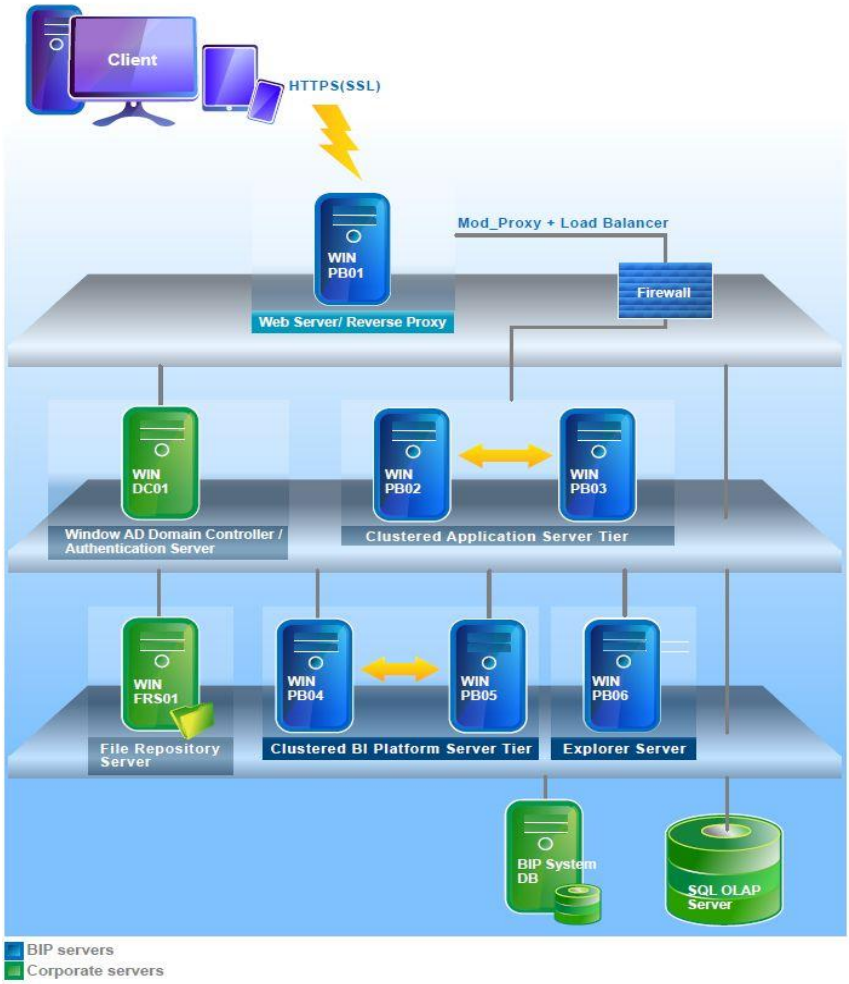
SAP BusinessObjects BI Pattern Books



Deploying SAP Business BI Platform on Windows with Mobile and Explorer

ABSTRACT

In this pattern, we deploy SAP BusinessObjects BI platform on Windows 2008 release 2.

Disclaimer

- This pattern book is for informational purpose only and may not be copied / reproduced without the permission of SAP
- The information provided in this book are based on the SAP BI Pattern Books project for a specific set of patterns / use cases applied within SAP lab environment. Hence, make sure to review and apply the steps / workflows that are applicable to your use cases / patterns, based on your SAP BusinessObjects BI landscape
- Contents of this, or any related document and SAP's strategy and possible future developments, products and or platforms directions and functionality that are discussed in this book all subject to change and may be changed by SAP at any time for any reason without notice. Therefore, read the latest official product guides, release notes to understand the differences and act accordingly

For further comments and questions, email to SAPEnableBI@sap.com

Contents

BIP on Windows with Mobile and Explorer Pattern Book 4
System landscape overview 4
Pattern Overview 8
Pattern Prerequisites 8
Database Overview 11
CMS Database 11
Auditing Database 12
Reporting Database 15
Installing the SQL Server middleware 16
Configuring the File Repository Server (FRS) 52
BI platform 4.0 cluster configuration 58
Configuring and installing BI platform on server 1 58
Configuring and installing BI platform on server 2 82
Changing the cluster name 101
Splitting the Adaptive Processing Server (APS) 106
Setting up the Application Server 107
Setting up Application Server 1 107
Setting up Application Server 2 114
Installing the BI platform web tier 114
Configuring the Application Server Cluster 132
Setting up Apache 2.4 136
Installing Apache 2.4 as a service 136
Securing the Apache web server 143
Configuring the reverse proxy 146
Enabling the proxy cache 151
Setting up the Authentication Server 159
Setting up the SAP plug-in 160
Setting up SAP SSO using the Security Token Service (STS) 167
Setting up the Windows Active Directory (AD) server 173
Setting up the Windows AD plug-in 182
Kerberos 188
Setting up Manual Java Authentication 190

Setting up Single Sign On using Vintela 197
Adding SAP BusinessObjects Explorer 199
Setting up SAP BusinessObjects Mobile 200
Troubleshooting the Windows Pattern 211
Explorer Troubleshooting 211
Application Server Troubleshooting 212
Apache Troubleshooting 216

BIP on Windows with Mobile and Explorer Pattern Book

This pattern showcases the real-world example of deploying SAP BusinessObjects BI platform in a company's existing infrastructure. It is robust, scalable, and secure enough to handle a moderate number of user requests.

In our examples, all BI platform machines are running Windows 2008 R2. We will use number of machines in this pattern and examine the procedures required to set up the Windows pattern in detail from start to finish.

For an overview of the machines in this pattern, see System landscape overview. To follow the pattern, complete the tasks in the order presented in Pattern Overview.

This pattern is for SAP BusinessObjects 4.0 SP4. For previous pattern books, see the following list:

- BusinessObjects Enterprise XI 3.1 Pattern Book for Windows
- BusinessObjects XI Release 2 Pattern Book for IBM

System landscape overview

The following illustration shows the technical architecture of the environment used in this pattern. Each server node is identified with the logical name corresponding to the architecture components it hosts.

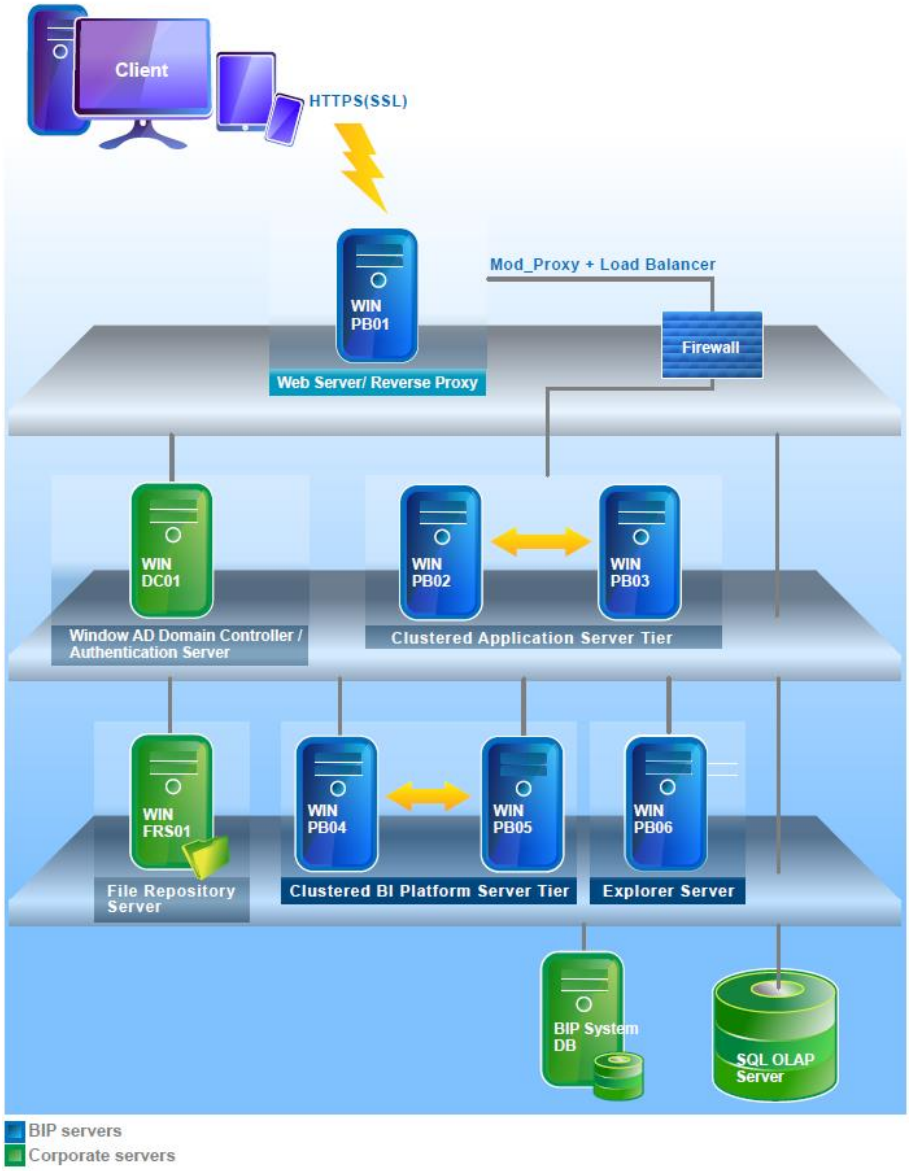
Note: This illustration provides an overview of the system landscape and shows the role of each machine, not the workflow order of tasks to complete. To follow the pattern, complete the tasks in the order listed in Pattern Overview rather than the order shown below.

Key configurations of this technical architecture

The architecture shown in the illustration highlights four key aspects of the system landscape required for deployment:

- Clustered servers.
- Load balancing.
- Support for reverse proxy.
- Secured SSL.

Web Server / Reverse Proxy (WIN PB01)



Web Server / Reverse Proxy (WIN PB01)

The machines that host the web server, reverse proxy server, and load ballancer commonly reside outside your external firewall. Customers can access Business Intelligence platform web

applications, such as BI Launch Pad and the Central Management Console (CMC), from the client machine.

Apache is the web server chosen for this pattern, because Apache is the most commonly used web server on the web, hosting over 60% of all websites.

The latest supported version of Reverse Proxy Server in SAP Business Intelligence (BI) platform 4.0 Service Pack 4 is Apache 2.4, the current mainstream release.

For information about setup details, see Setting up Apache 2.4.

Windows AD Domain Controller / Authentication Server (WIN DC01)

This pattern uses Windows Active Directory and SAP BW authentication methods. However, BI 4.0 supports many authentication modes. Depending on the infrastructure of your system, you may be able to choose a preferred authentication method.

For information about setup details, see Setting up the Authentication Server.

