PUBLIC

SAP BusinessObjects Business Intelligence Platform

Document Version: 4.3 – 2022-12-07

Integration Option for Microsoft SharePoint Software Installation and Administration Guide

THE BEST RUN SAP

Content

1 Document History

Version	Date	Description
SAP BusinessObjects Business Intelligence Platform 4.3	June 2020	For Integration Option for Microsoft SharePoint Content specific webparts are depreciated. The following viewer usage is not supported. • Crystal report Viewer • Xcelsius Viewer Web Part • Analytical Report viewer

2 Who should read this guide

This information is intended for base administrators, Microsoft SharePoint administrators, and SAP administrators.

This guide describes how to install and to configure the SAP BusinessObjects integration option for Microsoft SharePoint software in a Business Intelligence (BI) platform deployment.

Administrators installing integration option for SharePoint should have:

- Familiarity with SharePoint 2016, SharePoint 2013, SharePoint Server 2010, SharePoint Foundation 2010, Windows SharePoint Services, Office SharePoint Portal Server 2007
- A working knowledge of SAP Crystal Reports and of the BI platform

For information about using the integration option for SharePoint software after it is installed and configured, see the *SAP BusinessObjects Integration Option for SharePoint Software Getting Started Guide* or the Integration Option for SharePoint Help.

3 Overview of the integration option for SharePoint

The integration option for SharePoint software enables Business Intelligence (BI) solutions to work with the SharePoint software. The integration option is available as a free download.

Administrators deploy the integration option for SharePoint to a site and then use the Team Site template to create a dedicated site for accessing BI content.

The integration option for SharePoint provides a gallery of SAP BusinessObjects web parts, that users with administrative rights can configure for SharePoint sites. In this way, any SharePoint site can be enabled to access and to manage BI content objects, including Crystal reports, Web Intelligence documents, publications, Xcelsius reports, Advanced Analysis documents, PDF documents, Microsoft Excel spreadsheets, Microsoft Word files, program files, object packages, and other reports.

When there is an existing site available with the deprecated webparts, the expected behavior is:

1. The deprecated webparts are listed in the Webparts gallery of an existing site (the site created before upgrading from BI 4.2 to BI 4.3). If you use the deprecated webparts in the site, errors/exceptions are seen.
2. If an existing site has deprecated webparts, after an upgrade, the webparts will not function and throw errors when the site is opened for viewing.

It is recommended to create a new site after an upgrade from BI 4.2 to BI 4.3.

> ℹ Note
>
> You can now access any report in the Integration of Microsoft sharepoint (IOMS) document viewer.
>
> For Integration Option for Microsoft SharePoint, certain content specific webparts are deprecated. The deprecated viewers are:
>
> - IOMS-Analytical Report Viewer
> - IOMS-Crystal Report Viewer
> - IOMS-Xcelsius Viewer

4 Planning

4.1 Installation requirements

Before installing the integration option for SharePoint software, confirm that the SharePoint server meets the system requirements and that the SharePoint installation meets prerequisites.

The SharePoint server must meet all SharePoint requirements in additional to the following system requirements:

System requirement	SharePoint 2016 requirement	SharePoint 2013 requirement	SharePoint Server 2010 requirement	Microsoft Office SharePoint Server (MOSS) 2007 requirement
Operating system	• Windows Server 2012 or Windows Server 2016, with Microsoft Internet Information Services (IIS) 8	• Windows Server 2012, with Microsoft Internet Information Services (IIS) 8 • Windows 2008 Server R2 SP1, with IIS 7.5	Windows 2008	64 bit
Processor	Two dual-core 2.8 GHz	Two dual-core 2.8 GHz	Two dual-core 2.8 GHz	Two dual-core 2.8 GHz
RAM	Minimum: 8 GB Recommended: 16 GB	8 GB	8 GB	Minimum: 3 GB Recommended: 4 GB
Minimum disk space	1.3 GB	1.3 GB	1.3 GB	1.3 GB
Free space required for installation with all language packs	1.4 GB	1.4 GB	1.4 GB	1.4 GB

> **i Note**
>
> SharePoint 2016 and SharePoint 2013 supports IIS 8 (the default version for Windows Server 2012) and IIS 7.5 (the default version for Windows 2008 Server R2 SP1).

The SharePoint installation must meet the following prerequisites:

Prerequisite	Requirement
Business Intelligence (BI) platform version, installed and configured	4.1 or later
SharePoint installed and configured	SharePoint 2016, SharePoint 2013, SharePoint Server 2010, SharePoint Foundation 2010, or Office SharePoint Server 2007
Administrator access rights	Granted as needed
Microsoft .NET version, installed	3.5 or later
System reboot	Suppressed

If a prerequisite is not met and you attempt to install the integration option for SharePoint, a *Prerequisite check* dialog box appears, indicating which prerequisites still need to be met. You must meet all prerequisites before the installation will continue.

This document does not include detailed system requirements for the BI platform or for SharePoint. For more information about requirements, see the *Supported Platforms* document on the SAP Support Portal. For a detailed list of supported operating systems and detailed hardware requirements, see the *SAP BusinessObjects Enterprise XI 4.0 Platform Availability Matrix* document. For additional information about the deployment, see the *Integration Option for SharePoint Software Release Notes*.

4.2 Installation steps

Installing the integration option for SharePoint software involves two general steps—running the installation and configuring the software.

You start the installation, and the installation program installs the web part package that you use to access and to manage Business Intelligence (BI) platform content through the Central Management Server (CMS). The web part package is a part of the Intelligence tier in the BI platform framework.

The installation adds the following web parts to the `Home Gallery` folder on the SharePoint deployment:

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

The installation does not add icons or shortcuts to the *Start* menu.

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

4.3 Installation methods

You can install the integration option for SharePoint software with the installation wizard or at the command line.

Use the installation wizard if you want to be prompted for installation options.

Use the command line to run either a silent or quiet-mode installation. Both types of installation use a response file. For a silent installation, you specify switch parameters and installation-option parameters at the command line or in a response file. (You can also use the silent installation command in scripts.) For a quiet-mode installation, you specify installation-option parameters at the command line or in a response file.

5 Installation

5.1 Response files

A response file is an ASCII text file that stores installation options in key-value format. You can modify response files in a text editor.

A silent installation uses a response file and the command line. The response file specifies switch parameters and installation-option parameters. For example, you might use a response file to set up a cluster or to create a development or test environment with standardized options.

When you need to override an installation option in a response file, enter that option at the command line. Installation options entered at the command line take precedence over options in a response file. Installation options have the following three levels of priority:

1. Options entered at the command line override the response file and the default value for options.
2. Options configured in a response file override the default value for options. Response-file values are used when no options are entered at the command line.
3. The default value for options is used when no options are entered at the command line or configured in a response file.

For example, the following command reads installation options from the `C:\response.ini` file but overrides the response-file value for the installation destination folder:

```
setup.exe
             -r
             C:\response.ini
            <InstallDir>="C:\Program Files (x86)\SAP BusinessObjects\SAP
BusinessObjects Enterprise XI
                4.0\"
```

If an unexpected condition is encountered while reading a response file, a message is written to the installation log file, and the installation program stops. Installation activity, warning messages, and error messages are written to the installation log file in the `<BOEInstallDir>\InstallData\logs\<date>\InstallDU<component>.log` folder.

> → Tip
>
> If the `<BOEInstallDir>` folder does not exist when the installation program stops, look for a file named `setupengine.log` in a timestamp folder in the temporary folder specified by the system `TEMP` environment variable.

Related Information

Verifying the installation [page 18]

5.1.1 Sample response file

```
### Installation directory installdir=C:\Program Files (x86)\SAP BusinessObjects\
\\\\\\\\
### #property.InstalledState.description# installedstate=true
### The URL to the Web Server that hosts Java InfoView (e.g., <http://
InfoviewServer/>)
javaopendocinfo= [http://<YourEnterpriseServer>:8080/BOE]
### Remote CMS administrator name remotecmsadminname=Administrator
### Remote CMS administrator password remotecmsadminpassword=Password1
### Remote CMS name remotecmsname=<YourEntepriseServer>
### Remote CMS port remotecmsport=6400
### Selected iPoint Virtual Server selectedipointvserver=http://
<YourIpointServer>:32843 http://<YourIpointServer>:43652 http://
<YourIpointServer>:80 http://<YourIpointServer>:80
### #property.SelectedIPointVServerAppPool.description#
selectedipointvserverapppool="SharePoint Web Services" "SharePoint Web Services
Root" "SharePoint Central Administration v4" "SharePoint Central Administration
v4" "Default Web Site" "DefaultAppPool" "SharePoint - 80" "SharePoint - 80"
### #property.SelectedIPointVServerInetPort.description#
selectedipointvserverinetport=%SystemDrive%
\inetpub\wwwroot\wss\VirtualDirectories\32843 %SystemDrive%
\inetpub\wwwroot\wss\VirtualDirectories\43652 %SystemDrive%
\inetpub\wwwroot\wss\VirtualDirectories\80 %SystemDrive%
\inetpub\wwwroot\wss\VirtualDirectories\80
### Selected iPoint Virtual Server Meta Number
selectedipointvservermetanum=2 672319142 1 1768581603 ### Selected iPoint
Virtual Server selectedipointvservername="SharePoint Web Services" "SharePoint
Central Administration v4" "Default Web Site" "SharePoint - 80"
### #property.SelectedLanguagePack.description#
selectedlanguagepacks=en
### UI Setup Language setupuilanguage=en
### Available features
### ------------------
### root
### IPoint.IPointRoot features=IPoint.IPointRoot,root
```

5.2 Installing with the wizard

The installation wizard prompts you to enter parameters and installation options.

Before starting the wizard, install the following tools:

- .NET Framework 3.5 or later
- IIS 7 or later

1. On the SAP Support Portal, in the *Software Downloads* area, locate and download `IPOINT03_0-20008227.exe`.
2. Double-click the `setup.exe` file.
3. When prompted, click *Run* in the installation wizard.
4. Select the installation language, and click *OK*.

   The *Prerequisite checking* dialog box appears, listing prerequisites that are not met. If a prerequisite was not met, you can click it to identify how to meet it.
5. Click *Next*.

6. On the welcome page, click *Next*.
7. On the *License Agreement* page, select *I accept the License Agreement*, and click *Next*.
8. On the *Select Language Packs* page, select one or more languages to install or select *All Languages* to install all available language packs, and click *Next*.

   The operating system language is automatically selected. You cannot remove English language support because it is the default language when a problem is detected with another language. Carefully consider which languages to install for your organization. If, at a later date, your organization needs different language packs, you can add or remove languages then, without uninstalling and reinstalling the integration option for SharePoint software.
9. On the *Configure destination folder* page, select the check box for the folder in which to install the software, and click *Next*.
10. On the *Deployment Options* page, select the server URL to deploy the integration option for SharePoint to, and click *Next*.
    For example, the server URL might be `http://<SharepointServerName>/`.

    Do not configure multiple SharePoint sites with the same URL (even with different protocols) on the same machine. It is possible to enter the URLs, but the installation will fail. For example, do not create one SharePoint site called “http://my_site” and another site “https://my_site” (same name but encrypted) on one machine.
11. (Optional) If the site will need to view Web Intelligence documents in SharePoint 2016 or SharePoint 2013, on the *Web Intelligence Gateway Configuration* page, enter a port number on which to create an IIS site called "WebIntelligence Gateway," and click *Next*.

    The IIS site created on this port is required for Web Intelligence document viewing in SharePoint 2016 and SharePoint 2013.
12. On the *Existing CMS Deployment Information* page, enter the Central Management Server (CMS) name, CMS port, and CMS user credentials for the BI platform, and click *Next*.
13. On the *Configuration Settings* page, perform one of the following actions:

    - If your organization will need to view SAP BusinessObjects Analysis, edition for OLAP documents, select *Yes, I will view objects in BI launch pad*, enter the URL of the web server that hosts the BI launch pad, and click *Next*.
      For example, the web server URL might be `http://<ServerName>:<PortNumber>/BOE`.
    - To set up manual object viewing, select *No, I want to manually set up object viewing*, and click *Next*.
14. On the *Start Installation* page, click *Next* to start the installation.
15. When the wizard has finished installing the software, click *Finish*.

