administrator Guide*.
5. To verify if the Windows AD authentication is configured successfully on the BI platform, logon to the CCM (Central Configuration Manager) using the credentials of a Windows AD authorized user.
6. Set the value of the `authentication.visible` flag to “true” in the following files of the integration option for Microsoft SharePoint software:
   a. The InfoViewapp at `C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\Web Content\SharepointApp\InfoViewApp`
7. To verify if Windows AD NTLM authentication has been configured correctly for the integration option for Microsoft SharePoint software, logon to integration option using the credentials of a Windows AD authorized user.

3.2.1.4 Configuring the software for Windows AD NTLM SSO (Single Sign On)

To configure the integration option for Microsoft SharePoint for Windows AD single sign on (SSO), perform the following steps:

1. Make sure that a Windows AD user is able to logon to the integration option for Microsoft SharePoint software.
2. Enable SSO (Single Sign On) in the Central Managment Console. For understanding how to do so, refer to the "Authentication" section of the *SAP BusinessObjects Business Intelligence(BI) platform Administrator Guide*.

3. Set the value of the `sso.enabled` flag to “true”, `authentication.default` to “secWinAD” and “identity impersonate” flag to “true” in the following files of the integration option for Microsoft SharePoint software:
   a. The InfoViewapp at `C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\Web Content\SharepointApp\InfoViewApp`
   b. The SharePoint platform services at `C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\Web Content\SharepointApp\PlatformServices`
   c. The OpenDocument file at `C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\Web Content\SharepointApp\OpenDocument`
4. Restart the IIS server.
5. Logon to the client machine with the credentials of a Windows AD authorized user.
6. If the browser is Internet Explorer, go to**Internet Options** > **Security** > **Custom Level** > **User Authentication** > **Logon** and select the *Automatic logon with current user name & password* option.
7. From the client, access the URL of the machine hosting the integration option for Microsoft SharePoint software. The user should be able to login to the software automatically using his Windows AD account credentials.

Note:
If the SSO logon fails, take the following steps for troubleshooting:
- Clear the browser cookies, launch a new browser window and access the URL of the machine having the integration option software deployed on it.
- Refer to the CMS (Central Management Server) logs.
- Make sure that the Windows AD authentication types of SharePoint & the SAP BusinessObjects BI platform (Enterprise) are the same (AD NTLM).

3.2.1.5 Configuring the software for LDAP Authentication

You must install MOSS 2007 and LDAP Server. You must also create groups and users in LDAP.

A SharePoint web application must be created on MOSS 2007. If MOSS 2007 and LDAP are on different systems, then you must ensure that these two systems can communicate with each other.

To configure the integration option software for Windows LDAP, complete the following steps:

1. Log into the SharePoint 3.0 Central Administration site.
2. Click the **Application Management** tab.
3. Under SharePoint Web Application Management, click the **Create or extend Web Application** link.
4. Click **extend web application**.
5. Specify the port name, host name, and so on.
6. From the **Zone** drop-down list, select **Custom**, and click **Create**.

   The extended application is created.

7. Click **Application Management**.
8. Under **Application Security**, click the **Authentication Providers** link.
9. In the "Authentication Providers" page, click the **Zone** link.
10. In the "Edit Authentication" page, select **Forms** as the authentication type.
11. Enter the membership provider name in the **Membership Provider Name** field.

    The LDAP membership name refers to the name of LDAP membership provider that you specify in the `web.config` file.

12. Enter the role manager name in the **Role Manager Name** field.
13. Select **No** for the **Enable Client Integration?** option.
14. Click **Save**.

The <Authentication mode> in the `web.config` file of the extended web application is modified to "Forms".

3.2.1.5.1 Modifying the `web.config` File of the Extended Web Application for LDAP

To modify the `web.config` file of the extended application for LDAP, complete the following steps:

1. Open the Central Administration Console from IIS, and open the `web.config` file.
2. In the `web.config` file, add the following lines between the </system.web> and <runtime> elements:

```
<connectionStrings>
<add name="LDAPConnectionString"
connectionString="ldap://bo-test.product.businessobjects.com:35020/dc=product,
dc=businessobjects, dc=com"/>
</connectionStrings>
```

3. In the `web.config` file, add the following membership provider details between the </authorization> and <httpModules> elements:

```
<membership defaultProvider="LDAPMembership">
<providers>
<add name="LDAPMembership"
type="Microsoft.Office.Server.Security.LDAPMembershipProvider,Microsoft.Office.Server,
Version=12.0.0.0,
Culture=neutral,PublicKeyToken=71e9bce111e9429c"
server="bo-test"
port="35020"
useSSL="false"
userDNAttribute="dn"
userNameAttribute="uid"
userContainer="dc=product,dc=businessobjects,dc=com"
userObjectClass="top"
useDNAttribute="false"
userFilter="(ObjectClass=top)"
scope="Subtree"
otherRequiredUserAttributes="sn,givenname,cn"/>
</providers>
</membership>
```

Note:
The values specified may differ based on how the user has been created in LDAP.