Web Application Servers (WIN PB02 and WIN PB03)

The application servers host Business Intelligence Platform web applications, such as BI launch pad and the CMC. For production systems, you must deploy at least two web application servers to manage failover and load balancing. Your system may require more than two. The only way to know how many web application servers your system will need is to do a detailed sizing exercise.

This pattern uses Tomcat version 6.

For information about setup details, see Setting up the Application Server.

BI Platform Servers (WIN PB04 and WIN PB05)

In this pattern, two nodes are dedicated to BI platform services. Those two machines are clustered and host all the BI platform services.

BI platform web applications detect each BI platform server machine (specifically, they detect all CMS Servers in a cluster), and then automatically load balance their requests. If one machine fails, the web applications automatically send all requests to the other machine.

For production systems, you must deploy at least two BI platform server machines. If you need to increase scalability, you can deploy more BI platform server machines. To determine the exact number of servers and server instances needed, do a detailed sizing exercise.

For information about setup details, see BI platform 4.0 cluster configuration.

BI Explorer Server (WIN PB06)

For this pattern, SAP BI Explorer is deployed on a dedicated host.

For information about how to size for BI Explorer, and how to set up and configure SAP BusinessObjects Explorer, see Adding SAP BusinessObjects Explorer.

File repository server (WIN FRS01)

The File Repository Server (FRS) contains all reports and other BI documents that have been created. When a user creates a BI document, the BI platform servers retrieve the data from your company database (Reporting DB), generates the document, and stores it in the FRS.

For production systems, it's best to host the FRS on a separate machine because the BI documents it stores can grow to a large number. Also, because BI documents often contain sensitive information, be sure to host the FRS on a secured machine.

For information about setup details, see Configuring the File Repository Server (FRS).

BI platform System & Audit Database Server

BI platform uses a database for its system data, which is referred to as the system database or "CMS database". It's called the CMS database because, when a user wants to see a report, the CMS checks the system database to obtain the location of the report.

For production systems, you can host the CMS database either on the database included with BI platform or on your existing database. Both are recommended for production systems, but often companies use their own databases to simplify administration.

This pattern uses MS SQL Server for BI platform System and Audit databases.

For information about setup details, see Database Overview.

OLAP Reporting DB Server (WIN PB07)

MS SQL OLAP server is used as one of the reporting databases in this pattern.

For information about how to set up OLAP BP, the client, and to connect to SAP BI OLAP, see the OLAP Overview.

Pattern Overview

Here is the workflow for deploying this pattern:

Task	Objective
Review Pattern prerequisites.	Review a checklist of items to consider before deploying this pattern.
Set up File Sharing.	Configure access to a shared file repository location.
Install SQL Server middleware.	Install and configure database middleware.
Install the BI platform cluster	Install BI platform servers on two machines, and then cluster them.
Install the Application Server.	Install Tomcat (version 6) on two machines, and then cluster them.
Install Apache.	Install Apache, configure firewall, configure reverse proxy, and then enable proxy cache
Set up the Authentication Server.	Setup domain controller and Windows AD authentication system.

For information about the databases that you'll need for this pattern, see Database Overview.

Pattern Prerequisites

The following checklist shows the prerequisite skills, system rights, and tools you'll need to successfully deploy this pattern. Details on each prerequisite are explained here.

Pattern prerequisite checklist

Intermediate knowledge of the Windows operating system and the third-party software components used.	✅
Install package downloaded and available.	✅
Required License Keys.	✅
Ensured OS compatibility with all software.	✅
Operating System Update Utility preconfigured.	✅
UPDATED - Configure Linux User for optimal virtual memory usage	✅
Network access and Internet/Proxy configured.	✅
Root/Admin access on machines or System Administrator rights granted.	✅
Database access granted to System (CMS/Auditing) and Reporting databases.	✅

Intermediate knowledge of operating system (Windows) and third-party software components used

You must be able to use Windows at an intermediate skill level, and be familiar with third-party tools such as Apache, Tomcat, and Samba.

Install package downloaded and available

Make sure the software installation package is downloaded, copied, and available in the planned directory.

Required License Keys

You'll need to have the valid license keys available for use throughout this deployment. The license keys shown in this pattern are examples only and will not work in the deployment.

Ensured OS compatibility with all software

If you are using versions of software that are different from the ones indicated in this pattern, check the documentation for each component to ensure it will be compatible. This pattern has been tested for compatibility only with the specific versions of software listed.

For a complete list of supported components, version, and compatibility, review the latest Product Availability Matrix.

UPDATED - Configure Linux User for optimal virtual memory usage

Some versions of the Linux operating system utilize some new memory allocator functionality. For some applications, this will result in very high virtual memory allocations on multicore servers which can cause issues with the Web Intelligence Processing Servers. The more cores your Linux server has, the higher the virtual memory usage will be. For more details on this, please refer to KBA - 1968075and follow the steps outlined within to help address this issue.

Operating System Update option enabled

All machines used in this deployment must be preconfigured to automatically install regular operating system updates.

Operating System Update option enabled

All machines used in this deployment must be preconfigured to automatically install regular operating system updates.

Network access and Internet/Proxy configured

Machines must be networked and have Web access. This is required for certain workflows.

Admin access on machines or System Administrator available

You'll need administrator access to the servers used in this deployment.

Database access is in place for system (CMS and auditing) and reporting databases

Access to the specified databases (system (CMS) database, auditing database, and reporting databases), with sufficient user permissions, is essential. Make sure the required database

access is in place before deploying SAP Business Intelligence. It is also recommended that the CMS database and auditing database be kept separate from the databases used to store reporting data (reporting databases). For more information, see Database Overview.

Database Overview

The following sections examine in detail each database you need in this pattern:

Database	Description
CMS Database	Set up the BI platform repository to obtain user, server, folder, document, configuration, and authentication information.
Auditing Database	Set up the BI platform repository to obtain audit information.
Reporting Database	Set up and configure databases to obtain reporting information.
Installing the SQL Server middleware	Set up and configure the SQL Server middleware client

CMS Database

The CMS system database is used to store BI platform information, such as user, server, folder, document, configuration, and authentication details. It is maintained by the Central Management Server (CMS), and in other documentation may be referred to as the system database or repository.

During installation of BI platform, you are asked to select a database to connect to. Once you select a database, the setup program creates the tables and views needed to use that database as the system database. During the installation, default servers, users, groups, and content are added to this database.

For this Windows pattern, a SQL Server 2008 Release 2 database client and server is used. A database user account and schema has been created specifically for this pattern for use in the CMS database. The database user account will require read, write, and modify-table permissions. And it will need permissions to create stored procedures on the schema. This pattern reviews the SQL Server 2008 Release 2 configuration in installing the SQL Server middleware.

The CMS database is a central and critical component of the BI platform architecture. It therefore needs appropriate support from data safety policies. Although this pattern uses single database server to host the CMS database, in a production environment, policies for redundancy and appropriate database recovery are necessary.

For more information about the CMS database and other servers within the BI platform, see the BIP 4.0 SP5 Administrators Guide.

Warning: Each BI platform environment requires a unique set of users and schemas. If you use an existing schema, the data is overwritten and your existing system is lost.

Here is an example of suggested naming conventions to use for user accounts and schemas. Note that the user name and schema are often the same.

Stage of Deployment	CMS User/Schema Name	Audit User/Schema Name
Proof of concept (POC)	BI4CMSPOC	BI4AUDPOC
Development	BI4CMSDEV	BI4AUDDEV
Quality Assurance	BI4CMSQA	BI4AUDQA
Production	BI4CMSPROD	BI4AUDPROD

Details on the SQL Server database used for the CMS database in this pattern

CMS Database overview for this Windows pattern

Version	SQL Server 2008 R2
Database Name	cms08r2u03
Server Name	VANPGDBSQL03.dhcp.pgdev.sap.corp
Port	1433
Username	i817318a
DSN	CMSDB

Before installing BI platform 4.0, you must create a new ODBC DSN so that it can be referenced later during the installation process. This DSN will be used by the CMS service. Because the CMS is a 64-bit process, the DSN must be created using the 64bit ODBC Administrator.
The 64-bit version of the ODBCAD32.exe file is located in the %systemdrive%\Windows\System32 folder.

Auditing Database

The Central Management Server (CMS) collects audit information from the other BI platform servers and writes the details to the Auditing Data Store (ADS), known as the Auditing database.

This information lets System Administrators manage their BI platform environment, and content usage, through reporting and analysis of ADS data.

In this pattern, the same SQL Server 2008 Release 2 database server is used for the CMS and Auditing databases. A user account and schema has been created for auditing use only.

For more information about the SQL Server client configuration, see Installing the SQL Server middleware.

During the installation of your primary BI platform server, you are asked for the connection information to your auditing database. An Audit user account and schema has been created specifically for this pattern.

For more information about auditing set up and configuration, see Chapter 20: Auditing in the BI Platform Administrator Guide.

The auditing database user account requires its own schema (preferably separate from the CMS database schema) with create, modify, and delete table permissions.

Checklist

Before installing BI platform, ensure the following conditions have been met:

The database client is installed and configured for the BI platform user account.	✅
The Auditing database user and schema have been created.	✅
The Auditing database user has been granted create, modify, and delete permissions for tables and stored procedures.	✅
A new ODBC DSN has been created on each node where the CMS will be run for auditing.	✅

Warning: Each BI platform environment requires a unique set of users and schemas. If you use an existing schema, the data will be overwritten and your existing system will be lost.

Here is an example of suggested naming conventions to use for user accounts and schemas. Note that the user name and schema are often the same.

Stage of Deployment	CMS User/Schema Name	Audit User/Schema Name
Proof of concept (POC)	BI4CMSPOC	BI4AUDPOC
Development	BI4CMSDEV	BI4AUDDEV
Quality Assurance	BI4CMSQA	BI4AUDQA
Production	BI4CMSPROD	BI4AUDPROD

The installation program does not request the name of the schema that you create. It uses the default schema name specified for the user account.

Before starting your installation, do the following test: connect to the database from the BI platform machine with your CMS and Auditing user account.

Details on the SQL Server 2008 R2 database server used for our Auditing database in this pattern

Auditing Database Overview for our Windows pattern

Version	SQL Server 2008 R2
Database Name	cms08r2u03
Server Name	VANPGDBSQL03.dhcp.pgdev.sap.corp
Port	1433
Username	i817318b
DSN	AUDITDB

Before installing BI platform 4.0, you must create a new ODBC DSN so that it can be referenced later during the installation process. This DSN will be used by the CMS service. Because the CMS is a 64-bit process, the DSN must be created using the 64bit ODBC Administrator.

The 64-bit version of the ODBCAD32.exe file is located in the %systemdrive%\Windows\System32 folder.

Reporting Database

The databases that are used to store reporting data are referred to as reporting databases.