After the installation completes, you can configure the software.

Related Information

Verifying the installation [page 18]

5.2.1 Creating a response file from the installation wizard

When creating a response file with the installation wizard, passwords entered in the wizard are written to the response file in plain text.

For example, the following command creates a response file at `C:\response.ini`:

```
setup.exe -w C:\response.ini
```

Run the installation program with the `-w <response-file>` parameter, and use the installation wizard to select installation options.

After the wizard completes, the installation program closes and the response file is created.

5.3 Silent installation

Run a silent installation from the command line, using switch parameters and installation-option parameters. You can specify the parameters at the command line or in a response file.

This type of installation is particularly useful when you need to perform multiple installations or do not want to interrupt people who are using machines on your system. You can also use the silent installation command in scripts. For example, organizations that use scripts to install software can add the silent installation command to those scripts.

After the installation completes, you can configure the software.

Related Information

Response files [page 10]
Verifying the installation [page 18]

5.3.1 Switch parameters

You can use switch parameters instead of using a response file to configure a silent installation.

Switch parameter	Description	Example
`-w <FileName>`	Writes a response file to `<FileName>` that lists options selected by the installation program	`setup.exe -w "C:\response.ini"`

Switch parameter	Description	Example
`-r <FileName>`	Reads installation options from a response file named `<FileName>`	`setup.exe -r "C:\response.ini"`
`-q`	Runs the installation program in quiet mode with no console output or prompting. If an issue is encountered, the installation program writes a message in the installation log file and then ends. Always use this parameter in combination with the `-r <FileName>` switch parameter.	`setup.exe -q -r "C:\response.ini"`

5.3.2 Installation-option parameters

Parameter	Description
`SetupUILanguage`	Language displayed in the installation program. Replace `<code>` with one of the following language codes: • Czech: CS • Danish: DA • Dutch: NL • English: EN • Finnish: FI • French: FR • German: DE • Hungarian: HU • Italian: IT • Japanese: JA • Korean: KO • Norwegian Bokmal: NB • Polish: PL • Portuguese: PT • Russian: RU • Simplified Chinese: zh_CN • Slovak: SK • Spanish: ES • Swedish: SV • Thai: TH • Traditional Chinese: zh_TW • Turkish: TR If you do not enter this parameter, the language selection page appears at the beginning of the installation, even if you specified parameters for a no-prompt installation.
`InstallDir`	Folder in which to put the installation program
`RemoteCMSPort`	Remote Central Management Server (CMS) port number
`RemoteCMSAdmin`	User account for remote CMS administration
`SelectedIPointVServer`	SharePoint site where deployed—for example, `http://<site>:<port>` or `http://<site1>:<port>`

Parameter	Description
`SelectedLanguagePacks`	Language displayed in the integration option for SharePoint software. Replace `<code>` with one of the following language codes: - Czech: CS - Danish: DA - Dutch: NL - English: EN - French: FR - German: DE - Hungarian: HU - Italian: IT - Japanese: JA - Korean: KO - Norwegian Bokmal: NB - Polish: PL - Portuguese: PT - Russian: RU - Simplified Chinese: zh_CN - Slovak: SK - Spanish: ES - Swedish: SV - Thai: TH - Traditional Chinese: zh_TW - Turkish: TR The EN (English) language pack is selected by default. To install more than one language, separate the codes with a semicolon, use no spaces, and enclose all codes inside one set of quotation marks. In the following example, language support for English, Japanese, Simplified Chinese, and Thai will be installed: `SelectedLanguagePacks="en;ja;zh_CN;th"`
`SelectedIPointVServerAppPool`	Names of SharePoint sites for which virtual directories must be created in Internet Information Services (IIS) and in the application pool to which to associate a site's virtual directories

Parameter	Description
JavaOpenDocInfo	(Optional) URL for the Business Intelligence (BI) launch pad—for example, http://<YourEnterpriseServer>:8080/BOE. When this URL is specified, the OpenDocument link is automatically configured.
SelectedIPointVServerInetPort	Virtual folder location of the SharePoint site
SelectedIPointVServerMetaNum	Metabase ID of the deployed SharePoint site
SelectedIPointVServerName	Virtual folder location of the SharePoint site

5.4 Quiet-mode installation

You run a quiet-mode installation from the command line, using the he -q switch.

This method does not prompt you for installation option parameters; you must enter options at the command line or in a response file. Options not entered at the command line or provided in a response file are set to the default value.

The -q switch bypasses the installation wizard and performs the installation with no human input and no console output. For example, the following command uses default values for all installation options, except for the installation destination folder:

```
setup.exe
         -q
          InstallDir="C:\Program Files (x86)\SAP BusinessObjects\SAP
BusinessObjects Enterprise XI 4.0\"
```

Note that the installation destination folder is set to C:\SAP\SAP BusinessObjects Enterprise XI 4.0\ instead of the default C:\Program Files (X86)\SAP BusinessObjects folder.

If an unexpected condition is encountered, a message is written to the installation log file in the <BoeInstallDir>\InstallData\logs\<date>\InstallDU<component>.log folder, and the installation program ends. All installation activities, warning messages, and error messages are written to the log file.

If the <BoeInstallDir> folder is not created when the installation program ends, locate the file named setupengine.log file in a time-stamped folder, in the temporary folder that is specified by the system TEMP environment variable.

After the installation completes, you can configure the software.

Example

```
setup.exe -q SetupUILanguage="en" InstallDir="c:\IPoint"
SelectedLanguagePacks="zh_cn;zh_tw;en;hu;da;es;it;ko;de;nl;nb;pl;pt;ru;sk;th;tr;f
i;fr;cs;sv;ja" JavaOpenDocInfo="http://<YourEnterpriseServer>:8080/BOE"
SelectedIpointVServer="http://<YourIpointServer>:2662"
SelectedIPointVServerAppPool= "\\\"SharePoint Web Services\\\" \\\"SharePoint
Web Services Root\\\" \\\"SharePoint Central Administration v4\\\" \\
\"SharePoint Central Administration v4\\\" \\\"Default Web Site\\\" \\
\"DefaultAppPool\\\" \\\"SharePoint - 80\\\" \\\"SharePoint - 80\\\""
SelectedIPointVServerMetaNum="1934304204"
SelectedIPointVServerInetPort="C:\inetpub\wwwroot\wss\VirtualDirectories\2662 "
SelectedIPointVServerName="\\\"SharePoint Central Administration v4\\\""
RemoteCMSName="<YourEnterpriseServer>" cmsport=6400
RemoteCMSAdminName="administrator" RemoteCMSAminPassword="<CmsPassword>"
features="IPoint.IPointRoot,root"remote
```

Related Information

Response files [page 10]

Verifying the installation [page 18]

5.5 Verifying the installation

Verify that the `web.config` file includes the appropriate SAP BusinessObjects features to activate on the SharePoint site.

1. In the `web.config` template configuration file, confirm that Business Intelligence (BI) platform security values are correct.

   If the values are not correct, the following message may appear when users attempt to access BI content on the SharePoint site:

   ```
   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.
   ```
2. In the `web.config` file, confirm that the URL for the BI launch pad and the URL for the Central Management Server (CMS) are correct.
3. Confirm that the following web parts are available in the web part gallery:
   - IOMS-Advertisement
   - IOMS-Content Explorer
   - IOMS-Recent Searches
   - IOMS-Recently Viewed
   - IOMS-Display Search Results
4. Confirm that SAP BusinessObjects site features are activated on the SharePoint site.

Related Information

Response files [page 10]
Activating SAP BusinessObjects features on a SharePoint site [page 29]

5.6 To use ONE Installer

ONE Installer is a single installation package that supports multiple BI installation scenarios such as, fresh installation of a Service Package or Patch, any Patch to Patch update, or any Service Package to Patch update.

If you are new to SAP BusinessObjects BI Platform, then you can use ONE Installer package for fresh installation of the latest available Support Package or Patch version of the BI release.

For more information about ONE Installer, see the *Business Intelligence Platform Installation Guide for Unix* and the *Business Intelligence Platform Installation Guide for Windows*.

6 SharePoint configuration

When you first install the integration option for SharePoint software, you must configure or update options in SharePoint to optimize your deployment.

6.1 SharePoint web.config template configuration file

When creating a web site, SharePoint automatically creates a `web.config` template file that stores configuration parameters and the values you chose. Use the `web.config` file to enable logging and tracing, activate SSL for a SharePoint site, configure reverse proxy or LDAP for an extended web application, and so on.

The integration option for SharePoint software installation program creates a backup copy of the original `web.config` file (called `backup web.config`) in the installation folder and then updates the `web.config` file based on Business Intelligence (BI) platform system information you enter during the installation.

If you modify BI platform system information after the installation, you must modify the same information in the `web.config` file. For example, if you change where the BI platform Central Management Server (CMS) is located, you must update the `BusinessObjects Enterprise Central Management Server` key value in the `web.config` file to match the CMS location.

By default, the SharePoint site is hosted on port 80. The `web.config` file for SharePoint 2016, SharePoint 2013, and SharePoint 2010 is maintained on a different server than the `web.config` file for Microsoft SharePoint 2007, but the tags added by the integration option for SharePoint software installation are similar for all SharePoint versions.

Content object	Location of the web.config file
All content in SharePoint 2010 or earlier, including Web Intelligence documents	`C:\inetpub\wwwroot\wss\VirtualDirectories\80`, which is the standard root space of the SharePoint web server
Web Intelligence documents in SharePoint 2016 or SharePoint 2013 (The Web Intelligence Web Service must be deployed to a site.)	`C:\inetpub\wwwroot\WebIntelligenceGateway`

For information about general administrative tasks, see the SharePoint documentation.

6.1.1 Editable tags in the web.config file

As an administrator, you can edit the following tags in the `web.config` template configuration file to define how features behave in the integration option for SharePoint software.

You can edit the following tags in the document viewer:

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

You can edit the following tags in the CrystalReports viewer:

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

You can edit the following tags in the InfoViewAppSettings web part:

```
<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,resizabl
e=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/helppredir.aspx" />
</InfoViewAppActionMapping>
</configuration>
```

> ℹ Note
>
> BOE session timeout value must be greater than the IIS session timeout value.

6.1.2 Logging and tracing in the web.config file

Modify these values in the `web.config` file to enable logging and tracing for security and monitoring.

For a developer trace file, the `value` attribute of the `level` tag may contain one of the following values:

- `INFO`
- `DEBUG`
- `ERROR`

For an administrator log file, the `value` attribute of the `level` tag may contain one of the following values:

- `FATAL`
- `WARN`

If you want the `value` attribute of the `level` tag to have all possible values (including values for a developer trace file and an administrator log file), set `level value="ALL"/`. If you want the `value` attribute of the `level` tag to have specific values, add each `value` attribute individually.

Logging occurs only for certain actions, such as setting scheduling options for an object (for example, Enterprise and dynamic recipients for a publication), viewing an object's history, assigning categories to an object, sending an object to a BI Inbox, and so on.

The logging feature is implemented only in the software's Universal Repository Explorer (URE). URE is a custom control that is used to implement views on the *User actions* page of an SAP BusinessObjects site.

6.1.2.1 Enabling logging and tracing in the web.config file

To enable logging and tracing for security and monitoring, modify values in the `web.config` file.

Before enabling logging and tracing in the `web.config` file, install the following tools:

- .NET Framework 3.5 or later
- IIS 6.0 or later

Logging occurs only when you perform certain actions, such as setting scheduling options for an object (for example, Enterprise and dynamic recipients for a publication), viewing an object's history, assigning categories to an object, sending an object to a BI Inbox, and so on.