4. In the `web.config` file of the web application, add the following role manager details:

```
<roleManager defaultProvider="LDAPRoleProvider"
enabled="true" cacheRolesInCookie="true"
cookieName=".PeopleDCRole">
<providers>
<add name="LDAPRoleProvider"
type="Microsoft.Office.Server.Security.LDAPRoleProvider,
Microsoft.Office.Server, Version=12.0.0.0, Culture=neutral,
PublicKeyToken=71E9BCE111E9429C" server="bo-test" port="35020"
useSSL="false"
groupContainer="dc=product,dc=businessobjects,dc=com"
groupNameAttribute="cn"
groupMemberAttribute="uniquemember"
userNameAttribute="uid"
dnAttribute="dn"
useUserDNAttribute= "false"
groupFilter="(ObjectClass=top)"
scope="Subtree" />
</providers>
</roleManager>
```

5. In the `web.config` file of the Central Administration site, add the following role manager details between the </authorization> and <httpModules> elements:

```
<roleManager
defaultProvider="AspNetWindowsTokenRoleProvider"
enabled="true" cacheRolesInCookie="true"
cookieName=".PeopleDCRole">
<providers>
<add name="LDAPRoleProvider"
type="Microsoft.Office.Server.Security.LDAPRoleProvider,
Microsoft.Office.Server, Version=12.0.0.0, Culture=neutral,
PublicKeyToken=71E9BCE111E9429C"
server="bo-test"
port="35020"
useSSL="false"
groupContainer="dc=product,dc=businessobjects,dc=com"
groupNameAttribute="cn"
groupMemberAttribute="uniquemember"
userNameAttribute="uid"
dnAttribute="dn"
useUserDNAttribute= "false"
groupFilter="(ObjectClass=top)"
scope="Subtree" />
</providers>
</roleManager>
```

6. Restart IIS.
7. Log into Central Administration, and click the **Application Management** tab.
8. Click **Site Collection Administrators**.
9. Add any LDAP user as the primary administrator. While adding an LDAP user as the primary administrator, ensure that the user is identified.
10. Log into the SharePoint site as the site administrator with LDAP user rights.

3.2.1.5.2 Adding Users and Groups to the Web Applications

A user who logs into the web application as the site administrator can perform all administrative tasks, including creating and deleting users and user groups. However, other LDAP users can log in only if they have already been added to the web application.

To add users and user groups to the web application, complete the following steps:

1. Log into the web application as the site administrator.
2. Select **Site Settings** > **People and Groups**, and add the LDAP groups or users in the **Add the LDAP Groups or Users** field, as follows:
   - To add a group, use the following syntax: `ldaproleprovidername: groupname`
   - To add a user, specify the user name.

3.2.1.5.3 Logging into the Extended Application as an LDAP User

To log into the extended application as an LDAP user, complete the following steps:

Note:
All the steps must be performed manually in IIS.

1. Enable **Integrated Authentication**, and disable **Anonymous logon**.

   Note:
   Ensure that you have enabled LDAP authentication in CMS, and test whether the LDAP user can log into InfoView.

2. Compare the base application's *`web.config`* file with the extended application's *`web.config`* file, and modify the extended application's *`web.config`* file to include the missing entries.
3. Convert the InfoviewApp, InfoviewAppActions, PlatformServices, and AnalyticalReporting folders to virtual directories. Ensure that these virtual directories in the extended application point to the same application pool in the base application.
4. Copy the contents of the base application's *`"<Sharepoint:port\bin>"`* folder to the extended application's *`<"ExtendedApplication:Port\bin>`* folder.
5. Create a virtual directory called *`crystalreportviewers12`* and point it to `C:\Program Files\BusinessObjects\common\4.0\crystalreportviewers12`

3.2.2 User and Group Rights

Users need View rights to view the scheduled reports and the instances that have already been triggered. However, they need “View On Demand ”rights to access reports real-time.

To ensure that all users have view rights, in the BI platform CMC, add the users to the group “Everyone” and then assign view rights to this group. The view rights enable all users who belong to the group “Everyone” to view reports from within the SharePoint environment.

For more information about setting user rights, see the *SAP BusinessObjects Business Intelligence Platform Administrator Guide*.

3.2.3 Configuring Secure Socket Layer on IIS 6.0

To configure Secure Socket Layer (SSL) on IIS 6.0, complete the following steps:

1. Log into the SharePoint 3.0 Central Administration site.
2. Click the **Application Management** tab, and click **Create** or **Extend Web Application**.

3. From the **Web Application** drop-down list, select **Extend an Existing Web Application**, and select the web application for which you want to configure SSL.
4. In the "Create New IIS website" field, enter an appropriate value.
5. In the Port field, specify the default SSL port.
6. Select the **Use SSL** checkbox.

   Note:
   Ensure that correct value is specified in the "URL" field.

7. From the "Zone" field, select **Custom**.
8. Click **OK**.
9. Navigate to the IIS website, select the new site that you have created, and select **Properties**.

   Note:
   Ensure that this website is created on port 80. However, if another website already exists on port 80, change your newly created website's port to some other port. This is because two websites cannot run on port 80.