For this deployment, to report off of reporting databases you will need the connection information for them, and a list of the user accounts that have read access to the data on each one. If you do not have this information, ask your database administrator.

In this pattern, Microsoft SQL Server 2008 R2 64-bit and SAP BW 7.30 are used as the reporting databases. They are on servers separate from those that host the CMS and Auditing databases and must be configured and tested separately.

Warning: To avoid competition for resources, it is recommended to avoid hosting the CMS and Auditing databases on the same database server as your reporting databases. The CMS and Auditing databases are critical to the performance of your system, and therefore must operate independently of other resources.

Details on the reporting databases used in this pattern

SQL Server

Reporting database overview for this pattern

Version	Microsoft SQL Server 2008 R2 10.50.1600.1
Database Name	AdventureWorks2008R2
Character Encoding	UTF-8
Page Size	8KB
Server Name	vantgvmwinpb07.BI4PATTERN.COM
Machine	vantgvmwinpb07.BI4PATTERN.COM
Username	Sqluser

SAP BW 7.30

Reporting database overview for this pattern

Version	SAP BW 7.30
Release	730
Level	0007

Database Name	Netweaver Demo
Unicode System	Yes
Host	VANPGC34B3
Server Name	vanpgc34b3_R79_00
Username	Pattern

Installing the SQL Server middleware

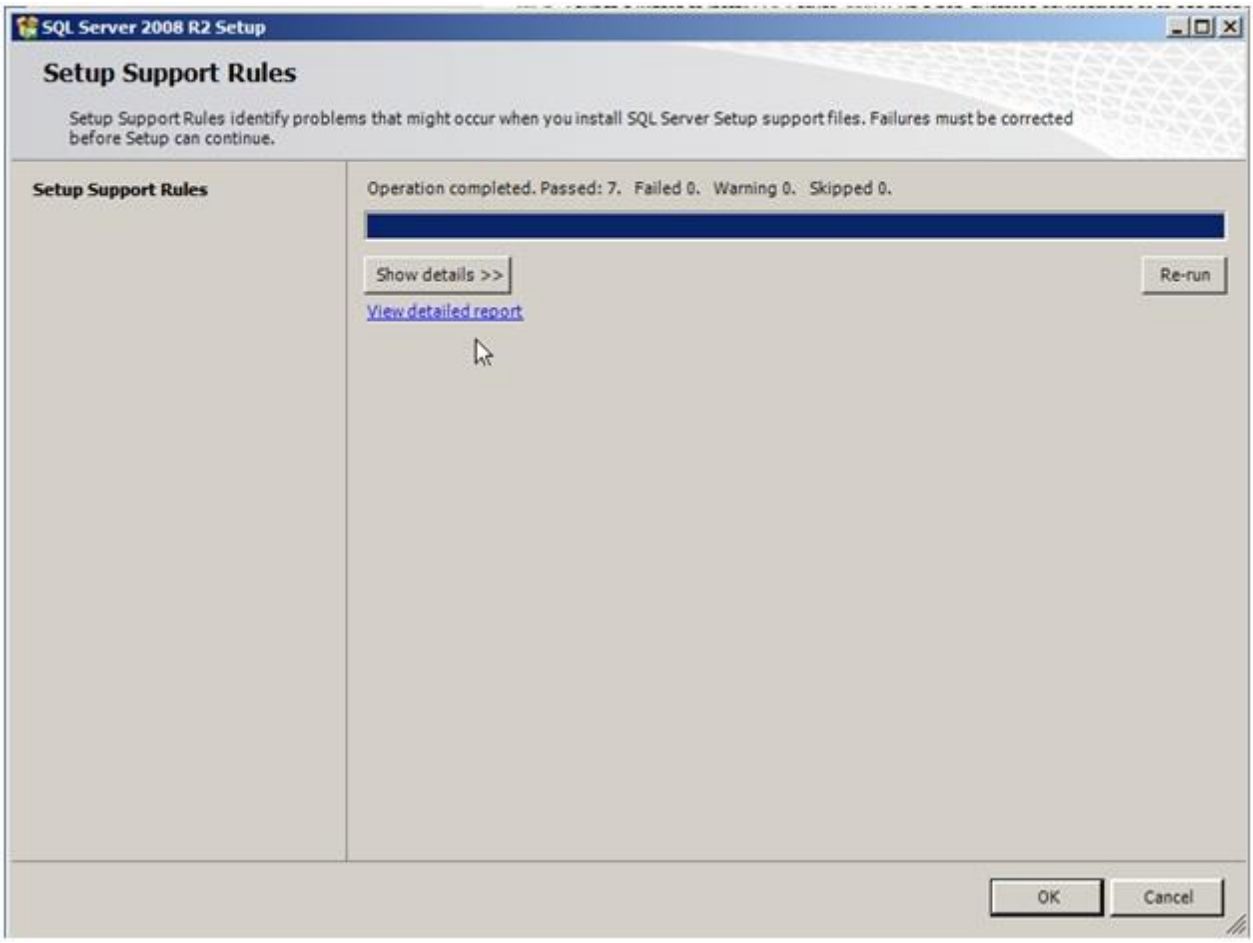
To install the SQL Server Client

Warning: As a prerequisite, SQL Server Client must have been installed on VANTGVMWINPB04 and VANTGVMWINPB05. To verify this, you must be logged into Windows with an Administrator account.

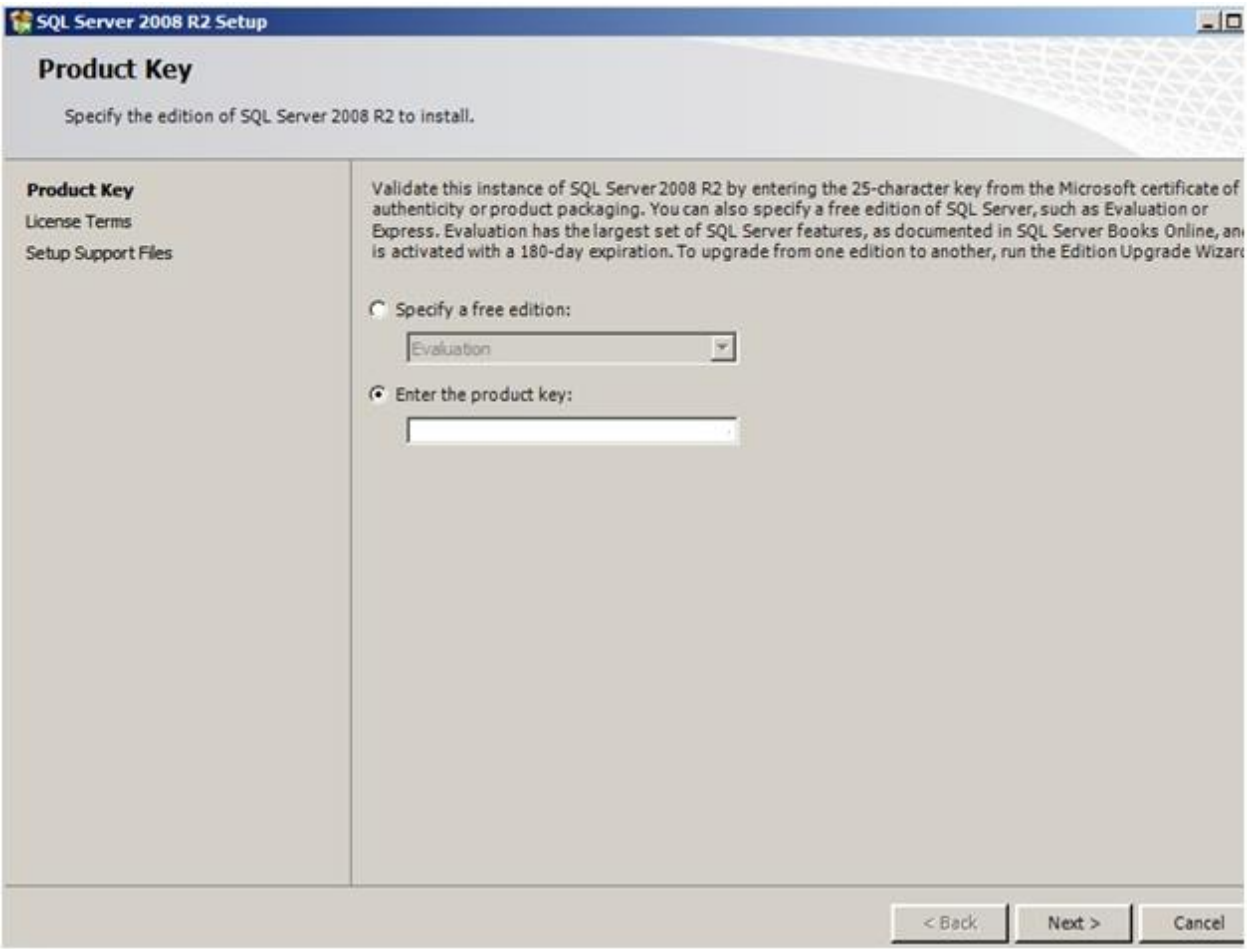
1. In Windows, go to the SQL Server 2008 R2 Setup folder, and double-click Setup.exe.

   The **SQL Server 2008 R2 Setup** wizard opens.