1. In the `web.config` file, add the following tag and attribute values to the `configSections` section:

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

2. Add the following tag and attribute values to the `appSettings` section of the `web.config` file:

```
<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 name specified in the `FileName` section of the `web.config` file, and add the following tags to the 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>
```

4. Save and close the `web.config` file.

6.1.3 Creating additional SharePoint sites

You can use a SharePoint template or an SAP BusinessObjects template to create additional SharePoint sites that can access Business Intelligence (BI) content.

Template	Description
SharePoint Team Site	Use to create a site and to add SAP BusinessObjects web parts to site pages.
SAP BusinessObjects Site Definition	Use to create a site for accessing and managing BI content.

6.1.3.1 SharePoint Team Site template

When using the SharePoint Team Site template to create sites, you must enable SAP BusinessObjects site features in SharePoint before users can access Business Intelligence (BI) content.

If you use the SAP BusinessObjects Site Definition template to create a SharePoint site, SAP BusinessObjects site features are automatically enabled. To manually enable site features, add the following items to the SharePoint Team Site template that you use to create SharePoint sites:

SAP BusinessObjects site feature	Description
SAP BusinessObjects Logon	(Required) Enable this feature to connect to the Central Management Server (CMS) in the BI platform. This site feature is mandatory because you must connect to the CMS in order to work with BI content.
SAP BusinessObjects Log Off	Enable this feature to log off from the CMS, which disconnects access to BI content.
SAP BusinessObjects Platform Action Pages	Enable this feature to perform actions on reports and objects—for example, setting object properties, scheduling, viewing history, assigning a category, sending, and so on.
SAP BusinessObjects Preferences Settings	Enable this feature to set preferences—for example, passwords, time zone and preferred viewing locale, date and time, Web Intelligence document preferences, Crystal report preferences, and so on. ℹ Note When you, or your administrator, change your password, you are logged out of all your current sessions. For limitations see the *SAP Business Intelligence Suite Release Restrictions* guide available on the SAP Help Portal.

Do not configure multiple SharePoint sites with the same URL (even with different protocols) on the same machine. It is possible to enter the URLs, but the integration option for SharePoint installation will fail. For example, do not create one SharePoint site called “http://my_site” and another site “https://my_site” (same name but encrypted) on one machine.

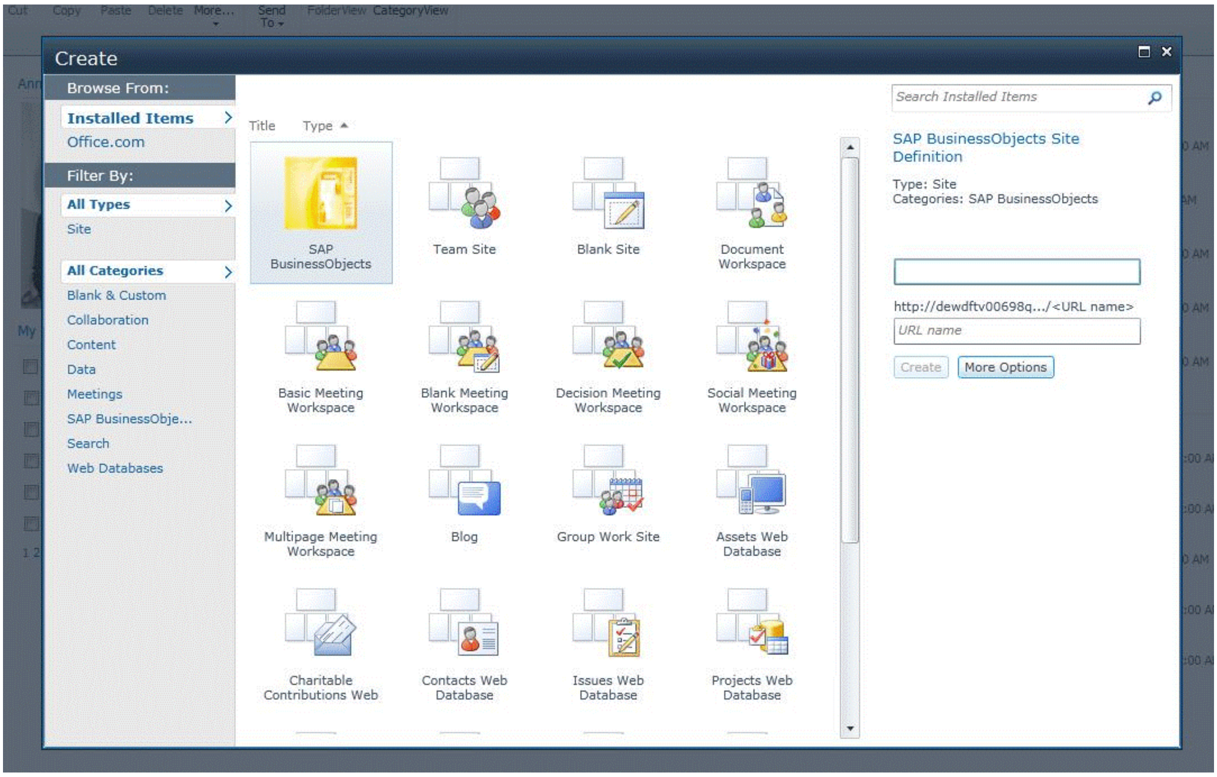
6.1.3.2 SAP BusinessObjects Site Definition template

Use the SAP BusinessObjects Site Definition template to create a ready-to-use site. The template handles all basic activities required to view, manage, and interact with Business Intelligence (BI) content in a SharePoint environment.

You must add web parts to a page on a SharePoint site before you can work with BI platform objects. Use the Site Definition template to add the following web parts to a page:

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

The Site Definition template appears in the SAP BusinessObjects category of templates available for creating a SharePoint site. After selecting the template, you can specify a unique URL for the site. Do not configure multiple SharePoint sites with the same URL (even with different protocols) on the same machine. It is possible to enter the URLs, but the integration option for SharePoint installation will fail. For example, do not create one SharePoint site called “http://my_site” and another site “https://my_site” (same name but encrypted) on one machine.



SharePoint 2010 platform (English example)

You can optionally add the viewer web part (provided by the integration option for SharePoint) to sites that you create with the template.

6.1.3.3 Activating SAP BusinessObjects features on a SharePoint site

You must activate SAP BusinessObjects features before they are available on a SharePoint site.

Before activating SAP BusinessObjects features on a SharePoint site, install the following tools:

- .NET Framework 3.5 or later
- IIS 7 or later

1. On the home page of the SharePoint site, select *Site Actions* > *Site Settings* > *Site Features*.
   The *Site Features* page appears, displaying the available SAP BusinessObjects features.
2. Select the *Activate* check box beside each feature that you want to enable.

Before you can access and work with Business Intelligence (BI) content, you must add web parts to pages on the SharePoint site.

6.1.4 Activating SSL for a SharePoint site

To configure Secure Sockets Layer (SSL) for a SharePoint site, modify values in the `web.config` file.

Before configuring SSL for a SharePoint site, install the following tools:

- .NET Framework 3.5 or later
- IIS 6.0 or later

1. In the `web.config` file, in the `system.serviceModel` section, perform the following actions under `basicHttpBinding`:
    a. Delete the following tag and attribute values:

    ```
    <binding name="ServerGatewayHttpBinding" messageEncoding="Mtom"
    maxBufferSize="2147483647" maxReceivedMessageSize="2147483647">
    <readerQuotas maxDepth="2147483647" maxStringContentLength="2147483647"
    maxArrayLength="2147483647" maxBytesPerRead="2147483647"
    maxNameTableCharCount="2147483647"/>
    <security mode="TransportCredentialOnly">
    <transport clientCredentialType="Ntlm"/>
    </security>
    </binding>
    ```

    b. Add the following tag and attribute values:

    ```
    <binding name="ServerGatewayHttpsBinding" messageEncoding="Mtom"
    maxBufferSize="2147483647" maxReceivedMessageSize="2147483647">
    <readerQuotas maxDepth="2147483647" maxStringContentLength="2147483647"
    maxArrayLength="2147483647" maxBytesPerRead="2147483647"
    maxNameTableCharCount="2147483647"/>
    <security mode="Transport">
    <transport clientCredentialType="Ntlm"/>
    </security>
    </binding>
    ```

2. In the `behaviors` section, under `serviceBehaviors`, perform the following actions:
    a. Delete `<serviceMetadata httpGetEnabled="true" />`
    b. Insert `<serviceMetadata httpGetEnabled="true" httpsGetEnabled="true" />`
3. In the `services` section, perform the following actions:
    a. Delete the following text:

    ```
    <endpoint address="" binding="basicHttpBinding"
    bindingConfiguration="ServerGatewayHttpBinding"
    name="GatewaySOAP" bindingName=""
    contract="BusinessObjects.Sdk.Core.Server.Service.GatewayPort"
    bindingNamespace="urn:services-businessobjects-com:coresdk:wsgateway" />
    ```

    b. Insert the following text:

    ```
    <endpoint address="" binding="basicHttpBinding"
    bindingConfiguration="ServerGatewayHttpsBinding"
    name="GatewaySOAP" bindingName=""
    contract="BusinessObjects.Sdk.Core.Server.Service.GatewayPort"
    bindingNamespace="urn:services-businessobjects-com:coresdk:wsgateway" />
    ```

4. Save and close the `web.config` file.

6.2 Adding a web part to a page on a SharePoint site

You can modify the appearance and functionality of a web page on the SharePoint portal by adding web parts.

Before adding a web part to a SharePoint page, install the following tools:

- .NET Framework 3.5 or later
- IIS 7 or later

SharePoint 2016, SharePoint 2013, and SharePoint 2010 do not support Microsoft Internet Explorer (IE) 11. To edit web parts for SharePoint sites in IE 11, the sites must be displayed in Compatibility View in the browser. To turn on Compatibility View, with the SharePoint site open in IE 11, select ▶ *Page* ▶ *Compatibility View settings* ▶ *Add* ◀, and enter the SharePoint site URL.

1. In a browser, navigate to the page to add a web part to on the SharePoint portal.
2. In the *Site Actions* list, select *Edit Page*.
   The page reloads in edit mode.
3. Click *Add a Web Part*.

   The web parts available for SharePoint deployments are listed in the *SAP BusinessObjects* area.
4. In the list of web part galleries, select a web part to add, and click *Add*.

6.2.1 Connecting web parts

When you configure SAP BusinessObjects web parts on a SharePoint site page, you may need to connect the web parts before you can view and interact with Business Intelligence (BI) content.

Before connecting web parts, install the following tools:

- .NET Framework 3.5 or later
- IIS 7 or later

For example, you can connect multiple viewer web parts to the IOMS-Content Explorer web part.

SharePoint 2016, SharePoint 2013, and SharePoint 2010 do not support IE 11. To edit web parts for SharePoint sites in IE 11, the sites must be displayed in Compatibility View in the browser. To turn on Compatibility View, with the SharePoint site open in IE 11, select ▶ *Page* ▶ *Compatibility View settings* ▶ *Add* ◀, and enter the SharePoint site URL.

1. In SharePoint edit mode, click *edit* in the IOMS-Content Explorer web part.
2. Select ▶ *Connections* ▶ *Send Repository Explorer To* ◀.
   Web parts added to the SharePoint page are listed.
3. Click a web part to connect it to the IOMS-Content Explorer web part.

6.2.2 Adding the IOMS-Display Search Results web part to a blank site

You can search the Business Intelligence (BI) repository and the SharePoint repository, and display search results from both repositories on one site.

Before adding the IOMS-Display Search Results web part to a blank site, site collection must be configured, and you must install the following tools:

- .NET Framework 3.5 or later
- IIS 7 or later

SharePoint 2016, SharePoint 2013, and SharePoint 2010 do not support IE 11. To edit web parts for SharePoint sites in IE 11, the sites must be displayed in Compatibility View in the browser. To turn on Compatibility View, with the SharePoint site open in IE 11, select *Page* > *Compatibility View settings* > *Add* , and enter the SharePoint site URL.