10. In the "Properties" page, click the **Directory Security** tab.
11. Click **Server certificates**.
    - If a server certificate already exists on the system, select **Assign an existing certificate**, and follow the on-screen instructions displayed in the Wizard.
    - If no certificates exist, then you must create a certificate. For IIS 6.0, download the certificate creation utility from the Internet and install it.
12. In the Secure Communications section of the **Directory Security** tab, click **Edit**.
    - Select **Require SSL** and **128 bit encryption** to access the site by using https. If these options are not enabled, the site can be accessed by using either http or https.
13. Select the **Ignore client certificates** radio button if there are no client certificates.
14. Click **OK**.
15. Click **Apply**.
16. Navigate to the "SharePoint 3.0 Central Administration" page, and select the **Operations** tab.
17. Click the **Alternate Access Mappings** link.
18. From the **Alternate Access Mapping Collection** drop-down list, select the collection for which you want to map SSL.

    Ensure that a public URL is specified for the custom zone. If a public URL is not already specified, you must add a public URL to the custom zone.

19. Open a browser, and specify the SSL URL.

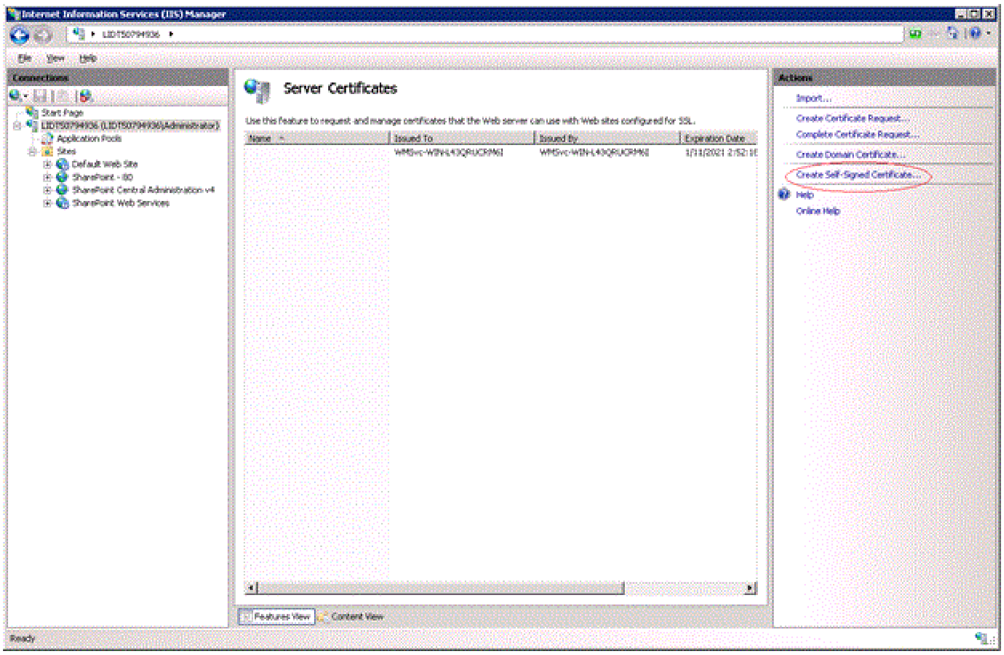
    Note:
    You can navigate through all the pages or web parts of the site. However, you must ensure that the URL does not change from https to http while you navigate the pages or web parts.

3.2.4 Configuring Secure Socket Layer on IIS 7.5

IIS 7.5 is the Web application server that supports Microsoft Office SharePoint Server(MOSS) 2010.

To configure the SSL on Internet Information Server 7.5, perform the following steps:

1. Login to the machine where the IIS 7.5 is running, and run `inetmgr` command through the "Run" window.
2. In the window which opens, select the root server node. You should see the features list in the right pane. If you dont find it, then right click on the root node and select the **Switch to Features View** option.
3. Double click the **Server Certificates** option to create a self signed certificate as shown below:



Internet Information Services (IIS) Manager
LIDT50794936
File
View
Help
Connections
Start Page
LIDT50794936 (LIDT50794936\Administrator)
Application Pools
Sites
Default Web Site
SharePoint - 80
SharePoint Central Administration v4
SharePoint Web Services
Actions
Import...
Create Certificate Request...
Complete Certificate Request...
Create Domain Certificate...
Create Self-Signed Certificate...
Help
Online Help
Features View
Content View
Ready