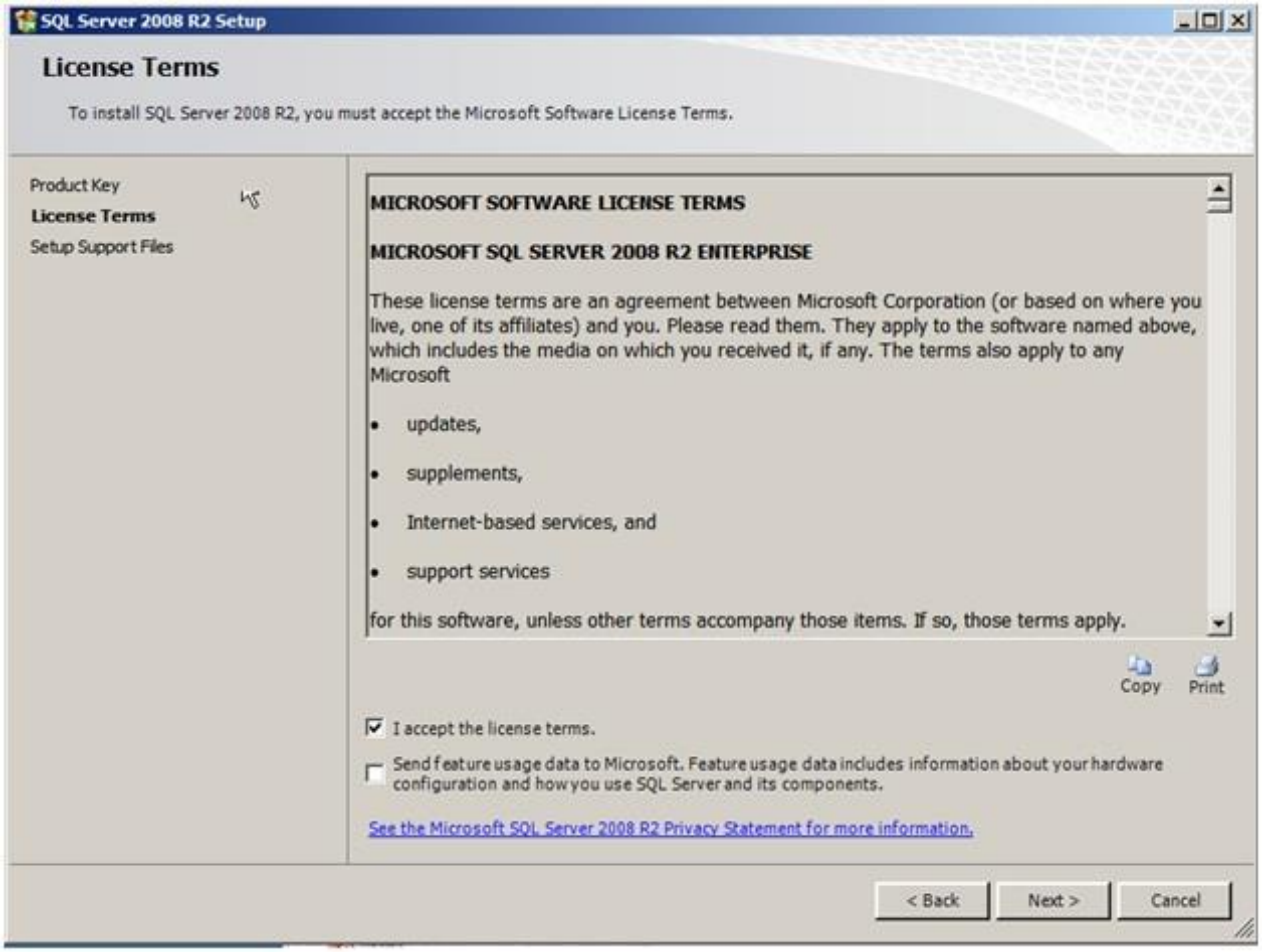
2. On the **Setup Support Rules** page, check that no failures have been reported, and click **Next**.



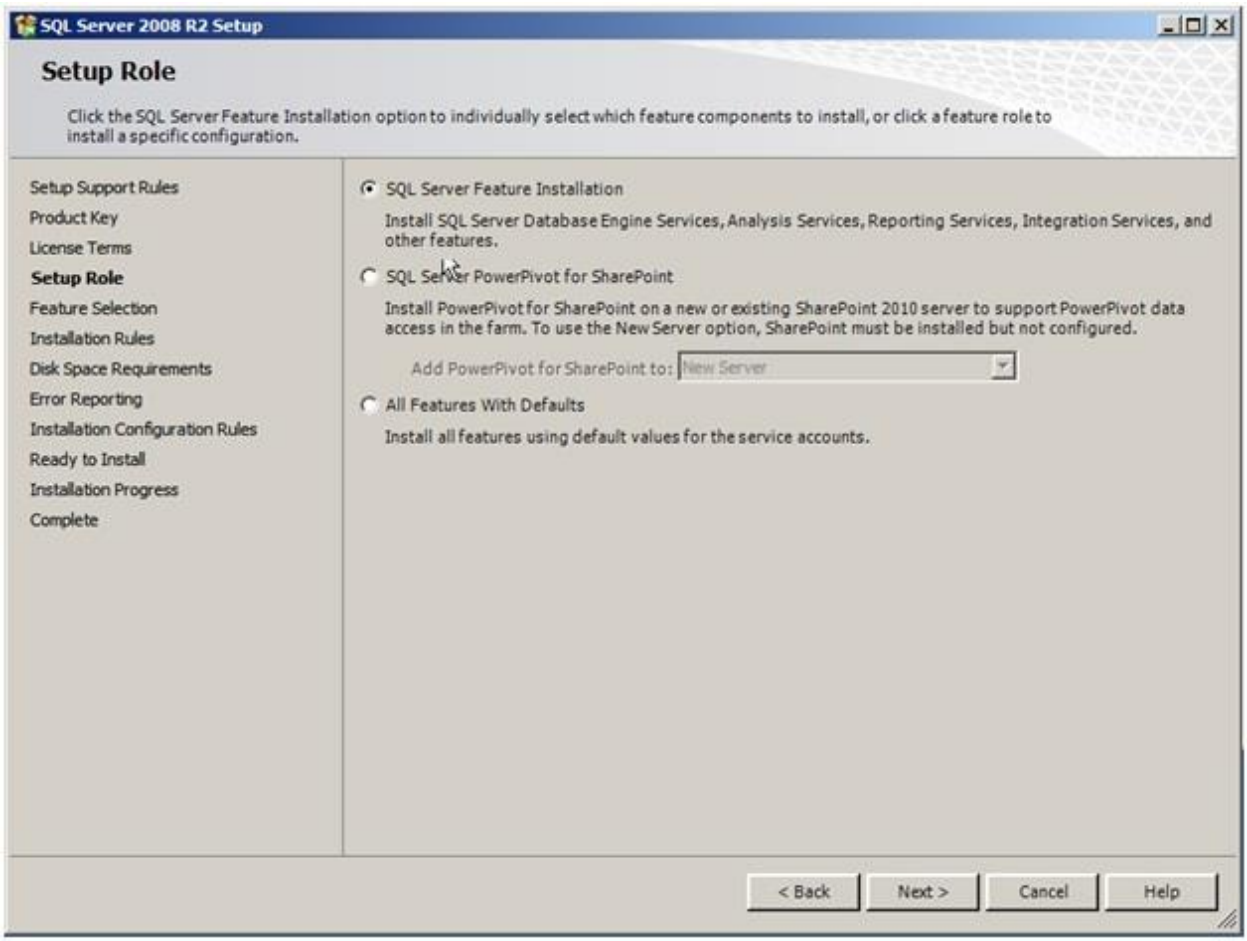
3. Click **Enter the product key**, type the product key, and click **Next**.


SQL Server 2008 R2 Setup
Product Key
Specify the edition of SQL Server 2008 R2 to install.
Product Key
License Terms
Setup Support Files
Validate this instance of SQL Server 2008 R2 by entering the 25-character key from the Microsoft certificate of authenticity or product packaging. You can also specify a free edition of SQL Server, such as Evaluation or Express. Evaluation has the largest set of SQL Server features, as documented in SQL Server Books Online, an is activated with a 180-day expiration. To upgrade from one edition to another, run the Edition Upgrade Wizar
Specify a free edition:
Evaluation
Enter the product key:
< Back
Next >
Cancel

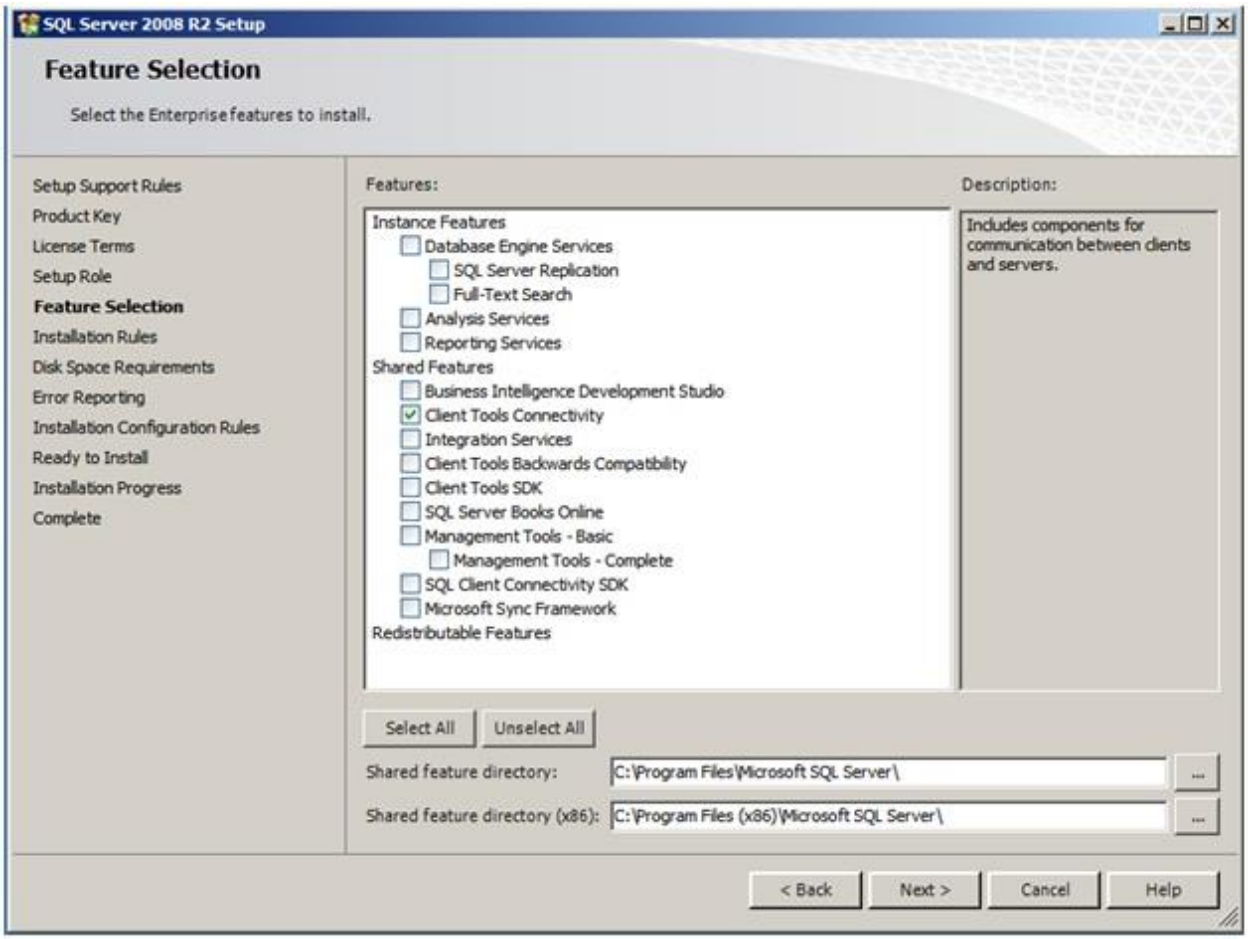
5. Accept the License Terms, and click **Next**.