1. Create a blank SharePoint site page.
   For example, create a page called `Bobjsrch.aspx`.
2. Add the *IOMS-Display Search Results* web part and the *Microsoft Search Core Results* web part to the page.
3. Select *Site Actions* > *Site Settings* , and click *Search settings* in the *Site Collection Administration* section.
4. In the *Site Collection Search Results Page* box, enter **`/SitePages/Bobjsrch.aspx`**
5. Perform a search on any web page on the site.

The page displays search results from both the BI and SharePoint repositories.

6.3 Enabling anonymous access on IIS for AnalyticalReporting

Before you can create or edit a Web Intelligence document on the SharePoint portal, you must enable anonymous access on IIS for AnalyicalReporting.

Before enabling anonymous access, install the following tools:

- .NET Framework 3.5 or later
- IIS 7 or later

Before you can view Web Intelligence documents in SharePoint 2016 or SharePoint 2013, you must deploy the Web Intelligence Web Service to a site. The service can be deployed during wizard installation of the integration option for SharePoint or manually deployed.

1. Select *Start* > *Control Panel* > *Administrative Tools* > *IIS Manager* .

   > → Tip
   >
   > You can also enter **`inetmgr`** at a command line.

2. In IIS Manager, select *Sites* > *SharePoint Site* `<port>` > *_layouts* > *AnalyticalReporting* .

3. In the *Features* view, double-click *Authentication*.
4. On the *Authentication* page, select *Anonymous Authentication*.
5. In the *Actions* pane, click *Enable*.

6.4 Installing a host header for SharePoint 2016, SharePoint 2013, or SharePoint 2010

Before installing a host header for SharePoint, ensure that all SharePoint prerequisites have been met, and install the following tools:

- .NET Framework 3.5 or later
- IIS 7 or later
- Microsoft SQL Server 2008
- SharePoint 2016, SharePoint 2013, or SharePoint Server 2010

1. In Server Manager, click ▶ *Roles* ▶ *Add Roles* ◢, and select the *DNS Server* check box in the *Select Server Roles* window of the Add Roles wizard.
2. Using the SharePoint Team Site template, create a top-level site for the default SharePoint web application on port 80.
3. In SharePoint Central Administration, create a web application for NT LAN Manager (NTLM) claim-based authentication:
    a. On the *Create New Web Application* page, beside *Authentication*, select *Classic Mode Authentication*.
    b. Beside *IIS Web Site*, select *Create a new IIS web site*, and enter **`sharepoint -<port>`** in the *Name* box.
    For example, enter **`sharepoint -19369`**

    `<port>` is the port where you are creating the web application.
    c. In the *Port* box, enter the same port number you entered in the previous step.
    For example, enter **`19369`**
    d. In the *Host Header* box, enter the host header name for the web application.
    For example, enter **`ioms.<HostHeader>.com`**

    The *Path* box displays
    `C:\inetpub\wwwroot\wss\VirtualDirectories\<HostHeader>:<port>`.
    e. If necessary, modify the path to the web application in the *Path* box.
    f. Beside *Security Configuration*, select *NTLM* under *Authentication provider*.
    g. If necessary, modify the URL to the web application in the *URL* box, but leave other options under *Authentication provider* set to the default values.

    Beside *Public URL*, the *URL* box displays `http://<HostHeader>:<port>`.

> **i Note**
>
> Do not configure multiple SharePoint sites with the same URL (even with different protocols) on the same computer. It is possible to enter the URLs, but the integration option for SharePoint software installation will fail. For example, do not create one SharePoint site called “http://my_site” and another site called “https://my_site” (the same name but encrypted).

h. Beside *Application Pool*, select *Create new application pool*.

   The *Application pool name* box displays **`SharePoint - <HostHeader>:<port>`**.

i. If necessary, modify the name of the application pool in the *Application pool name* box.

j. Under *Select a security account for this application pool*, select *Predefined*, select *Network Service* in the list, and click *OK*.

4. Using the Team Site template, create site collection:
   a. On the *Create Site Collection* page, enter a title and a description for site collection.
   b. Beside *Web Site Address*, select */* in the *URL* list.
   c. Beside *Template Selection*, select *Team Site* on the *Collaboration* tab.
   d. Beside *Primary Site Collection Administrator*, enter **`<SharepointMachine>\administrator`** in the *User name* box, and click *OK*.

      `<SharepointMachine>` is the name of the computer where SharePoint is installed.

   A *Top-Level Site Successfully Created* box appears, confirming that the new site was created successfully. You must configure the DNS server before you can access the site.
5. Configure the DNS server:
   a. In DNS Manager, under `<SharepointMachine>`, right-click *Forward Lookup Zones* and select *[new zone]*.

      `<SharepointMachine>` is the name of the computer where SharePoint is installed.
   b. Select *[primary zone]*, enter the host header name you entered for the web application in the *Zone name* box, and click *Next* until finished.
   c. In a text editor, open the `hosts` file on the SharePoint machine, and map the SharePoint machine's Internet Protocol (IP) address to the host header you entered for the web application.
   d. In the Windows Registry Editor, locate and open `HKLM\System\CurrentControlSet\Control\Lsa`, add *DWORD (32-bit) value* for *DisableLoopbackCheck* and set the value to **`1`**.
   e. In Internet Information Servers (IIS) Manager, right-click *Sharepoint - `<HostHeader>`:`<port>`* and select *Bindings*.
   f. In the *Site Bindings* dialog box, click *Edit*.
   g. In the *Edit Site Binding* dialog box, enter the SharePoint machine's IP version 4 (IPv4) address in the *IP address* box.
   h. Restart the SharePoint machine.
   i. Because a web site exists for `http://<HostHeader>:<port>`, disable the proxy server in the IE *Local Area Network (Settings)* dialog box.
6. Go to the `http://<HostHeader>:<port>` URL.
   The new site home page appears. SharePoint is ready for the integration option for SharePoint software installation.
7. Install the SAP BusinessObjects integration option for SharePoint software on the SharePoint machine.
   a. In the *SAP Integration for Microsoft SharePoint 4.1 setup* dialog box, select the *http://`<SharepointMachine>`:`<port>` [SharePoint - `<HostHeader>`:`<port>`]* check box.
   b. In a text editor, open the `hosts` file on the SharePoint machine, and add IP-host mapping for the BI platform machine.

      This ensures that the integration option for SharePoint software installation will set the Central Management Server (CMS) name and the OpenDocument base URL from the `hosts` file.
8. After installing the integration option for SharePoint software on the `http://<SharepointMachine>:<port>` IIS site, set up the SharePoint web application using the host header:

   a. In SharePoint Central Administration, select ▶ *System Settings* ▶ *Farm Management* ▶ *Manage farm solutions* ▶, and click `infoview.wsp`.
      The *Solutions Properties* page appears. Note that the integration option for SharePoint is not deployed to the `http://<HostHeader>:<port>` web application.
   b. Click *Deploy Solution* to deploy `infoview.wsp` to `http://<HostHeader>:<port>`.

      The *Deploy Solution* page appears.
   c. Beside *Deploy To*, select *http://*`<HostHeader>`*:*`<port>` in the *Choose a Web application to deploy this solution* list.

      The *Solutions Properties* page appears, showing that the integration option for SharePoint is deployed to the `http://<HostHeader>:<port>/; http://<SharepointMachine>:<port>/; http:<SharepointMachine>/` web application.
9. At the command line, enter the following command:

```
call "C:\Program Files\Common Files\Microsoft Shared\Web Server
Extensions\14\BIN\stsadm.exe" -o deploysolution -name
"InfoView.wsp" -allowgacdeployment -immediate -force -url http://
<HostHeader>:<port>
```

10. Go to `http://<HostHeader>:<port>`, and create a new SharePoint site:
   a. On the *New SharePoint site* page, enter a title and a description for the site.
   b. Beside *Web Site Address*, enter the URL to the new site in the *URL name* box.

      Do not configure multiple SharePoint sites with the same URL (even with different protocols) on the same machine. It is possible to enter the URLs, but the integration option for SharePoint software installation will fail. For example, do not create one SharePoint site called “http://my_site” and another site “https://my_site” (same name but encrypted) on one machine.
   c. Beside *Template Selection*, select *SAP BusinessObjects Site Definition* on the *SAP BusinessObjects* tab, and click *Create*.
      The site home page is created.
11. On the client machine, open the `host` file, and add the following text:

    `[<SHAREPOINT machine IPv4 ip> <HostHeader>]`

When opening the `http://<HostHeader>` site in a browser, you will be prompted to enter SharePoint administrator credentials.

6.5 Installing a server farm for SharePoint 2016, SharePoint 2013, or SharePoint 2010

Before installing a server farm for SharePoint, ensure that all SharePoint prerequisites have been met. Write down or otherwise note the physical architecture, logical architecture, specifications, account user names and passwords, license keys, and so on that you will need. In addition, install the following tools:

- .NET Framework 3.5 or later
- IIS 7 or later
- SharePoint 2016, SharePoint 2013, or SharePoint Server 2010

1. Run the installation file for the integration option for SharePoint software.

2. In the SharePoint installation wizard, under *Install*, click *Install software prerequisites*.
   The Microsoft SharePoint Products Preparation Tool *Welcome* window appears, listing the prerequisites that will be installed.
3. Review the list of the prerequisites, and remove any installed items.
   For example, if you do not uninstall Windows Identity Foundation before installing prerequisites, the installation wizard automatically terminates.
4. In the *Welcome* window, click *Next* to start installing prerequisites.

   If any prerequisites fail to install, you must correct the issue before continuing the installation, even if the wizard allows you to continue.
5. In the *License Terms for software products* window, accept the terms of the license agreement, and click *Next*.
   A status bar appears, showing the progress of prerequisite installation. After all prerequisites are installed, the *Installation Complete* window appears. Prerequisites not installed have `(no action taken)` appended to the name.
6. Click *Finish* to close the Microsoft SharePoint Products Preparation Tool wizard and to start the Microsoft SharePoint Server installation wizard.
7. In the *Enter your Product Key* window, enter your license key in the box, and click *Continue*.
8. In the *Read the Microsoft Software License Terms* window, select the check box to accept the terms, and click *Continue*.
9. In the *Choose the installation you want* window, click *Server Farm*.
10. In the *Server Type* window, select *Complete - Install all components. Can add servers to form a SharePoint farm*, and click *Install Now*.

An *Installation Progress* window appears, showing the progress of the installation.

6.5.1 Adding servers to a server farm

After installing a server farm, perform this task to add servers to it.

Before adding servers, write down or otherwise note the physical architecture, logical architecture, specifications, account user names and passwords, license keys, and so on that you will need. In addition, install the following tools:

- .NET Framework 3.5 or later
- IIS 7 or later

1. On the server that will handle SharePoint Central Administration, start the SharePoint Products Configuration wizard.
2. In the *Run Configuration Wizard* window, select the check box, and click *Close*.
3. In the *Welcome to SharePoint Products* window, click *Next*.

   As part of server farm configuration, some services may need to be stopped or reset and restarted.
4. If a message about stopping and restarting services appears, click *Yes* to continue.
5. In the *Connect to a server farm* window, select *Connect to an existing server farm*, and click *Next*.
6. In the *Specify Configuration Database Settings* window, perform the following actions:
   a. In the *Database server* box, enter the database server name.
   b. In the *Database name* box, enter the database name.

    c. In the *Username* box, enter the database-access-account user name.
    d. In the *Password* box, enter the database-access-account password, and click *Next*.

7. In the *Specify Farm Security Settings* window, enter the passphrase in the *Passphrase* box and in the *Confirm passphrase* box, and click *Next*.