Server Certificates

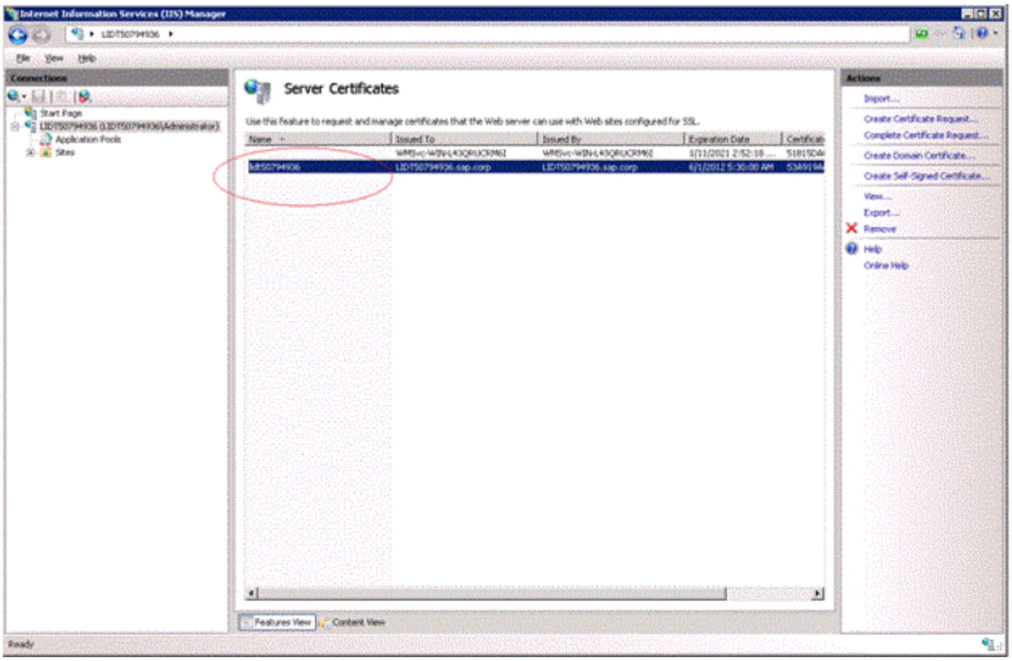
Use this feature to request and manage certificates that the Web server can use with Web sites configured for SSL.

Name	Issued To	Issued By	Expiration Date
	WMSvc-WIN-L43QRUCRM6I	WMSvc-WIN-L43QRUCRM6I	1/11/2021 2:52:1

4. Click on **Create Self-Signed Certificate** option from the Actions pane.

   The "Create Self-Signed Certificate" window opens asking you enter a friendly name for the certificate.
5. Give a friendly name for the certificate, generally it should be the machine name where the IIS is running. Click **OK**.

The certificate gets created and you can see it as follows:


Internet Information Services (IIS) Manager
LIDT50794936
File
View
Help
Connections
Start Page
LIDT50794936 (LIDT50794936\Administrator)
Application Pools
Sites
Server Certificates
Actions
Import...
Create Certificate Request...
Complete Certificate Request...
Create Domain Certificate...
Create Self-Signed Certificate...
View...
Export...
Remove
Help
Online Help
Features View
Content View
Ready

Use this feature to request and manage certificates that the Web server can use with Web sites configured for SSL.

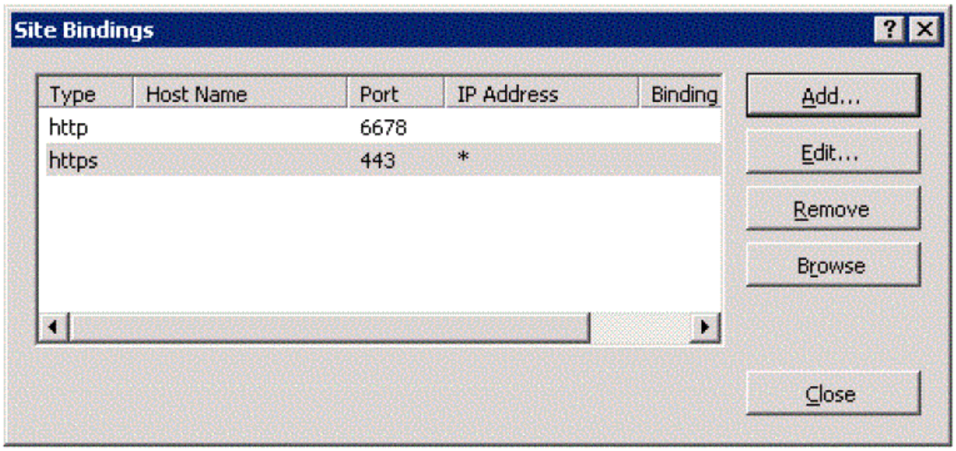
Name	Issued To	Issued By	Expiration Date	Certificat
	WMSvc-WIN-L43QRUCRM6I	WMSvc-WIN-L43QRUCRM6I	1/11/2021 2:52:18 ...	51815DA
ldt50794936	LIDT50794936.sap.corp	LIDT50794936.sap.corp	6/1/2012 5:30:00 AM	53A919A

6. Under **Sites** in the "Connections" pane on the left, select on the Sharepoint site for which you want to enable the SSL. Right click on it and select the **Edit Bindings** option.

   The "Site Bindings" window, opens up.

7. Click **Add** on the "Site Bindings" window . On the "Add Site Binding " window which opens, select the Type as 'https', keep the default port as 443, and select the certificate created in earlier from the SSL Certificate list box, and then click OK.