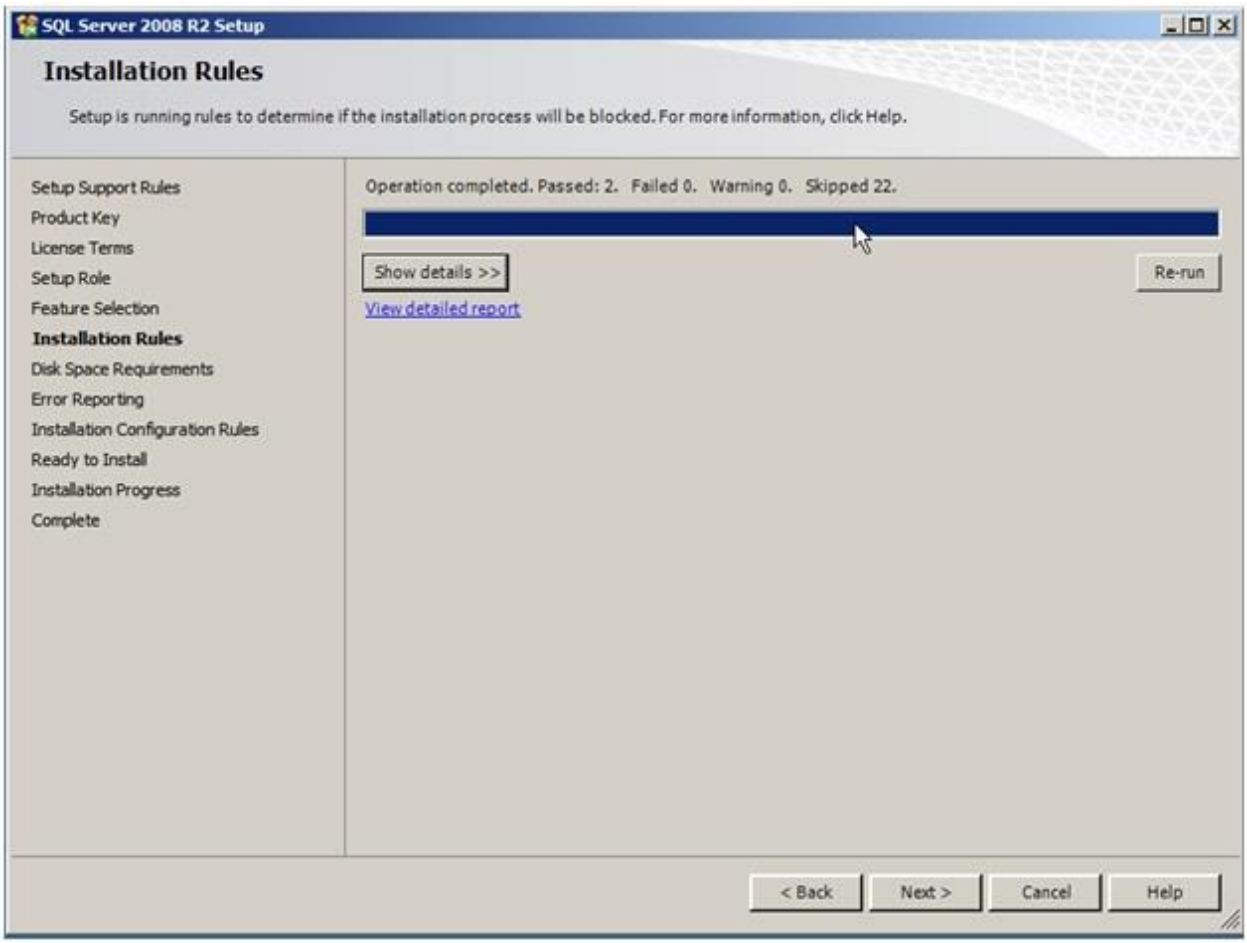
6. On the **Setup Role** page, click **SQL Server Feature Installation**, and click **Next**.



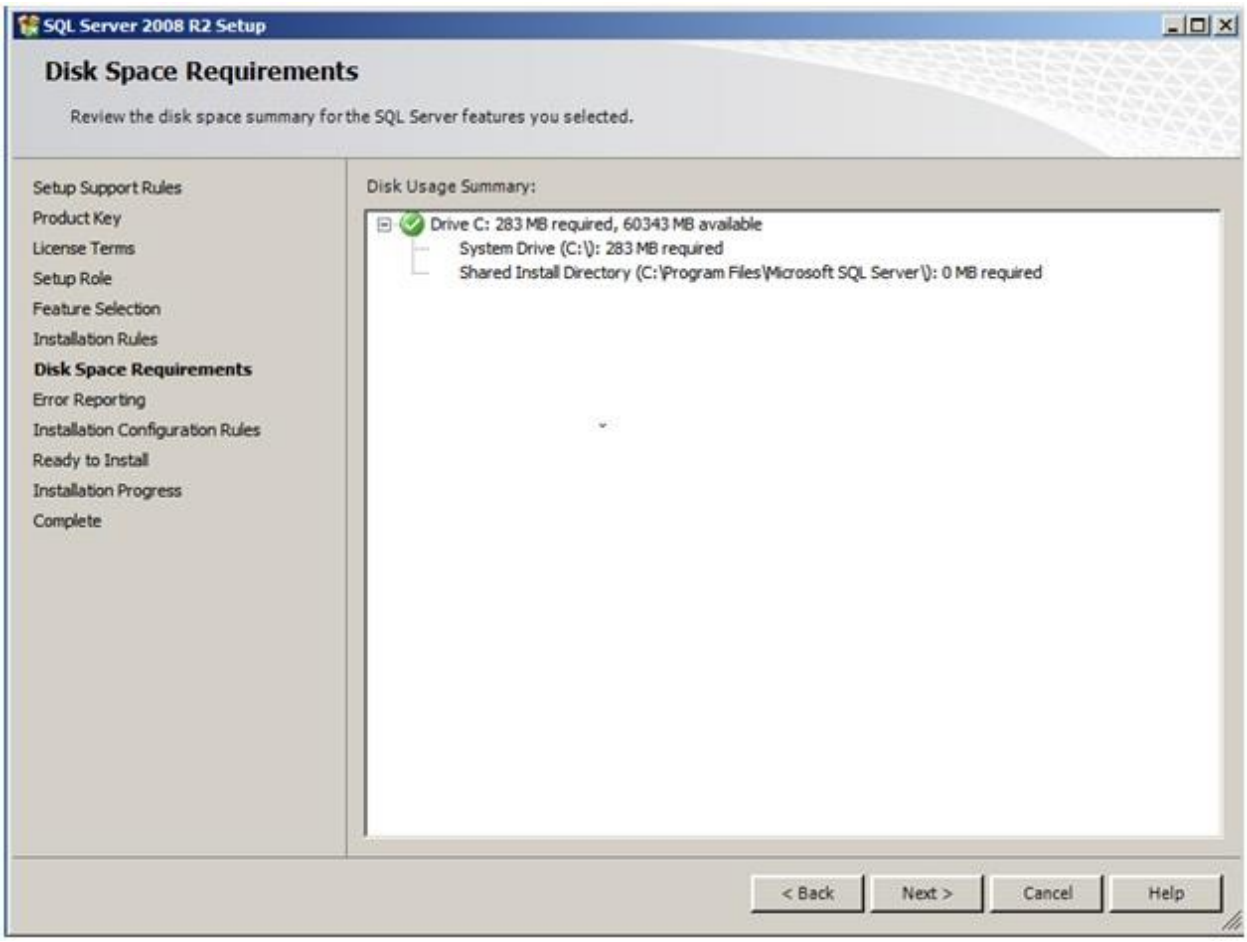
7. On the **Feature Selection** page, select only the check box next to **Client Tools Connectivity**, and click **Next**.



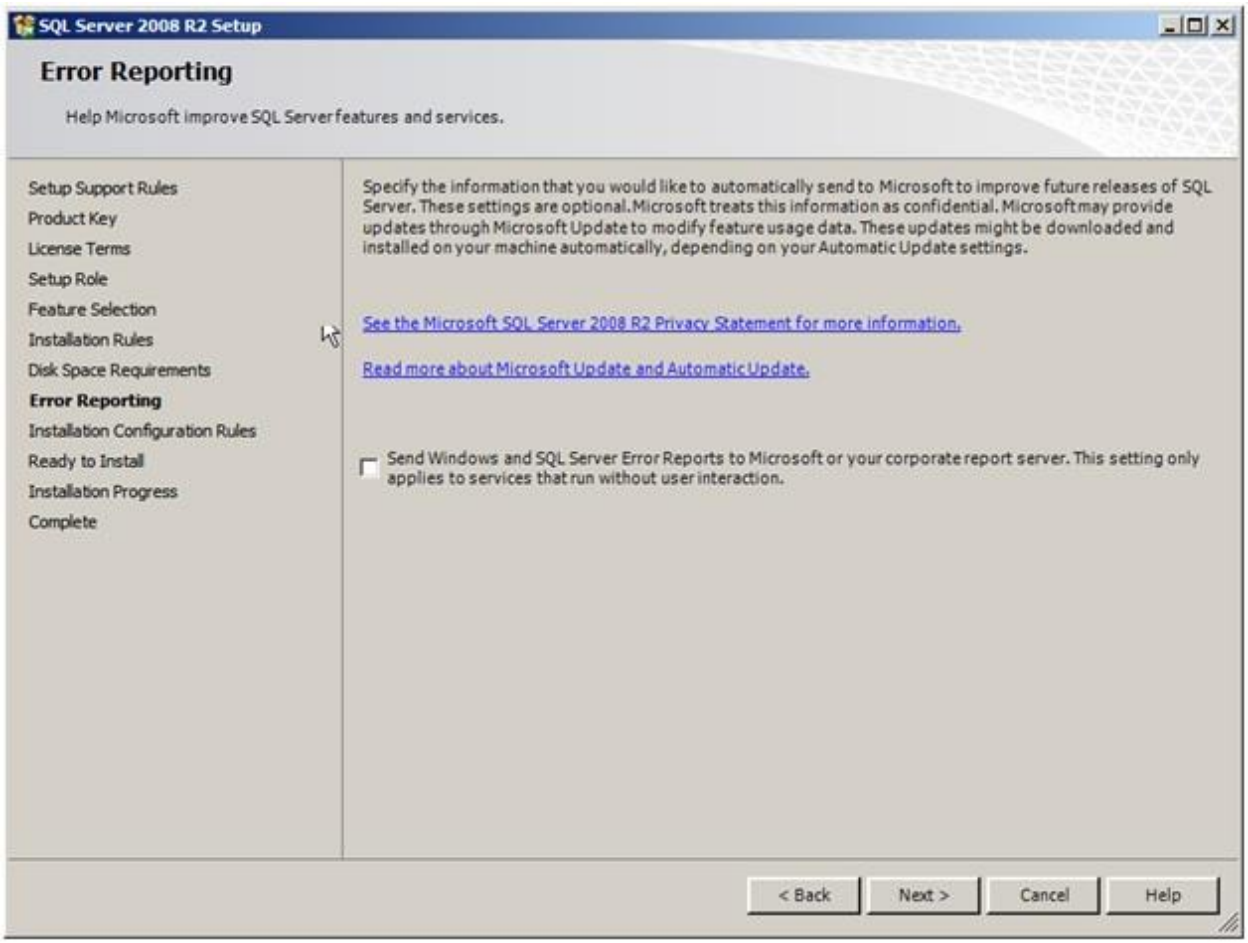
8. On the **Installation Rules** page, ensure that no failures have been reported, and click **Next**.