   The SharePoint passphrase secures farm configuration data and is required for adding servers to the farm.
8. In the *Configure SharePoint Central Administration Web Application* window, enter a port number in the *Specify port number* box, or accept the random number assigned by the wizard.
9. Under *Configure Security Settings*, select *NTLM* or *Negotiate (Kerberos)*, and click *Next*.
10. In the *Completing the SharePoint Products Configuration Wizard* window, review the configuration settings that will be applied, make corrections as needed, and click *Next*.
    The *Configuring SharePoint Products* window appears, showing the progress of the configuration. After the configuration completes, a *Configuration Successful* window appears.
11. Click *Finish*.
12. In SharePoint Central Administration, on the *Configure your SharePoint farm* page, click *Start the Wizard* to open the Farm Configuration Wizard.

    The wizard configuration uses the farm account for all service applications. To change the application pool and service accounts under which specific service applications run, create managed accounts and then make changes in the *Services on Server* or *Service Applications* window.
13. When the configuration completes, in the window that appears, click *Finish*.

6.6 Configuring SSL on IIS 6

Before configuring Secure Sockets Layer (SSL) on IIS, install the following tools:

- .NET Framework 3.5 or later
- IIS 6

1. Log on to SharePoint Central Administration where IIS is running.
2. On the *Application Management* tab, click the *Create or extend Web Application* link under *SharePoint Web Application Management*.
3. In the *Web Application* list, select *Extend an Existing Web Application*, and select the web application to configure SSL for.
4. In the *Create New IIS website* box, enter a web site name.
5. In the *Port* box, enter the default SSL port number.
6. Select the *Use SSL* check box.
7. Confirm that the correct URL is displayed in the *URL* box.
8. In the *Zone* list, select *Custom*, and click *OK*.
9. On the IIS web site, select the site you created, and click *Properties*.

   This web site should be on port 80. Only one web site can run on port 80. If another web site is already on port 80, change the new web site to another port.

   The *Properties* dialog box appears.
10. On the *Directory Security* tab, click *Server certificates*, and perform one of the following actions:

    - If a server certificate already exists on the system, select *Assign an existing certificate*, and follow the wizard instructions.
    - If no certificate exists, download the certificate creation utility, and install the certificate.
11. Under *Secure Communications* on the *Directory Security* tab, click *Edit*.
12. Select *Require SSL* and *128 bit encryption* to access the site using https.

    If these options are not available, the site can be accessed with either http or https.
13. If there are no client certificates, select *Ignore client certificates*.
14. Click *OK*, and click *Apply*.
15. On the *SharePoint 3.0 Central Administration* page, on the *Operations* tab, click the *Alternate Access Mappings* link.
16. In the *Alternate Access Mapping Collection* list, select the collection to map SSL for.

    Ensure that a public URL is specified for the custom zone. If a public URL is not specified, you must add it to the *Custom* zone.
17. In a browser, enter the SSL URL.

You can navigate through all pages and web parts on the site. Ensure that the URL does not change from "https" to "http" as you navigate.

6.7 Configuring SSL on IIS 8 or 7.5

IIS 8 is the web application server that supports SharePoint 2016 and SharePoint 2013, and IIS 7.5 is the web application server that supports SharePoint Server 2010.

Before configuring SSL on IIS 8 or 7.5, install the following tools:

- .NET Framework 3.5 or later
- IIS 8 or 7.5

1. Log on to SharePoint Central Administration where IIS is running, and enter **`inetmgr`** at the command line..
2. In the window that appears, select the root server node.
   The features list appears in the right pane. If the features list does not appear, right-click the root node and select *Switch to Features View*.
3. Double-click *Server Certificates*.
4. In the *Actions* pane of the *Server Certificates* window, click *Create Self-Signed Certificate*.

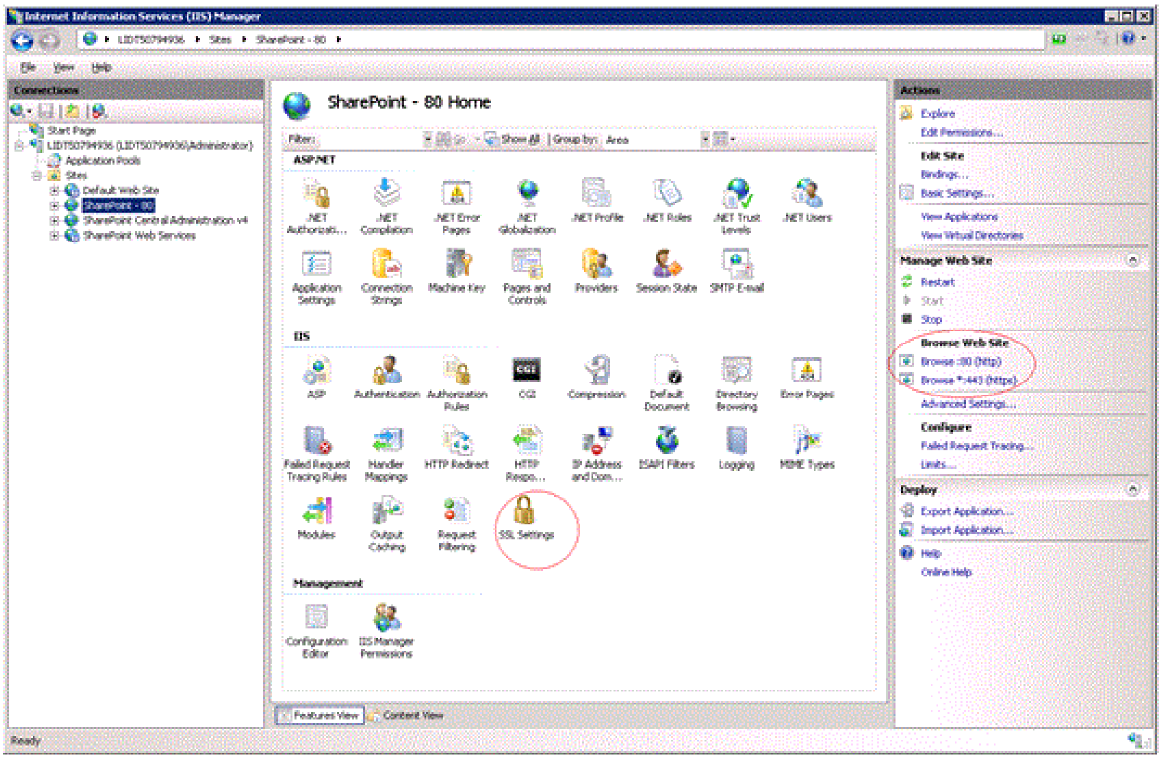
   The *Actions* pane is on the right side of the window.
5. In the *Create Self-Signed Certificate* window, enter a name for the certificate, and click *OK*.

   The certificate name is usually the name of the machine where IIS is running.
6. Under *Sites* in the *Connections* pane, right-click the SharePoint site to enable SSL for and select *Edit Bindings*.

   The *Connections* pane is located on the left side of the *Server Certificates* window.
7. In the *Site Bindings* window, click *Add*.
8. In the *Add Site Binding* window, for *Type*, select *http*.

9. Set the value of *Default port* to **443**
10. Select the certificate you added from the *SSL Certificate* box, and click *OK*.
    The certificate entry is added to the *Site Bindings* window.
11. Click *Close*.

    When you select the site (on the left side of the *IIS Manager* window), the *Browse Web Site* area (▶ *Actions* ▶ *Manage Web Site* ▶ *Browse Web Site* ▶) on the right side of the window displays the new binding value as *Browse *:443 (http)*.



IIS Manager window (English example)

12. Double-click *SSL Settings* in the IIS features list in the middle of the window.
13. Select the *Require SSL* check box, and click *Apply* in the *Actions* pane.
    The selected site is configured with the SSL URL and the default port.
14. Enter the site's URL (for example, `http://lidt50794936`), and click the *Continue to this website (not recommended)* link.

    After logging on, you can enter your regular SharePoint credentials to log on to the site.

    The following message appears:

    ```
    You may be trying to access this site from a secured browser on the server.
    Please enable scripts and re-load this page.
    ```
15. To prevent the message from appearing again, add the http URL to the trusted sites for your browser:
    a. In the browser, select ▶ *Tools* ▶ *Internet Options* ▶.
    b. On the *Security* tab, click *Trusted sites*, and click *Sites*.
    c. In the *Trusted sites* dialog box, in the *Add this website to the zone* box, enter the web site URL, and click *Add*.
16. Click *Close*, and click *OK*.
    When you access an SSL-enabled site, the message will not appear.

If you are accessing the SharePoint SSL URL from a remote client machine, you must export the certificate to the server and then import it to the remote client machine.

6.8 Configuring ISA Server 2006 for reverse proxy

Before configuring Internet Security and Acceleration (ISA) Server 2006 for reverse proxy, install the following tools:

- Microsoft ISA Server 2006 using Windows credentials
- .NET Framework 3.5 or later
- IIS 7 or later

1. Start ISA 2006.
2. Right-click *Firewall Policy* and select ▶ *New* ▶ *SharePoint Site Publishing Rule* ▶.
   The *Welcome to the SharePoint Publishing Rule Wizard* page appears.
3. In the *SharePoint publishing rule name* box, enter the publishing rule name, and click *Next*.
   The *Publishing Type* page appears.
4. Select *Publish a single Web site or load balancer*, and click *Next*.
   The *Server Connection Security* page appears.
5. Select *Use non-secured connections to connect the published Web server or server farm*, and click *Next*.
   The *Internal Publishing Details* page appears.
6. In the *Internal Site name* box, enter the internal site name.

   The internal site name is the system that Microsoft Office SharePoint Server (MOSS) is running on.
7. Select *Use a computer name or IP address to connect to the published server*, enter the system name or IP address in the *Computer name or IP address* box, and click *Next*.
   The *Public Name Details* page appears.
8. In the *Accept Request for* list, select *Any domain name*, and click *Next*.
   The *Select Web Listener* page appears.
9. Click *New*.
   The *Welcome to the New Web Listener Wizard* page appears.
10. Enter the web listener name, and click *Next*.
    The *Client Connection Security* page appears.
11. Select *Do not require SSL secured connections with clients*, and click *Next*.
    The *Web Listener IP Addresses* page appears.
12. Select *External*, *Internal*, and *Local Host*, and click *Next*.
13. On the *Authentication Settings* page, select *No Authentication*, and click *Finish*.
14. Select the newly created listener, and select ▶ *Properties* ▶ *Authentication* ▶.
15. Click *Advanced*, and select *Require all users to authenticate* and *Allow Client Connections over Http*.
16. On the *Authentication Delegation* page, select *No delegation, and client cannot authenticate directly* in the list, and click *Next*.
17. On the *Alternate Access Mapping Configuration* page, select one of the following options:
    - *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*.
19. On the *Completing the New SharePoint Publishing Rule Wizard* page, click *Finish*.
    The publishing rule is created.
20. Select the publishing rule, and click *Apply*.
21. Right-click the rule and select *Properties*.
22. On the *Listener* tab of the *Properties* dialog box, confirm that the correct port and protocol are displayed.

    By default, port 80 is used. You can change the port number on the *Connections* tab.
23. On the *Public Name* tab, select *Requests for the following Web sites* in the *This rule applies to* list, and enter the reverse proxy URL.
24. Beside *Path Names*, map the client path to the server path.
25. On the *To* tab, confirm that the correct name and IP address of the destination system are displayed.
26. On the *Bridging* tab, select *Redirect requests to HTTP port*, and enter the port on which the SharePoint extended web application is running.

    To point the reverse proxy to the extended web application URL, enter the port number of the extended web application. If you want the reverse proxy to point to the SharePoint base application, enter the port number of the base application.
27. Select the rule, and click *Apply*.

6.8.1 Configuring reverse proxy for the SharePoint base application

Before configuring reverse proxy for the SharePoint base application, configure Internet Security and Acceleration (ISA) Server for the integration option for SharePoint, and install the following tools:

- .NET Framework 3.5 or later
- IIS 7 or later

1. Log on to SharePoint Central Administration.
2. Click *Operations*, and click the *AlternateAccessmapping* link.
3. In the list, select the SharePoint base application.
4. Click the *Add Internal URL* link, and enter the reverse proxy URL.
5. In the *Zone* list, select *Default*.
6. In IIS, set *Authentication type* to *Basic*.