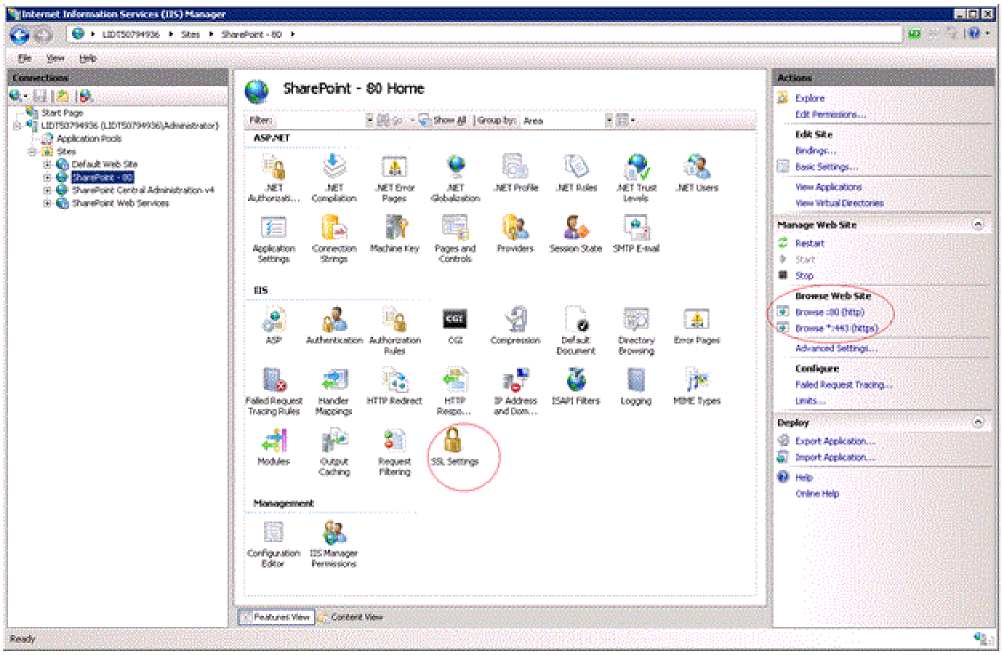
   Your entry will get added to the "Site Bindings" window as shown below:



Type	Host Name	Port	IP Address	Binding
http		6678		
https		443	*	

8. Close the "Site Bindings" window by clicking **Close**.

   Now, when you select your site(in the left panel of the "IIS Manager" window), then the on the right side pane , the "Actions"> "Manage Web Site">" Browse Web Site" section should list the new binding value as: "Browse *:443



(h

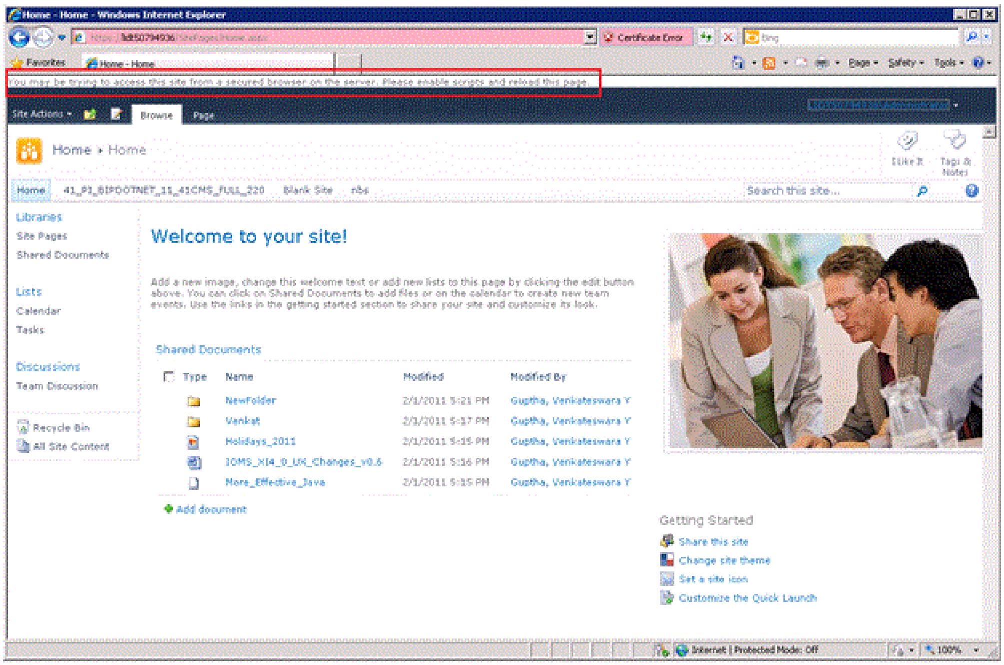
9. Double click on **SSL Settings** feature from the IIS features' list in the middle pane. In the view which opens, select the check box **Require SSL** and then click on **Apply** from "Actions" pane on the right side.

   Now your selected site is ready with the SSL URL and the default port.

10. Access the site through its URL (e.g https://lidt50794936), and select the**Continue to this website (not recommended)** link. Thereafter, give the Sharepoint login credentials and logon to the site.

    You should get the site warning as follows:

    "You may be trying to access this site from a secured browser on the server. Please enable scripts and re-load this page."



You may be trying to access this site from a secured browser on the server. Please enable scripts and reload this page.

Welcome to your site!