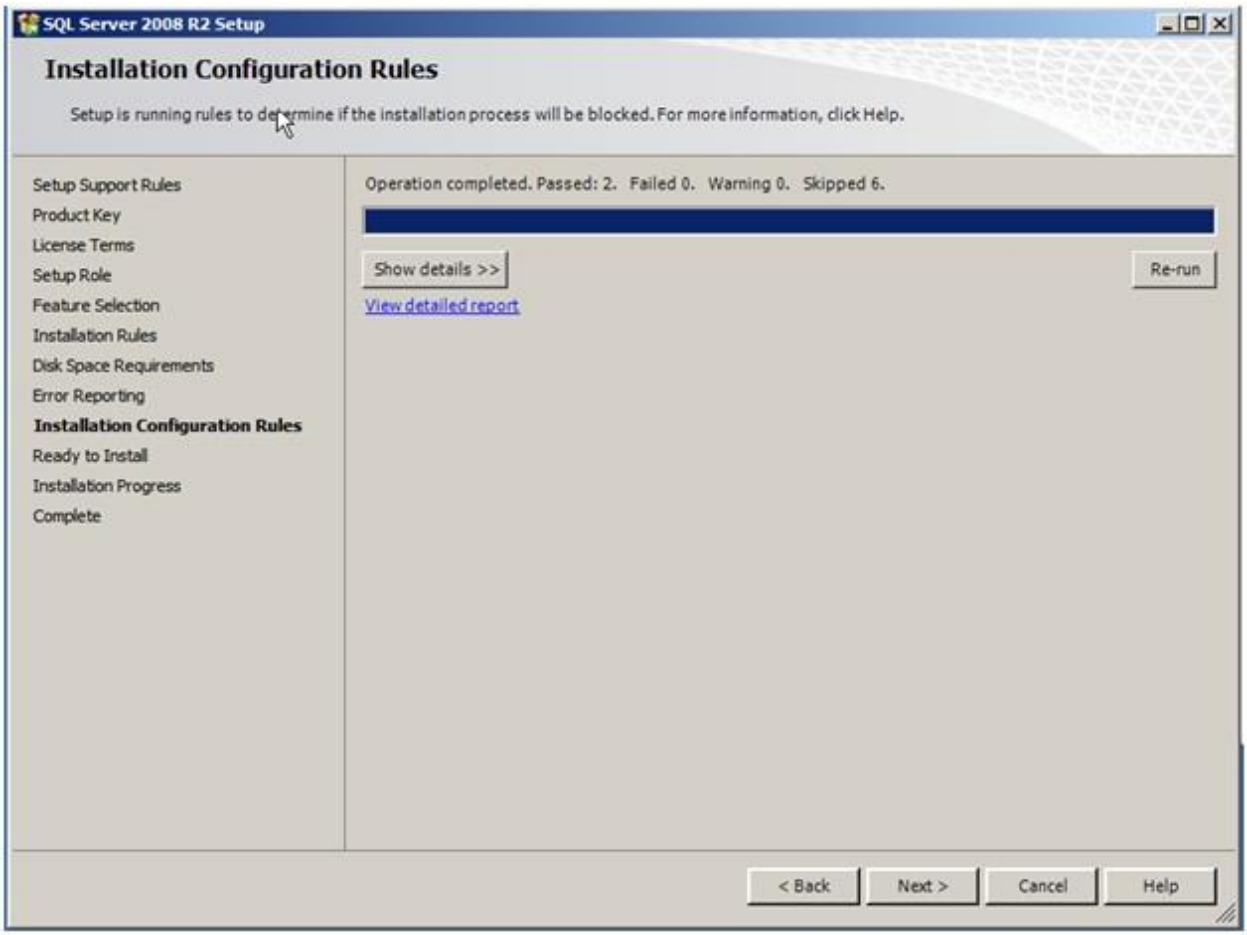
9. On the "Disk Space Requirements" page, click **Next**.



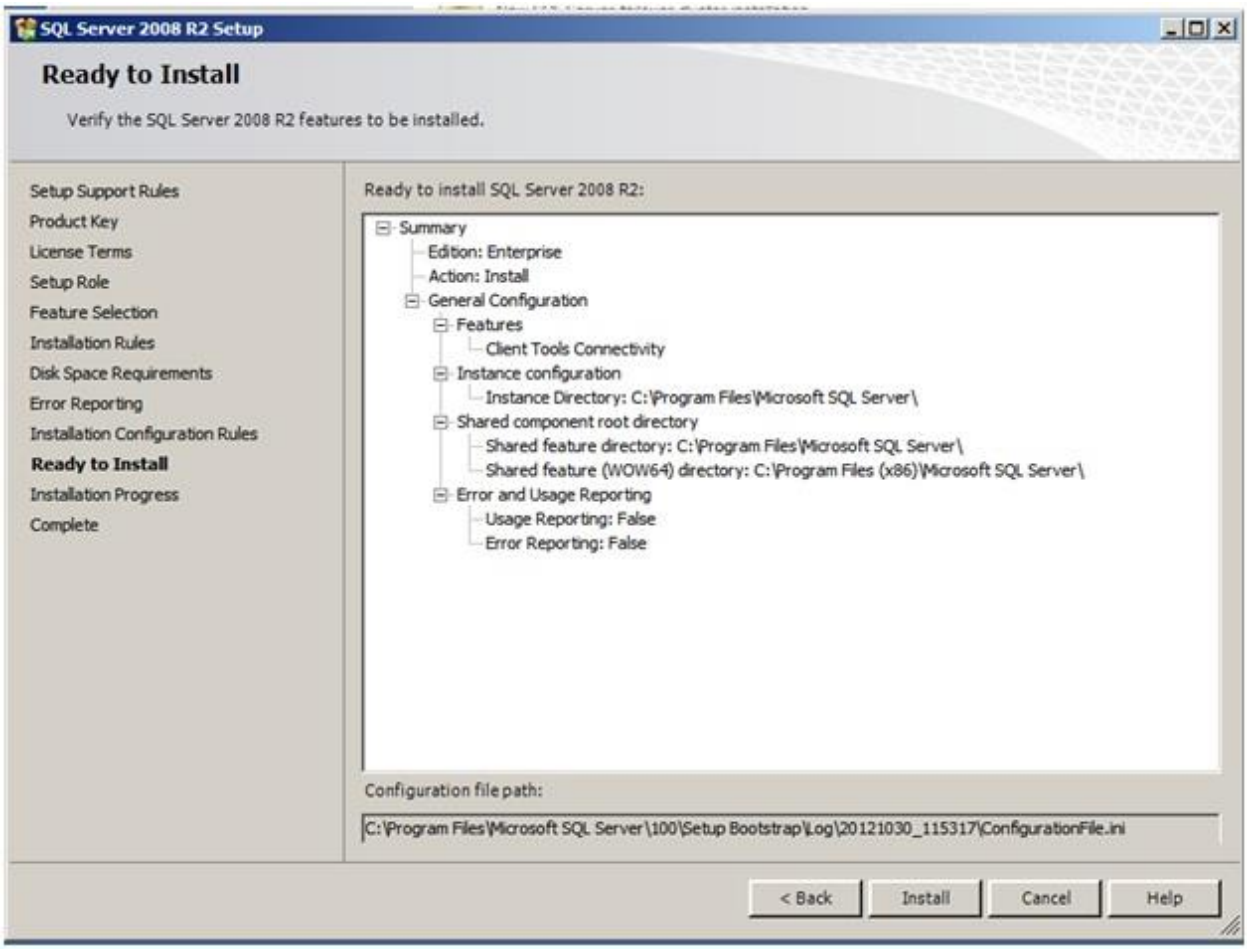
10. On the "Error Reporting" page, click **Next**.



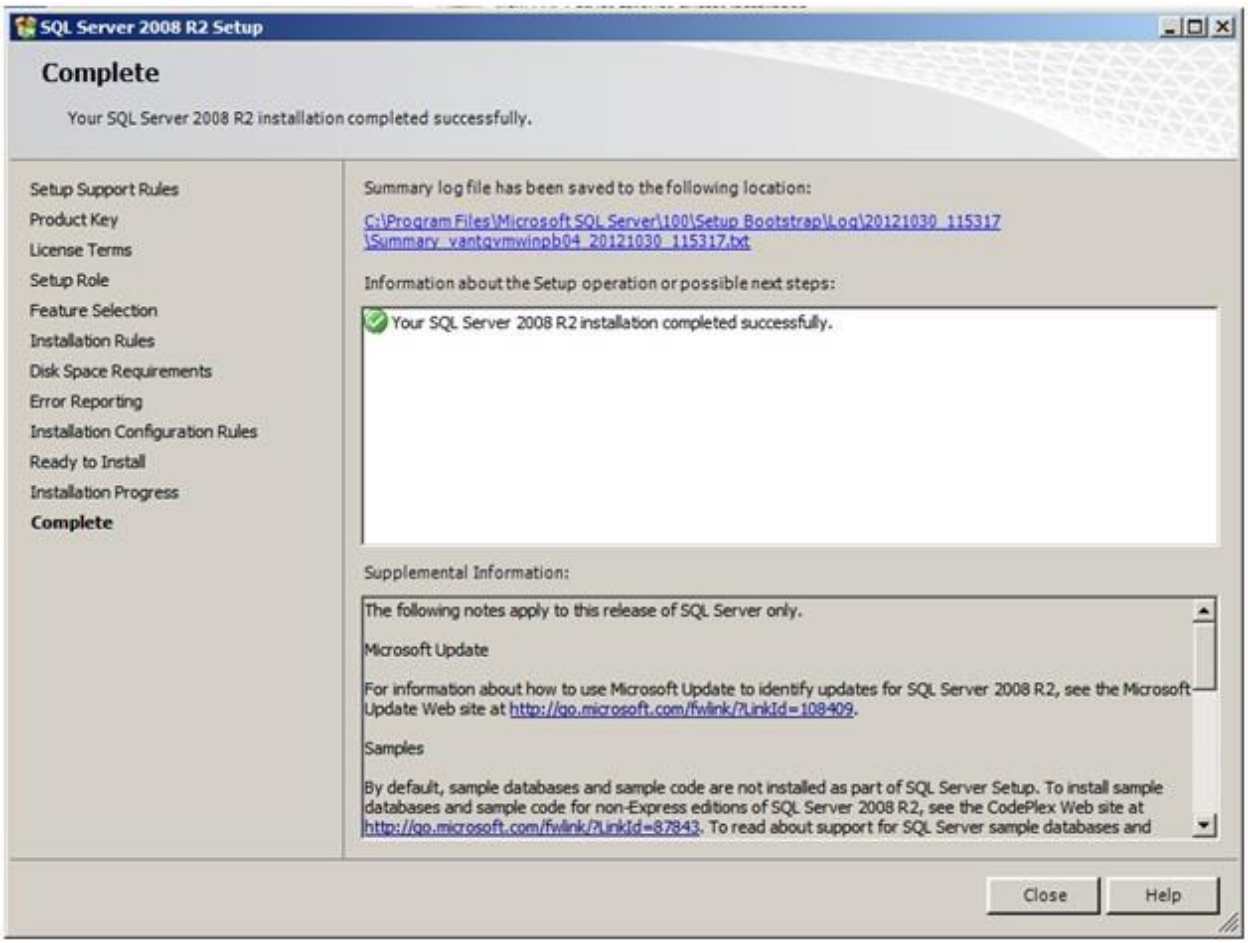
11. Ensure no failures have been reported, and click **Next**.