6.8.2 Extending an existing web application

Before extending an existing web application, install the following tools:

- .NET Framework 3.5 or later
- IIS 6 or later

1. Log on to SharePoint Central Administration.
2. On the *Application Management* tab, click the *create or extend web application* link.
3. In the *Web Application* list, select *Extend an Existing Web Application.*
4. Select the web application for which to configure a reverse proxy.
5. Enter the description, port, URL, and so on.
6. Select a zone (for example, *Internet*), and click *OK*.
7. On the SharePoint Central Administration site, on the *Operations* tab, click the *AlternateAccessMapping* link.
8. In the list, select the web application.
9. Click *Add Internal URL* link, and enter the reverse proxy URL.
10. In the *Zone* list, select the zone for the extended web application, and click *OK*.

An extended web site is created for the web application.

6.8.3 Configuring reverse proxy for the extended web application

Before modifying an extended web application's `web.config` file, install the following tools:

- .NET Framework 3.5 or later
- IIS 6 or later

1. Copy all `.dll` files and folders from the `bin` folder of the SharePoint base application to the `bin` folder of the extended web application.
2. Open the `web.config` file for the SharePoint base application, confirm that there is one `sessionState` entry, and comment out all other entries.

   The only `sessionState` entry should be `"sessionState mode = Inproc"/`.
3. In the extended web application, create a virtual folder 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 folders:
   - `InfoviewApp`
   - `InfoviewAppActions`
   - `PlatformServices`
   - `AnalyticalReporting`
   - `CrystalReports`
   - `Xcelsius`
5. Ensure that virtual folders in the extended web application point to the same application pool in the SharePoint base application.
6. Compare the SharePoint base application `web.config` file with the extended web application `web.config` file, and modify the extended application's `web.config` file to include any missing entries.

6.9 Configuring LDAP authentication

Before configuring Lightweight Directory Access Protocol (LDAP) authentication, install the following tools:

- MOSS 2007 or later and LDAP Server
- .NET Framework 3.5 or later
- IIS 7 or later

In addition, create groups and users in LDAP and create a SharePoint web application on MOSS 2007. (If MOSS 2007 and LDAP are on different systems, the two systems must be able to communicate with each other.)

1. Log on to SharePoint Central Administration.
2. On the *Application Management* tab, click the *Create or extend Web Application* link under *SharePoint Web Application Management*.
3. Click *Extend web application*.
4. Enter the port name, host name, and so on.
5. In the *Zone* list, select *Custom*, and click *Create*.

   The extended application is created.
6. On the *Application Management* tab, click the *Authentication Providers* link under *Application Security*.
7. On the *Authentication Providers* page, click the *Zone* link.
8. On the *Edit Authentication* page, select *Forms* as the authentication type.
9. In the *Membership Provider Name* box, enter the membership provider name.

   The LDAP membership provider name is specified in the `web.config` file.
10. In the *Role Manager Name* box, enter the role manager name.
11. For *Enable Client Integration*, select *No*.
12. Click *Save*.

    Authentication mode in the `web.config` file of the extended web application is renamed *Forms*.

After logging on to the SharePoint extended web application as a site administrator, you can perform all administrative tasks, such as adding and deleting users and user groups.

6.9.1 Configuring LDAP for the extended web application

Before modifying the `web.config` file of the extended web application, install the following tools:

- .NET Framework 3.5 or later
- IIS 7 or later

1. Log on to the IIS machine, and log on to SharePoint Central Administration.
2. In the `web.config` file, add the following lines between the `</system.web>` tag and the `<runtime>` tag:

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

3. Add the following lines between the `</authorization>` tag and the `<httpModules>` tag:

   ```
   <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>
   ```

   Values specified may differ, depending on how users were created in LDAP.
4. Open the `web.config` file of the extended web application, and add the following lines:

   ```
   <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. Open the `web.config` file of the SharePoint Central Administration site, and add the following lines between the `</authorization>` tag and the `<httpModules>` tag:

   ```
   <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, and log on to SharePoint Central Administration.
7. On the *Application Management* tab, click *Site Collection Administrators*.
8. Add any LDAP user as the primary administrator, and confirm that the user is identified.
9. Log on to the SharePoint site as the site administrator with LDAP user rights.

6.9.2 Adding users and groups to the extended web application

As the site administrator, you must add LDAP users to the extended web application before the users can log on.

Before you add users and groups to the extended web application, install the following tools:

- .NET Framework 3.5 or later
- IIS 7 or later

1. Log on to the extended web application as the site administrator.
2. Select ▶ *Site Settings* ▶ *People and Groups* ▶.
3. In the *Add the LDAP Groups or Users* box, add users or user groups:
   - To add a user, enter the user name.
   - To add a user group, use the following syntax: `<LdapRoleProviderName>:<GroupName>`

6.9.3 Logging on to the extended web application as an LDAP user

Before logging on to the SharePoint extended web application as an LDAP user, install the following tools:

- .NET Framework 3.5 or later
- IIS 7or later

In addition, enable LDAP authentication in the Central Management Server (CMS) in the Business Intelligence (BI) platform, and the LDAP user must be able to log on to the BI launch pad.

1. Log on to the IIS machine, and log on to SharePoint Central Administration.
2. Select the *Integrated Authentication* check box, and clear the *Anonymous logon* check box.
3. Compare the SharePoint base application's `web.config` file with the extended web application's `web.config` file, and modify the extended web application's `web.config` file to include any missing entries.
4. Convert the `InfoviewApp`, `InfoviewAppActions`, `PlatformServices`, and `AnalyticalReporting` folders to virtual folders.

5. Confirm that the virtual folders in the extended web application point to the same application pool in the SharePoint base application.
6. Copy the contents of the SharePoint base application's `SharePoint:<port>\<bin>` folder to the extended web application's `ExtendedApplication:<port>\<bin>` folder.
7. Create a virtual folder called `crystalreportviewers12` and point it to `C:\Program Files\BusinessObjects\common\4.0\crystalreportviewers12`.

6.10 Windows AD authentication

The Business Intelligence (BI) platform supports Active Directory (AD) authentication with the Windows security plug-in, which is included by default when the platform is installed on Windows.

Support for Windows AD authentication means that user and user group accounts in Microsoft AD can be used to authenticate with the BI platform. System administrators can map existing AD accounts, instead of setting up each user and group in the BI platform.

You use the Windows AD security plug-in to configure the following types of authentication:

- Windows AD with Kerberos
- Windows AD with NT LAN Manager (NTLM)

Windows AD authentication requires the following general steps:

1. Configure the required domain controller resources.
2. Prepare the host for Windows AD authentication.
3. Enable the AD security plug-in and map AD groups.
4. Choose an authentication method:
   - Windows AD with Kerberos
   - Windows AD with NTLM
5. (Optional) Set up single sign-on (SSO), using one of the following methods:
   - Kerberos SSO for Windows AD
   - NTLM SSO for Windows AD

6.10.1 Configuring Windows AD with Kerberos

Before configuring Windows AD with Kerberos, install the following tools:

- .NET Framework 3.5 or later
- IIS 7 or later

1. On the SharePoint portal, configure Windows AD authentication.

   For instructions, see the SharePoint documentation.
2. In the SharePoint software, create a web application, and select *Classic Mode Authentication*.
3. In the *Authentication provider* section, select *Negotiate (Kerberos)*.

4. In the Central Management Console (CMC) in the Business Intelligence (BI) platform, configure Windows AD authentication for Kerberos.

   For instructions, see the *SAP BusinessObjects Business Intelligence Platform Administrator Guide*.
5. In the BI launch pad, confirm that Windows AD authentication is correctly configured for the BI platform by logging on with the credentials of an authorized Windows AD user.
6. In the Windows AD domain controller for the SharePoint server and client machines, select *Trust this computer for delegation to any service (Kerberos only)*.
7. On the SharePoint server, in IIS manager, select the site where the integration option for SharePoint software is installed, and clear the *Enable Kernel Mode Authentication* check box.

   For example, select ▶ *SharePoint site* › *Authentication* › *Windows Authentication* › *Advanced Settings* ◀, and clear the *Enable Kernel Mode Authentication* check box under *Advanced Settings*.
8. In the following integration option for SharePoint files, set the value of `authentication.visible` to `true`:

   - `web.config` template configuration file at `C:\inetpub\wwwroot\wss\VirtualDirectories\80` (where `80` is the port where SharePoint is deployed)
   - InfoViewApp web part at `C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\Web Content\SharepointApp\InfoViewApp`
   - SharePoint platform services at `C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\Web Content\SharepointApp\PlatformServices`
   - OpenDocument files at `C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\Web Content\SharepointApp\OpenDocument`
9. In the integration option for SharePoint software, confirm that Windows AD Kerberos authentication is correctly configured by logging on with the credentials of an authorized Windows AD user.
10. For the *Client Browser* trusted site, select *Add SharePoint Fully Qualified Domain Name URL*.

    For example, if the browser is Internet Explorer, select ▶ *Tools* › *Internet Options* › *Security* › *Sites* ◀.
11. Select *SharePoint FQDN*, and click *Add*.

6.10.2 Configuring Windows AD with Kerberos SSO

Before configuring Windows AD with Kerberos SSO, install the following tools:

- .NET Framework 3.5 or later
- IIS 7 or later

1. In the integration option for SharePoint software, confirm that Windows AD authentication is correctly configured by logging on with the credentials of an authorized Windows AD user.
2. In Central Management Console (CMC) in the Business Intelligence (BI) platform, enable SSO.

   For instructions, search for "SSO" in the *SAP BusinessObjects Business Intelligence Platform Administrator Guide*.
3. In the following integration option for SharePoint files, set the value of `sso.enabled` to `true`, the value of `authentication.default` to `secWinAD`, and the value of `identity impersonate` to `true`:

   - InfoViewApp web part at `C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\Web Content\SharepointApp\InfoViewApp`

    - SharePoint platform services at `C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\Web Content\SharepointApp\PlatformServices`
    - OpenDocument files at `C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\Web Content\SharepointApp\OpenDocument`
4. On the SharePoint server, restart IIS.
5. On the client machine, confirm that Windows AD Kerberos SSO authentication is correctly configured by logging on to the client machine with the credentials of an authorized Windows AD user.
6. If the browser is Internet Explorer, select ▶ *Tools* ▶ *Internet Options* ◀, and perform the following actions:
    a. Click the *Security* tab, and click *Custom Level*.
    b. In the *Security Settings - Trust Sites Zone* dialog box, under *Settings*, locate *User Authentication*.
    c. Under *Logon*, select *Automatic logon with current user name and password*, click *OK*, and click *OK* again.

    If the browser is not Internet Explorer, skip this step.
7. On the client machine, access the URL of the machine hosting the integration option for SharePoint. The user should be logged on automatically to the software with Windows AD credentials.

Related Information

Troubleshooting Windows AD with SSO [page 50]

6.10.3 Configuring Windows AD with NTLM

When using IIS on the Windows operating system, you can configure NTLM for Windows AD authentication.

Before configuring Windows AD with NTLM, install the following tools:

- .NET Framework 3.5 or later
- IIS 7 or later

1. On the SharePoint portal, configure Windows AD authentication, and confirm that a Windows AD user can log on to the integration option for SharePoint software.

    For instructions, see the SharePoint documentation.
2. In the SharePoint software, create a new web application, and select *Classic Mode Authentication*.
3. In the *Authentication provider* section, select *NTLM*.
4. In the Central Management Console (CMC) in the Business Intelligence (BI) platform, configure Windows AD NTLM authentication.