Add a new image, change this welcome text or add new lists to this page by clicking the edit button above. You can click on Shared Documents to add files or on the calendar to create new team events. Use the links in the getting started section to share your site and customize its look.

Shared Documents

Type	Name	Modified	Modified By
	NewFolder	2/1/2011 5:21 PM	Guptha, Venkateswara Y
	Venkat	2/1/2011 5:17 PM	Guptha, Venkateswara Y
	Holidays_2011	2/1/2011 5:15 PM	Guptha, Venkateswara Y
	IOMS_XI4_0_UX_Changes_v0.6	2/1/2011 5:16 PM	Guptha, Venkateswara Y
	More_Effective_Java	2/1/2011 5:15 PM	Guptha, Venkateswara Y

11. To get rid of the warning, add the https URL to the "Trusted Sites". (Go to "Internet Options"> click the "Security" tab > select "Trusted Sites" > click the **Add** button > add the URL and click **OK**.)

    When you access the SSL enables site now, the warning will not appear any more.

Note:
If you are accessing the Sharepoint SSL URL from any remote client machine, then you have to export the certificate to the server and import it on the remote client machine.

3.2.5 Configuring ISA 2006 for Reverse Proxy

Install ISA 2006 by using your Windows credentials.

To configure ISA 2006, complete the following steps:

1. Launch ISA 2006.
2. Right-click **Firewall Policy** > **New** > **SharePoint Site Publishing Rule**.

   The "Welcome to the SharePoint Publishing Rule Wizard" screen appears.
3. Enter the publishing rule name in the **SharePoint publishing rule name** field, and click **Next**.

   The "Publishing Type" screen appears.
4. Select **Publish a single Web site or load balancer**, and click **Next**.

   The "Server Connection Security" screen appears.

5. Select **Use non-secured connections to connect the published Web server or server farm**, and click **Next**.

   The "Internal Publishing Details" screen appears.

6. In the **Internal Site name** field, enter the internal site name. The internal site name refers to the system on which MOSS is running.
7. Select **Use a computer name or IP address to connect to the published server**, specify the system name or IP address in the **Computer name or IP address** field, and click **Next**.

   The "Public Name Details" screen appears.

8. From the **Accept Request for** drop-down list, select **Any domain name**, and click **Next**.

   The "Select Web Listener" screen appears.

9. Click **New**.

   The "Welcome to the New Web Listener Wizard" screen appears.

10. Specify the web listener name, and click **Next**.

    The "Client Connection Security" screen appears.

11. Select **Do not require SSL secured connections with clients**, and click **Next**.

    The "Web Listener IP Addresses" screen appears.

12. Select **External**, **Internal**, and **Local Host**, and click **Next**.

    The "Authentication Settings" screen appears.

13. Select **No Authentication**, and click **Finish**.
14. Select the newly created listener, and click **Properties** > **Authentication**.
15. Click the **Advanced** button, and select **Require all users to authenticate** and **Allow Client Connections over Http**.

    The "Authentication Delegation" screen appears.

16. From the drop-down list, select **No delegation, and client cannot authenticate directly**.

    The "Alternate Access Mapping Configuration" screen appears.

17. Select one of the following options based on your requirements:
    - **SharePoint AAM is already configured on the SharePoint server**
    - **SharePoint AAM is not yet configured. Also select this option if you are unsure if AAM is configured.**
18. Click **Next**.

    The "Completing the New SharePoint Publishing Rule Wizard" screen appears.

19. Click **Finish**.

    The publishing rule is created.

20. Select the publishing rule, and click **Apply**.
21. Right-click the rule, and select **Properties**.

    The "Properties" screen appears.

22. Select the **Listener** tab, and verify the port and protocol.

Note:
By default, port 80 is used. To change the port number, use the **Connections** tab.

23. Select the **Public Name** tab.
24. From the **This rule applies to** drop-down list, select **Requests for the following Web sites**, and specify the reverse proxy system.

    In "Path Names", map the client path to the server path.
25. Select the **To** tab, and verify the name and IP address of the destination system.
26. Select the **Bridging** tab.
27. Select **Redirect requests to HTTP port**, and specify the port in which the extended SharePoint website is running.

    Note:
    If you want the reverse proxy to point to the extended application, then you must specify the port number of the extended application. If you want the reverse proxy to point to the base application, then you must specify the base application's port.
28. Select the rule, and click **Apply**.

3.2.5.1 Configuring Reverse Proxy for the Base SharePoint Application

Ensure that ISA 2006 is configured on the Integration Option software.

To configure reverse proxy for the base SharePoint application, complete the following steps:

1. Log into the Central Administration site.
2. Click **Operations**, and click the **AlternateAccessmapping** link.
3. From the drop-down list, select the web application.
4. Click the **Add Internal URL** link, and add the reverse proxy URL.
5. From the **Zone** drop-down list, select the **Default** zone.
6. In IIS, change **Authentication type** to **Basic**.

3.2.5.2 Creating an Extended Website for the Web Application

To create an extended website for the web application, complete the following steps:

1. Log into the SharePoint 3.0 Central Administration site.
2. Click the **Application Management** tab, and click the **create or extend web application** link.
3. From the **Web Application** drop-down list, select **Extend an Existing Web Application.**
4. Select the web application for which you want to configure a reverse proxy application.
5. Specify the description, port, URL and so on in the appropriate fields.