12. On the **Ready to Install** page, click Install.



13. When the installation is complete, click **Close**.



Setting up OLAP Microsoft Analysis Service through an XMLA connection with SSO

Prerequisites and additional information

The following checklist shows the prerequisite configurations, system rights, and tools you'll need to successfully set up the OLAP connection.

Microsoft Internet Information Services 7.5 (IIS) installed and configured.	✔
Windows Server 2008 R2.	✔
Microsoft SQL Server 2008 R2 with MSAS installed.	✔
Service Account created for setting up the SPN for MSAS.	✔
Service Account granted permissions and assigned a role on MSAS	✔

IIS And MS SQL Server are on the same domain.	✔

- To make a connection to MSAS through TCP/IP, the OLE database must be installed on the same machine that hosts the IIS server. You will need the drivers for Microsoft Analysis Services OLE DB Provider for Microsoft® SQL Server® 2008 R2, which are available at: http://www.microsoft.com/en-us/download/details.aspx?id=16978.
- For information about setting up IIS with Windows 2003, refer to the following Microsoft TechNet article at http://technet.microsoft.com/en-ca/library/gg492140.aspx
    - For general information about configuring IIS, see these Microsoft articles: http://technet.microsoft.com/en-us/library/cc754628%28WS.10%29.aspx http://technet.microsoft.com/en-us/library/cc753473.aspx
    - For a Kerberos configuration checklist, refer to the following blog article: http://blogs.msdn.com/b/psssql/archive/2010/06/23/my-kerberos-checklist.aspx

Workflow

The workflow involves the following tasks:

- Copying the required files from the MSAS server to the IIS server.
- Creating an Application Pool.
- Creating a Virtual Directory.
- Setting up IIS Authentication and adding the requisite extension.
- Setting up a service account for MSAS and IIS, and creating the Service Principal Name (SPN).
- (SPN) Defining the OLAP connection in the Central Management Console (CMC).
- Configuring MDAS (Multi-Dimensional Analysis Services) for the Adaptive Processing Server(s).

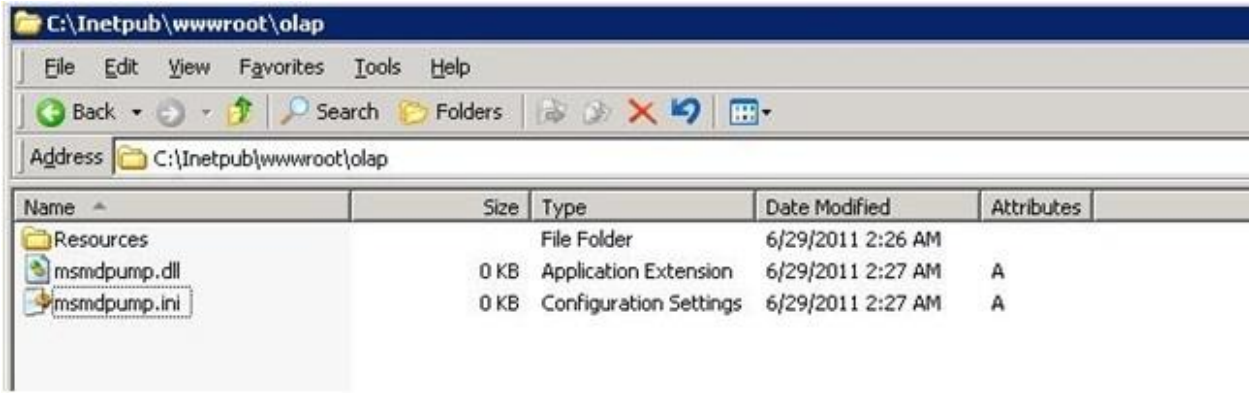
The steps for each of the tasks are shown here. For more background information on the tasks, see http://msdn.microsoft.com/en-us/library/gg492140.aspx.

To create a connection from Analysis for OLAP through XMLA

1. On the Web Server, under the patch c:\inetpub\wwwroot, create a new folder named "OLAP".

2. Go to the folder named "ISAPI", copy the contents of the ISAPI folder, and paste to the "OLAP" folder you created on the previous step.
   For example, on a standard installation of SQL Server 2008 Release 2, copy all files inside C:\Program Files\Microsoft SQL Server\MSAS10_50.MSSQLSERVER\OLAP\bin\isapi, and paste them to c:\inetpub\wwwroot\olap.

   The OLAP folder will have a Resources folder containing two files: msmdpump.dll and msmdpump.ini.



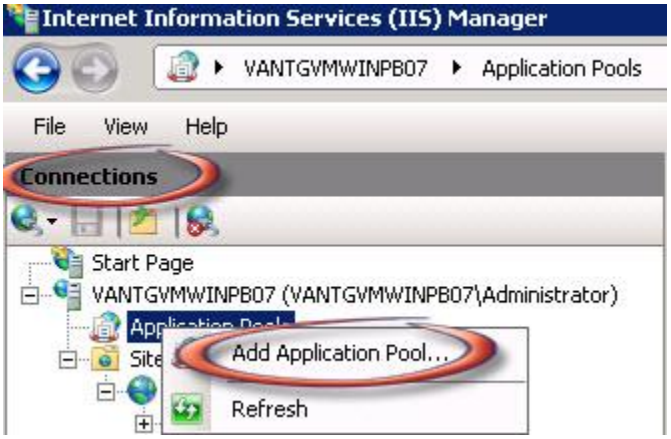
To create an Application Pool

1. Click Start > All Programs > Administrative Tools > Internet Information Services (IIS) Manager.

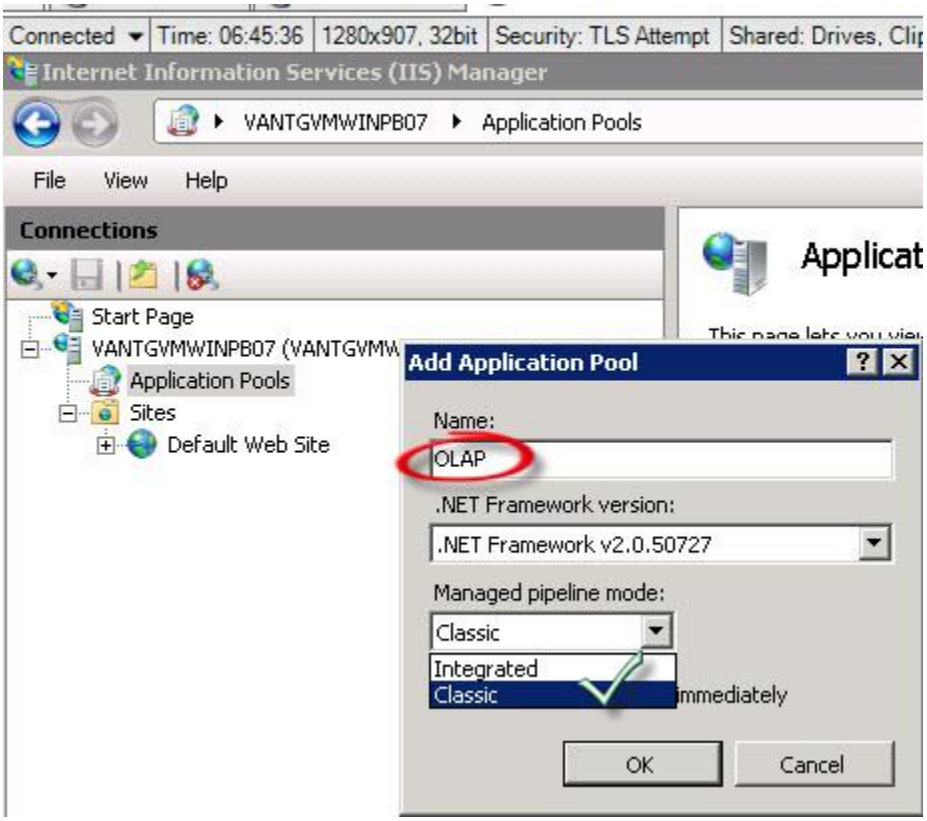
   The "Internet Information Services (IIS) Manager" dialog box opens.

2. In the "Connections" area, expand your server name (VANTGVMWINPB07.BI4PATTERN.COM).
   The "Application Pools" node appears.