    For instructions, search for "Windows AD authentication" in the *SAP BusinessObjects Business Intelligence Platform Administrator Guide*.
5. To confirm that Windows AD authentication is configured successfully in the BI platform, log on to the Central Configuration Manager (CCM) with the credentials of an authorized Windows AD user.
6. On the machine where the integration option for SharePoint software is installed, set the value of `authentication.visible` to `true` for the InfoViewApp web part in the `C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\Web Content\SharepointApp\InfoViewApp` file.

7. In the integration option for SharePoint software, confirm the configuration by logging on with the credentials of an authorized Windows AD user.
   The user should be logged on automatically to the software with Windows AD account credentials.

6.10.4 Configuring Windows AD with NTLM SSO

When using the IIS on the Windows operating system, you can configure NTLM SSO for Windows AD authentication.

Before configuring Windows AD with NTLM SSO, install the following tools:

- .NET Framework 3.5 or later
- IIS 7 or later

1. On the SharePoint portal, configure Windows AD authentication, and confirm that a Windows AD user can log on to the integration option for SharePoint software.

   For instructions, see the SharePoint documentation.
2. In the Central Management Console (CMC) in the Business Intelligence (BI) platform, enable SSO.

   For instructions, see the *SAP BusinessObjects Business Intelligence Platform Administrator Guide*.
3. In the CMC in the BI platform, configure NTLM for Windows AD authentication.

   For instructions, search for "Windows AD authentication" in the *SAP BusinessObjects Business Intelligence Platform Administrator Guide*.
4. In the BI launch pad, confirm that Windows AD authentication is correctly configured for the BI platform by logging on with the credentials of an authorized Windows AD user.
5. In the following integration option for SharePoint files, set the value of `sso.enabled` to `true`, the value of `authentication.default` to `secWinAD`, and the value of `identity impersonate` to `true`:
   - InfoViewApp web part at `C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\Web Content\SharepointApp\InfoViewApp`
   - SharePoint platform services at `C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\Web Content\SharepointApp\PlatformServices`
   - OpenDocument files at `C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\Web Content\SharepointApp\OpenDocument`
6. Restart IIS.
7. On the client machine, confirm that Windows AD authentication is correctly configured for the BI platform by logging on with the credentials of an authorized Windows AD user.
8. If the browser is Internet Explorer, select *Tools* > *Internet Options*, and perform the following actions:
   a. Click the *Security* tab, and click *Custom Level*.
   b. In the *Security Settings - Trust Sites Zone* dialog box, under *Settings*, locate *User Authentication*.
   c. Under *Logon*, select *Automatic logon with current user name and password*, click *OK*, and click *OK* again.

   If the browser is not Internet Explorer, skip this step.
9. On the client machine, confirm that you can access the URL of the machine hosting the integration option for SharePoint software.
10. In the integration option for SharePoint software, confirm the configuration by logging on with the credentials of an authorized Windows AD user.

The user should be logged on automatically to the software with Windows AD account credentials.

Related Information

Troubleshooting Windows AD with SSO [page 50]

6.10.5 Troubleshooting Windows AD with SSO

If a Windows Active Directory (AD) single sign-on (SSO) logon attempt fails, perform these actions:

- Clear the browser cookies, open a new browser window, and go to the URL of the machine where the integration option for SharePoint is deployed.
- Review the log files on the Central Management Server (CMS) in the Business Intelligence (BI) platform.
- Confirm that the same Windows AD authentication type (either NTLM or Kerberos, with or without SSO) is configured for SharePoint and for the BI platform.

6.11 Security and single sign-on

Users can log on directly to the Business Intelligence (BI) platform from SharePoint, using different types of authentication.

Single sign-on workflows are supported using Kerberos or CA SiteMinder.

Authentication mode	Description
Claims-based authentication for SharePoint	When a user logs on to SharePoint Server, a security token is validated and used to log on to SharePoint. The token is issued by a claims provider. Beginning with SharePoint 2013, claims-based authentication is the default method.
BusinessObjects Enterprise credentials	
Lightweight Directory Access Protocol (LDAP) authentication	• LDAP deployment must be set up correctly. • Portal user names must match aliases in the authentication system.
Windows Active Directory (AD) authentication	• AD deployment must be set up correctly. • Portal user names must match aliases in the authentication system.

For information about configuring authentication modes in the Central Management Console (CMC) in the BI platform, see the *SAP BusinessObjects Business Intelligence Platform Administrator Guide*.

Single sign-on

Single sign-on (SSO) is enabled when you set the value of `sso.enabled` to `true` in the `web.config` template configuration file. For example:

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

Related Information

SharePoint web.config template configuration file [page 20]

6.11.1 Configuring claims-based authentication for SharePoint 2016, SharePoint 2013, or SharePoint 2010

This task uses the `TrustedPrinciple.conf` file to pass the shared secret to the client machine when configuring NTLM claims-based authentication for SharePoint 2016, SharePoint 2013, or SharePoint 2010.

Before configuring claims-based authentication for SharePoint:

- You must be a member of the SharePoint Administrators group and a member of the Windows Administrators group on the server that is running Central Administration.
- Ensure that all SharePoint prerequisites have been met.
- Install the following tools:
  - .NET Framework 3.5 or later
  - IIS 7 or later
  - Microsoft SQL Server 2008
  - SharePoint 2016, SharePoint 2013, or SharePoint Server 2010

1. Create a SharePoint site that uses NTLM claims-based authentication.
2. Confirm that users can access the SharePoint site.
3. In the Central Management Console (CMC) in the BI platform, enable the Windows Active Directory (AD) plug-in, and import users.

   For instructions, see the *SAP BusinessObjects Business Intelligence Platform Administrator Guide*.
4. Confirm that users can manually log on to the BI platform.
5. Install the integration option for SharePoint software on the site you created in step 1.
6. Install the integration option for SharePoint software on the SharePoint machine.
7. In the `web.config` file for the InfoViewApp web part, perform the following actions:
   a. Set the value of `authentication.default` to `secWinAD`.
   b. Set the value of `authentication.visible` to `true`.

The InfoViewApp web part is located at `<InstallDir>:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\Web Content\SharePointApp\InfoViewApp`.

8. At the command line, enter **`iisreset /noforce`** to restart IIS.
9. Confirm that Windows AD users can manually log on to the integration option for SharePoint site that you created in step 1.
10. In the CMC in the BI platform, perform the following actions:
    a. Enable trusted authentication, and use the `web.config` file to generate a shared secret.
    b. Assign aliases to map Windows AD user names to Enterprise user names.

    For instructions, see the *SAP BusinessObjects Business Intelligence Platform Administrator Guide*.
11. Confirm that Windows AD users can log on to the BI launch pad using SSO with trusted authentication.
12. Copy the shared secret (in the `TrustedPrinciple.conf` file) from the BI platform machine to the `<InstallDir>:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\win64_x64` folder on the SharePoint server.
13. In the `web.config` file for the InfoViewApp web part, set the value of `isTrusted` to `true`.
14. At the command line, enter **`iisreset /noforce`** to restart IIS.

From client machines, users can automatically log on (via SSO) to the integration option for SharePoint site you created.

6.11.2 Creating a web application on port 1250 for SharePoint 2013

Before creating a web application on port 1250 for SharePoint 2013:

- You must be a member of the SharePoint Farm Administrators group and a member of the Windows Administrators group on the server that is running Central Administration.
- Ensure that all SharePoint prerequisites have been met.
- Install the following tools:
  - .NET Framework 3.5 SP1 or later
  - IIS 7 or later
  - SQL Server 2008 R2
  - SharePoint 2013

1. In SharePoint Central Administration, on the *Application Management* tab, click *Manage web applications*, and then click *New* on the toolbar.

   The *Create New Web Application* window appears.
2. Beside *Authentication*, select *Claims Based Authentication*.
3. Beside *IIS Web Site*, perform the following actions:
   a. Select *Create a new IIS web site*.
   b. In the *Name* box, enter **`SharePoint - 1250`**
   c. In the *Port* box, enter **`1250`**
   d. In the *Host Header* box, enter the host name that will be used to access the web application.
   e. In the *Path* box, enter the path to the root folder for the IIS web site on the server.

4. Beside *Security Configuration*, perform the following actions:
    a. Under *Allow Anonymous*, select *No*.
    b. Under *Use Secure Sockets Layer (SSL)*, select *No*.
5. Beside *Claims Authentication Types*, perform the following actions:
    a. Select the *Enable Windows Authentication* check box.
    b. Select the *Integrated Windows authentication* check box, and select *NTLM* in the list.
6. Beside *Sign In Page URL*, select *Default Sign In Page*.
7. Beside *Public URL*, enter **`http://SP:1250`** in the *URL* box.
8. Beside *Application Pool*, perform the following actions:
    a. Select *Create a new application pool*.
    b. In the *Application pool name* box, enter **`SharePoint - 1250`**
    c. Under *Select a security account for this application pool*, select *Predefined*, and select *Network Service* in the list.
9. Beside *Database Name and Authentication*, perform the following actions:
    a. In the *Database Server* box, enter **`SP\SharePoint`**
    b. In the *Database Name* box, enter a database name for the new web application.
    c. Under *Database authentication*, select *Windows Authentication (recommended)*.
10. Click *OK* to create the web application, and click *OK* again.

The web application is created and appears on the *Web Applications Management* page in Central Administration.

7 Integration option for SharePoint software deployment

7.1 Adding or removing languages

Before adding or removing a language, install the following tools:

- .NET Framework 3.5 or later
- IIS 7 or later

1. Open the *Control Panel* in the Windows operating system, and perform one of the following actions:
   - In newer versions of Windows (for example, Windows Server 2008), click ▶ *Programs* ▶ *Programs and Features* ▶ *SAP Integration for Microsoft SharePoint 4.1* ◀, and click *Uninstall/Change*.
   - In older versions of Windows (for example, Windows Server 2003), click *Add or Remove Programs*, select *Integration Option for SharePoint software*, and click *Change*.

   The *Application Maintenance* page appears.
2. Click *Modify*, and click *Next*.
3. On the *Select Language Packages* page, select the check box for the language to add or to remove, and click *Next*.

   Select the *All Languages* check box to add or remove Arabic, English, French, German, Icelandic, and Japanese.
4. On the *Deployment Options* page, select the check box for the SharePoint server to which to deploy the language(s), and click *Next*.

   Select the *Select All* check box to deploy the language(s) to all servers.
5. Click *Next* to start the language deployment.

7.2 Deploying the software to additional sites

If the integration option for SharePoint was deployed to a subset of available virtual sites, you can modify your installation to deploy to the remaining sites.

Before deploying the software to an additional site, install the following tools:

- .NET Framework 3.5 or later
- IIS 7 or later

1. Open the *Control Panel* in the Windows operating system, and perform one of the following actions:
   - In newer versions of Windows (for example, Windows Server 2008), click ▶ *Programs* ▶ *Programs and Features* ▶ *SAP Integration for Microsoft SharePoint 4.1* ◀, and click *Uninstall/Change*.

- In older versions of Windows (for example, Windows Server 2003), click *Add or Remove Programs*, select *Integration Option for SharePoint software*, and click *Change*.

 The *Application Maintenance* page appears.

2. Click *Modify*, and click *Next*.
 The *Deployment Options* page appears.
3. Select each site to which to deploy the software.

 Sites at which the software is already deployed are unavailable.
4. Click *Next* to start the software deployment.

7.3 (Optional) Manually deploying the Web Intelligence Web Service to a site

The integration option for SharePoint software requires the Web Intelligence Web Service to open Web Intelligence documents in SharePoint 2016 or SharePoint 2013. The service can be deployed to a new web site during installation. If you did not deploy the service to a site during installation, you can manually deploy it to the site.

Before deploying the Web Intelligence Web Service to a site, install and configure the integration option for SharePoint.