6. Select a zone (for example, Internet), and click **OK**.
7. Navigate to the Central Administration site, click the **Operations** tab, and click the **AlternateAccessMapping** link.
8. From the drop-down list, select the web application.
9. Click **Add Internal URL** link, and add the reverse proxy URL.
10. From the Zone drop-down list, select the zone for the extended application.
11. Click **OK**.

An extended website is created for the web application.

3.2.5.3 Modifying the *`web.config`* File of the Extended Web Application for Reverse Proxy

To modify the *`web.config`* file of the extended web application for reverse proxy, complete the following steps:

1. Copy all the dlls and folders from the bin folder of the base application to the bin folder of the extended applications.
2. In the *`web.config`* file of the base application, ensure that only one sessionState entry exists, that is, `<"sessionState mode = Inproc"/>`. Comment any other entries.
3. In the extended application, create a virtual directory called crystalreports12 and point it to `C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\win64_x64\dotnet\crystalreportviewers12`
4. Convert the following folders to virtual directories:
   - Infoviewapp
   - InfoviewAppActions
   - PlatformServices
   - Analytical Reporting
   - CrystalReports
   - Xcelsius

   Note:
   Ensure that the virtual directories in the extended application point to the same application pool in the base application.
5. Compare the base application's *`web.config`* file with the extended application's *`web.config`* file, and modify the extended application's *`web.config`* file to include the entries that are missing.

3.3 Configuring the Optional BI Platform Settings

This section describes how to configure the optional BI platform settings for your SharePoint deployment.

3.3.1 Specifying a Server for Processing Reports

By default, the reports that users view are processed by the SAP BusinessObejcts BI platform page server. If the page server is not available, then the Report Application Server (RAS) is used.

If you want to configure the system to use the RAS to process reports, create a new Server Group for your RAS in the BI platform, specify this server group in all the reports, and then stop the platform page server.

To specify a server for report processing, complete the following steps:

1. Log into the CMC.
2. In the **Object Management** area of the Central Management Console (CMC), select an object by clicking its link.
3. Click the **Process** tab.
4. In the **Default Servers To Use For Viewing** area, select any of the following options:
   - **Use the first available server** - If you select this option, then the BI platform uses the server that has the maximum number of free resources when you view a report.
   - **Give preference to servers belonging to the selected group** - If you select this option, then the BI platform attempts to process the object by using the servers in the server group that you select from the list. If the specified servers are not available, then the object is processed by using the next available server, which may not belong to the selected group.
   - **Only use servers belonging to the selected group** - If you select this option, then the BI platform uses only the servers in the server group that you select from the associated drop-down list. If none of the servers in the server group are available, then the object is not processed.
5. Click **Update**.

3.3.2 Specifying Parameter Settings

Parameter prompts are enabled only when you view reports real-time (unless the parameter is a stored procedure). In the Central Management Console (CMC), you must ensure that the **Prompt when viewing** check box is selected; otherwise, the prompts are disabled, and the users cannot modify the values of the prompts in the report.

You must ensure the following to enable users to work with reports that contain parameters:

- Ensure that users are given View On Demand rights to enable them to view reports that include parameters.
- To allow users to modify parameter values, you must ensure that the reports they view are real-time reports. However, real-time reports can be resource-intensive; therefore, to reduce the processing

load on the BI platform services, you must ensure that users work with scheduled reports whenever possible.

- If you want users to work with a report for two different purposes (for example, real-time filtering and general viewing by date), then you must create two copies of the report. Allow users to view the report on demand for real-time filtering. To facilitate general viewing by date, you can schedule the report to run as often as required. Creating two copies of the report reduces the processing load on the system resources, because only the real-time filtering report needs to be viewed on demand.

To specify parameter settings, complete the following steps:

1. Log into the CMC.
2. In the **Objects Management** area of the CMC, select a report by clicking its link.
3. In the report, click the **Process** tab, and then click the **Parameters** link.
4. Under the **Value** column, select the value that is associated with the parameter that you want to modify.
5. Select **Prompt when viewing** to ensure that users are prompted when they view the report instance in the corresponding web part.
6. Click **Submit**.

3.4 Scheduling and Scaling Recommendations

The Business Intelligence (BI) platform schedules, processes, and runs reports. The general scheduling and scaling recommendations for the BI platform also apply to the integration option for Microsoft SharePoint. Use the Central Management Console (CMC) to specify the different scheduling properties for reports. For information about additional scheduling recommendations, see the *SAP BusinessObjects Business Intelligence Platform Administrator Guide*.

When setting scheduling properties for reports, consider the following recommendations:

- If you have reports that need to be updated regularly, and if users are going to access the same set of data, then you must schedule the reports to run per your requirements.
- If you want to view a report, you must schedule and run the report instead of viewing it on demand. Scheduled reports are less resource-intensive.
- If you grant View on Demand rights to users, the reports access the data source whenever users attempt to refresh them.
- When designing your portal, you must exercise caution while combining the web parts of integration option software, which contain real-time views, with third-party web parts that are page refresh intensive. When a user refreshes a page, all the reports in the web page are refreshed. For example, if a web page contains a stock ticker that is refreshed every ten seconds, all the reports in this web page are also refreshed every ten seconds.

3.4.1 Exporting Reports

For reasons related to the performance of the integration option software, you must set the export options (Microsoft Excel, Adobe Acrobat, and so on) at schedule time. When users export reports dynamically by selecting the alternative format viewing options on the toolbar, the requests become process and resource intensive.

3.4.2 Data Source Information

Set your database logon information for your reports through the CMC; otherwise, users need to log into the database each time they refresh or view a report.

3.4.3 Report Rights

If the report contains parameters, users who view the report require View On Demand rights.

If you are using the Page Server to view the summaries of different reports, you must grant Edit rights to users.

3.4.4 Performance Improvement

To improve the performance of the integration option for Microsoft Office SharePoint if you are not using a web farm, the session state on the web application server is enabled by default.

3.5 Crystal Report Considerations

When you create a Crystal report, consider the following recommendations:

- Ensure that the background of your report is transparent.
- Ensure that you have the Adobe Flash Player installed on your machine.

- Make maximum use of your screen resolution and space for your report parts.
- Ensure that parameter names are short and that parameter descriptions are meaningful and useful, because users can view the parameter names and descriptions in the toolbar.

For information about creating Crystal reports, see the *Crystal Reports User' Guide*.

More Information

Information Resource	Location
SAP BusinessObjects product information	http://www.sap.com
SAP Help Portal	Navigate to http://help.sap.com/businessobjects and on the "SAP BusinessObjects Overview" side panel click **All Products**. You can access the most up-to-date documentation covering all SAP BusinessObjects products and their deployment at the SAP Help Portal. You can download PDF versions or installable HTML libraries. Certain guides are stored on the SAP Service Marketplace and are not available from the SAP Help Portal. These guides are listed on the Help Portal accompanied by a link to the SAP Service Marketplace. Customers with a maintenance agreement have an authorized user ID to access this site. To obtain an ID, contact your customer support representative.
SAP Service Marketplace	http://service.sap.com/bosap-support > Documentation • Installation guides: https://service.sap.com/bosap-instguides • Release notes: http://service.sap.com/releasenotes The SAP Service Marketplace stores certain installation guides, upgrade and migration guides, deployment guides, release notes and Supported Platforms documents. Customers with a maintenance agreement have an authorized user ID to access this site. Contact your customer support representative to obtain an ID. If you are redirected to the SAP Service Marketplace from the SAP Help Portal, use the menu in the navigation pane on the left to locate the category containing the documentation you want to access.
Docupedia	https://cw.sdn.sap.com/cw/community/docupedia Docupedia provides additional documentation resources, a collaborative authoring environment, and an interactive feedback channel.
Developer resources	https://boc.sdn.sap.com/ https://www.sdn.sap.com/irj/sdn/businessobjects-sdklibrary

Information Resource	Location
SAP BusinessObjects articles on the SAP Community Network	https://www.sdn.sap.com/irj/boc/businessobjects-articles These articles were formerly known as technical papers.
Notes	https://service.sap.com/notes These notes were formerly known as Knowledge Base articles.
Forums on the SAP Community Network	https://www.sdn.sap.com/irj/scn/forums
Training	http://www.sap.com/services/education From traditional classroom learning to targeted e-learning seminars, we can offer a training package to suit your learning needs and preferred learning style.
Online customer support	http://service.sap.com/bosap-support The SAP Support Portal contains information about Customer Support programs and services. It also has links to a wide range of technical information and downloads. Customers with a maintenance agreement have an authorized user ID to access this site. To obtain an ID, contact your customer support representative.
Consulting	http://www.sap.com/services/bysubject/businessobjectsconsulting Consultants can accompany you from the initial analysis stage to the delivery of your deployment project. Expertise is available in topics such as relational and multidimensional databases, connectivity, database design tools, and customized embedding technology.

Index

A

adding
    Users and Groups 25
    Web Parts 16
authentication modes
    Enterprise 19
    LDAP 19
    Windows AD 19

B

base SharePoint application
    Reverse Proxy 33
BusinessObjects template 13

C

configure
    Integration option for Microsoft
        SharePoint software 7
    web.config tags 7
configuring
    Web Parts 15
connecting
    Web Parts 16
considerations
    Crystal Report 37

E

exporting
    reports 37
extended website 33
extending web application
    LDAP 24

I

Integration option for Microsoft
    SharePoint software
    template configuration file 7
ISA 2006 31

L

LDAP
    extending web application 24
LDAP authentication 23

P

parameter prompts 35
parameter settings 35
processing reports 35

R

recommendations
    scheduling and scaling 36
Reverse Proxy 31

S

Secure Socket Layer 26
Single Sign-On 19

V

View on demand 26

W

Web Parts
    addition 16
    configuration 15
    connection 16
web.config tags
    AppSetting Configurations 7
    Crystal Viewer 7
    Document Viewer 7
    Infoview App Settings 7
    Infoview Logon Page 7
    Session State 7
Windows AD SSO 21