1. In Internet Information Services (IIS) Manager, right-click the `<YourMachineName>\Sites\SharePoint - <PortNumber>\_vti_bin\AnalyticalReporting` folder and select *Explore*.
2. Copy all files in the `AnalyticalReporting` folder.
 For example, copy `ReportEngine.svc`, `ServerGateway.svc`, `web.config`, and so on.
3. Create a new folder, and paste the copied files in the folder.
 For example, create a folder at `C:\inetpub\wwwroot\WebIntelligenceGateway`.
4. In IIS Manager, right-click the `<YourMachineName>\Sites\SharePoint - <IpointPortNumber>\bin` folder and select *Explore*.
5. Copy the entire `bin` folder to the `C:\inetpub\wwwroot\WebIntelligenceGateway` folder.

 The `bin` folder contains `BusinessObjects.Sdk.Core.dll`, `BusinessObjects.Sdk.Core.Server.dll`, `BusinessObjects.Sdk.Core.Server.Service.dll`, `Microsoft.Practices.ServiceLocation.dll`, and so on.
6. In IIS Manager, right-click the *Sites* node and select *Add New Site*.
7. In the *Add Web Site* dialog box, perform the following actions:
   a. In the *Site name* box, enter a name for the site.
   For example, enter **`WebIntelligence Gateway`**
   b. In the *Application Pool* box, click *Select* and choose the application pool on which the integration option for SharePoint software is installed.
   c. In the *Physical path* box, browse to locate the folder you created in step 3.
   For example, the folder might be located at `C:\inetpub\wwwroot\WebIntelligenceGateway`.
   d. Under *Binding*, enter an unused port number in the *Port* box, make note of the port number, and click *OK*.
   For example, use port 2550.

8. In IIS Manager, select the Web Intelligence Gateway site and open the *Authentication* properties.
9. Enable *Anonymous* and *Windows* authentication, and disable all the other types of authentication.
10. In IIS Manager, right-click `DEWDFWADEPT394\Sites\SharePoint - <IpointPortNumber>\_layouts\AnalyticalReporting` and select *Explore*.
11. Locate and open the `web.config` file, search for `webi_gateway_port` in the file, and set it to the same port value as in step 7d.
    For example, if you entered port 2550 in step 7d, enter port 2550 here.

You can open Web Intelligence documents in SharePoint 2016 or SharePoint 2013 at the site.

7.3.1 (Optional) Removing the Web Intelligence Web Service from a site

If you remove the Web Intelligence Web Service from a site, you cannot view Web Intelligence documents in SharePoint 2016 or SharePoint 2013 at the site.

1. In IIS Manager, stop the WebIntelligence Gateway site that is running the Web Intelligence Web Service.
2. Delete the WebIntelligence Gateway site.
3. Locate and delete the `WebIntelligenceGateway` folder for the site.
   For example, delete `C:\inetpub\wwwroot\WebIntelligenceGateway`.

7.4 Repairing the integration option for SharePoint software

The repair process restores files and options to default values and the integration option for SharePoint software to its default configuration.

Before repairing the software, install the following tools:

- .NET Framework 3.5 or later
- IIS 7 or later

1. Open the *Control Panel* in the Windows operating system, and perform one of the following actions:
   - In newer versions of Windows (for example, Windows Server 2008), click *Programs* > *Programs and Features* > *SAP Integration for Microsoft SharePoint 4.1*, and click *Uninstall/Change*.
   - In older versions of Windows (for example, Windows Server 2003), click *Add or Remove Programs*, select *Integration Option for SharePoint software*, and click *Change*.
   - On UNIX (for Business Intelligence platform server installations), run the `modifyOrRemoveProducts.sh` program, and select the integration option for SharePoint software.
2. On the *Application Maintenance* page, click *Repair*.
3. On the *Software has been installed successfully* page, click *Finish*.
   The integration option for SharePoint software is restored to its default configuration and values.

7.5 Removing the integration options for SharePoint software

All web parts, samples, and documentation are removed from virtual servers when you remove the integration option for SharePoint software. Instances and other content in the Business Intelligence (BI) platform that web site creators and information consumers added are not removed.

Before removing the software, install the following tools:

- .NET Framework 3.5 or later
- IIS 7 or later

1. Open the *Control Panel* in the Windows operating system, and perform one of the following actions:
    - In newer versions of Windows (for example, Windows Server 2008), click *Programs* > *Programs and Features* > *SAP Integration for Microsoft SharePoint 4.1*, and click *Uninstall/Change*.
    - In older versions of Windows (for example, Windows Server 2003), click *Add or Remove Programs*, select *Integration Option for SharePoint software*, and click *Change*.
    - On UNIX (BI platform server installations), run the `modifyOrRemoveProducts.sh` program, and select *Integration Option for Microsoft SharePoint software*.
2. On the *Application Maintenance* page, click *Remove*.
3. When prompted, click *Yes* to confirm the uninstallation.
4. Click *Finish*.

8 BI platform configuration

When you first install the integration option for SharePoint, you must configure or update options in the Business Intelligence (BI) platform to optimize your deployment.

8.1 Assigning viewing rights to users and user groups

You must assign access rights to users and to user groups before users can open reports.

Users must have the View right to open scheduled reports and triggered instances and the View on Demand right to access reports in real-time. For more information about setting user rights, see the *SAP BusinessObjects Business Intelligence Platform Administrator Guide*.

1. In the Central Management Console (CMC) in the Business Intelligence (BI) platform, add all users to the group called *Everyone*.
2. Assign viewing rights to the *Everyone* group.
   Viewing rights enable all users in the *Everyone* group to view reports in SharePoint.

8.2 (Optional) Specifying a RAS for report processing

You can change the default server used to process the reports that users view from the Business Intelligence (BI) platform page server to the Report Application Server (RAS).

By default, reports are processed by the BI platform page server. If the page server is not available, the RAS is used. To configure the BI platform to use the RAS, by default, to process reports, you must create a new server group for the RAS in the BI platform, specify the server group in all reports, and then stop the BI platform page server.

1. Log on to the Central Management Console (CMC) in the BI platform.
2. In the *Object Management* area of the CMC, click an object link to select the object.
3. Click the *Process* tab.
4. In the *Default Servers To Use For Viewing* area, perform one of the following actions:
   - Select *Use the first available server* if you want the BI platform to process objects on the server that has the maximum number of free resources.
   - Select *Give preference to servers in the selected group* if you want the BI platform to process objects only on servers in the selected server group, and then select the server group.
     If servers are not available, objects are processed by the next available server, which may not belong to the selected group.
   - Select *Only use servers in the selected group* if you want the BI platform to process objects only on servers in the selected server group, and then select the server group.

If no servers in the server group are available, no objects are processed.

5. Click *Update*.

8.3 (Optional) Specifying parameter prompt values

1. Log on to the Central Management Console (CMC) in the Business Intelligence (BI) platform.
2. In the *Objects Management* area, click the link for the report for which to specify parameter prompt values.
3. In the report, on the *Process* tab, click the *Parameters* link.
4. In the *Value* column for a parameter, select the value.
5. Select *Prompt when viewing* to prompt users who view the report instance in the corresponding web part.
6. Click *Submit*.

8.4 Opening documents using OpenDocument links

To open documents using OpenDocument links instead of opening within SharePoint, follow the procedure below:

1. Open ipointconfig.xml in `<Install Directory>\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\conf\iPoint\ipointconfig.xml`
2. In the *<BusinessObjectsEnterpriseSharePointInfoViewDocumentViewerUrl>* field, replace `:8080/BOE/OpenDocument/opendoc/openDocument.jsp?sIDType=CUID&amp;iDocID=%id %&amp;token=%token%&amp;lang=%lang%` with `/_layouts/OpenDocument/opendoc/openDocument.aspx?sKind=%type%&amp;sIDType=CUID&amp;iDocID=%id%&amp;token=%token%&amp;lang=%lang%`.
3. To reset the Internet Information Server (IIS), choose *Windows* > *Run* > *iisreset*. You can also choose *Windows* > *Command Prompt* > *iisreset*.

9 Scheduling and scaling best practices

The same general scheduling and scaling recommendations apply to the Business Intelligence (BI) platform and to the integration option for SharePoint software.

Use the BI platform to schedule, process, and run reports, and use the Central Management Console (CMC) in the platform to specify scheduling properties for reports. When defining scheduling properties for reports:

- If reports must be regularly updated, and if all users will access the same data, schedule reports to run per your requirements.
- To view a report, you must schedule and run the report instead of viewing it on demand.
  Scheduled reports use fewer resources in the BI platform.
- If you assign the View on Demand right to a user, when the user refreshes a report, the report accesses its data source.
- When designing your SharePoint portal, be careful when combining web parts of the integration option for SharePoint software (which contain real-time views) with third-party web parts that are page-refresh intensive. When a user refreshes a page, all reports on the web page are refreshed. For example, if a web page contains a stock ticker that is refreshed every 10 seconds, all reports on the web page are also refreshed every 10 seconds.

For scheduling information, see the *SAP BusinessObjects Business Intelligence Platform Administrator Guide*.

9.1 Exporting reports

For best performance, specify export options (Microsoft Excel, Adobe Acrobat, and so on) when scheduling a report. User requests to dynamically export reports by selecting alternative format viewing options are process- and resource-intensive.

9.2 Database logon information for reports

For best performance, specify database logon information for reports in the Central Management Console (CMC) in the Business Intelligence (BI) platform. If you do not, users must log on to the database each time they refresh or view a report.

9.3 Required user viewing rights for reports

If a report contains parameters, users must have the View on Demand right in order to view it. If you use the Business Intelligence (BI) platform page server to view summaries of multiple reports, users must also have the Edit right.

10 Crystal report best practices

When creating Crystal reports:

- The background must be transparent in reports.
- Make maximum use of screen resolution and space for report parts.
- Keep parameter names short and parameter descriptions meaningful, because users can see the parameter names and descriptions in tooltips.

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

Important Disclaimers and Legal Information

Hyperlinks

Some links are classified by an icon and/or a mouseover text. These links provide additional information.
About the icons:

- Links with the icon ➦ : You are entering a Web site that is not hosted by SAP. By using such links, you agree (unless expressly stated otherwise in your agreements with SAP) to this:
    - The content of the linked-to site is not SAP documentation. You may not infer any product claims against SAP based on this information.
    - SAP does not agree or disagree with the content on the linked-to site, nor does SAP warrant the availability and correctness. SAP shall not be liable for any damages caused by the use of such content unless damages have been caused by SAP's gross negligence or willful misconduct.
- Links with the icon ➦: You are leaving the documentation for that particular SAP product or service and are entering an SAP-hosted Web site. By using such links, you agree that (unless expressly stated otherwise in your agreements with SAP) you may not infer any product claims against SAP based on this information.

Videos Hosted on External Platforms

Some videos may point to third-party video hosting platforms. SAP cannot guarantee the future availability of videos stored on these platforms. Furthermore, any advertisements or other content hosted on these platforms (for example, suggested videos or by navigating to other videos hosted on the same site), are not within the control or responsibility of SAP.

Beta and Other Experimental Features

Experimental features are not part of the officially delivered scope that SAP guarantees for future releases. This means that experimental features may be changed by SAP at any time for any reason without notice. Experimental features are not for productive use. You may not demonstrate, test, examine, evaluate or otherwise use the experimental features in a live operating environment or with data that has not been sufficiently backed up.
The purpose of experimental features is to get feedback early on, allowing customers and partners to influence the future product accordingly. By providing your feedback (e.g. in the SAP Community), you accept that intellectual property rights of the contributions or derivative works shall remain the exclusive property of SAP.

Example Code

Any software coding and/or code snippets are examples. They are not for productive use. The example code is only intended to better explain and visualize the syntax and phrasing rules. SAP does not warrant the correctness and completeness of the example code. SAP shall not be liable for errors or damages caused by the use of example code unless damages have been caused by SAP's gross negligence or willful misconduct.

Bias-Free Language

SAP supports a culture of diversity and inclusion. Whenever possible, we use unbiased language in our documentation to refer to people of all cultures, ethnicities, genders, and abilities.

www.sap.com/contactsap

THE BEST RUN SAP