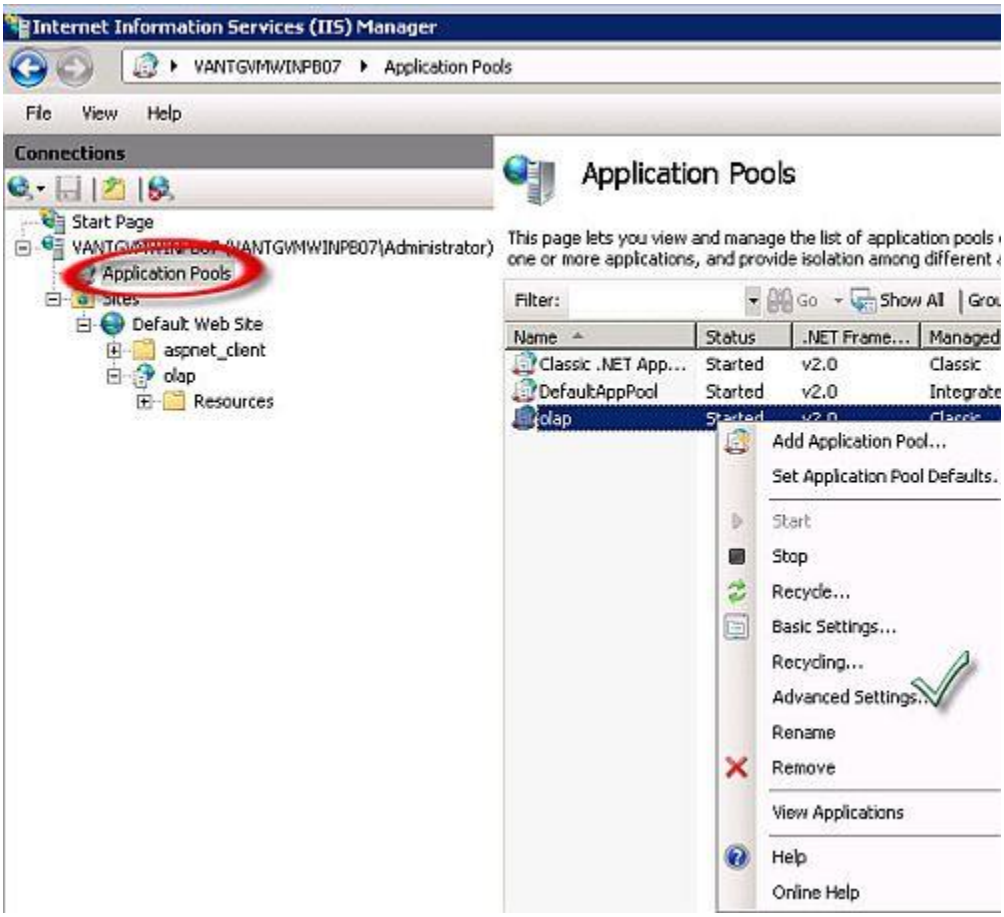
3. Right-click A**pplication Pools**, and select **Add Application Pools.**
   The "Add Application Pool" dialog box opens.



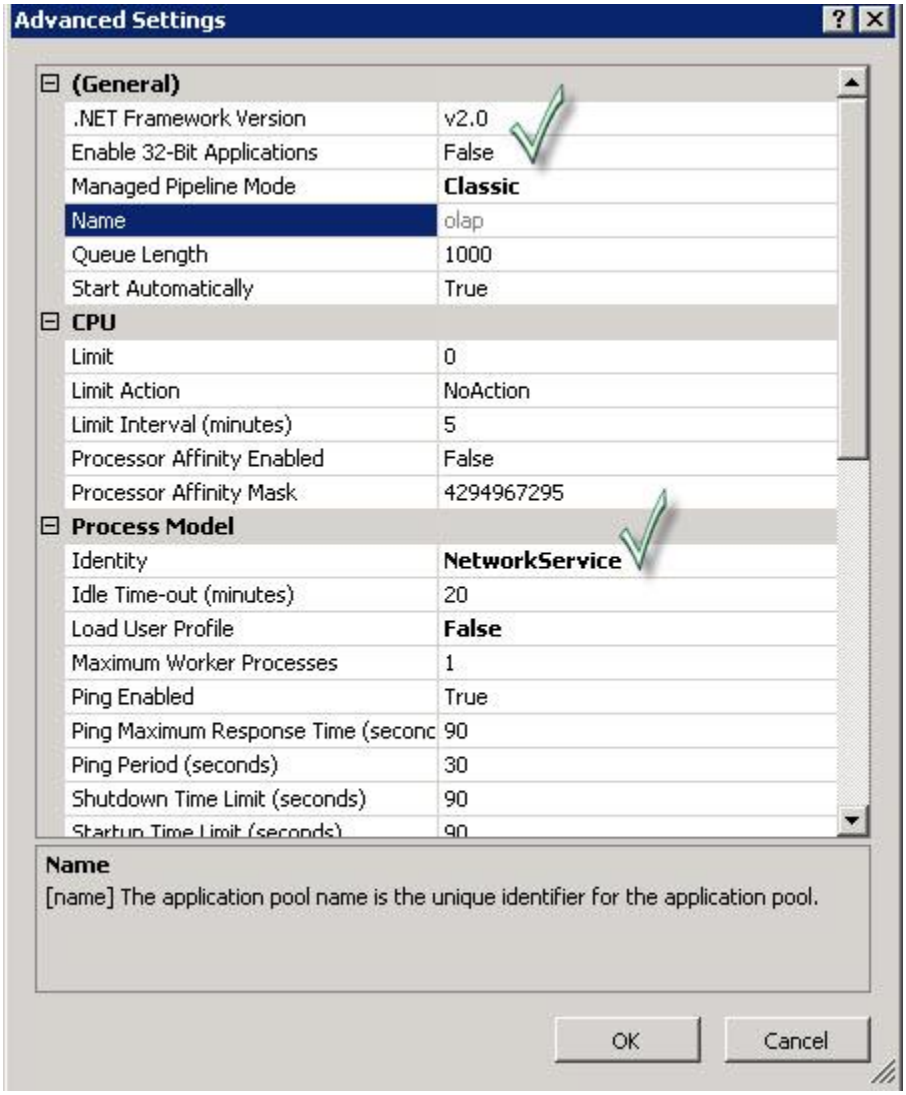
4. In the **Name** box, type **OLAP**, and from the **Managed Pipeline mode** list, select **Classic**.



5. In the .NET Framework version box, select .NET Framework v2.0.50727.
6. Right-click the OLAP application pool and select Advanced Settings.
7. The "Advanced Settings" dialog box opens.



8. In the “General” area, set **Enable 32-Bit Applications** to **False.**

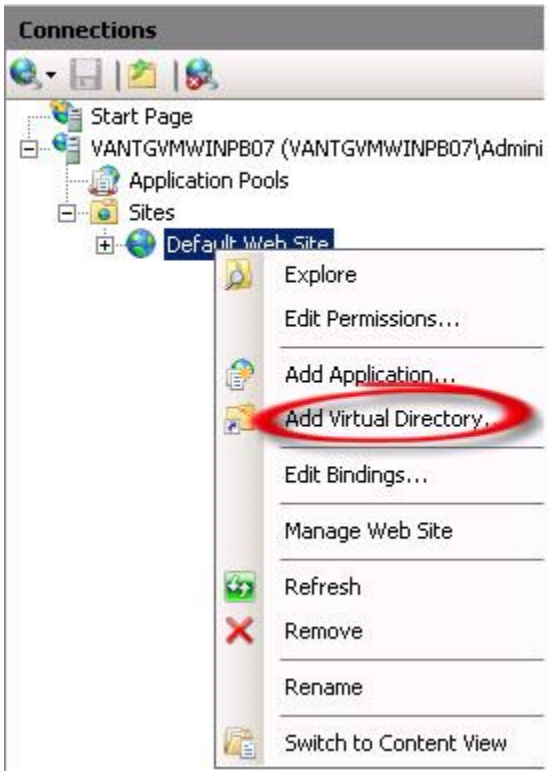


9. In the “Process Model” area, set the Identity to **NetworkService**, and click **OK**.

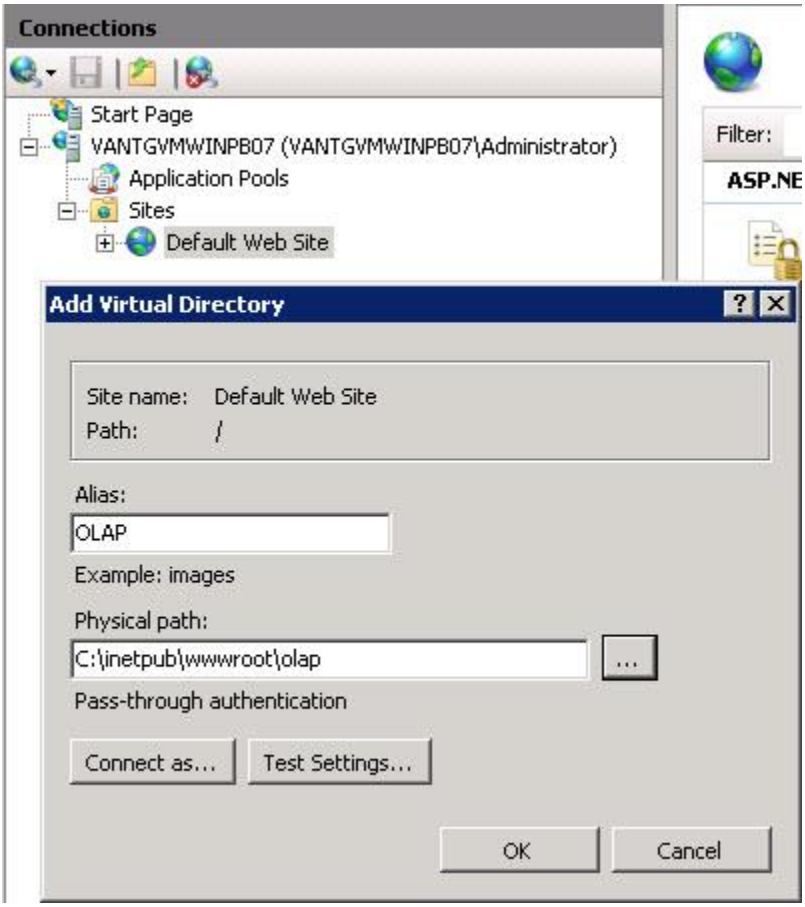
To create a Virtual Directory

1. In IIS Manager, expand **Sites**.
2. Right-click **Default Web Site** (or the name of the site you are using), and select **Add Virtual Directory**.

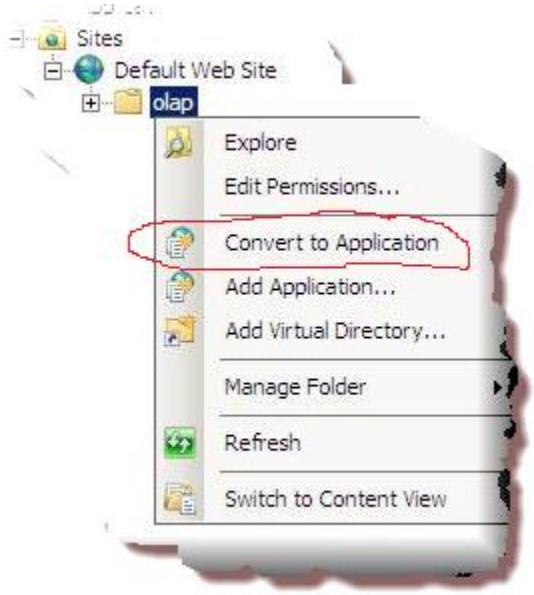
   The "**Add Virtual Directory**" dialog box opens.



3. In the **Alias** box, type **OLAP**.



4. In the **Physical Path** box, browse to **c:\inetpub\wwwroot\olap**, and then click **OK**.
5. When the virtual directory has been added, right-click the **olap** virtual folder, and select **Convert to Application**.

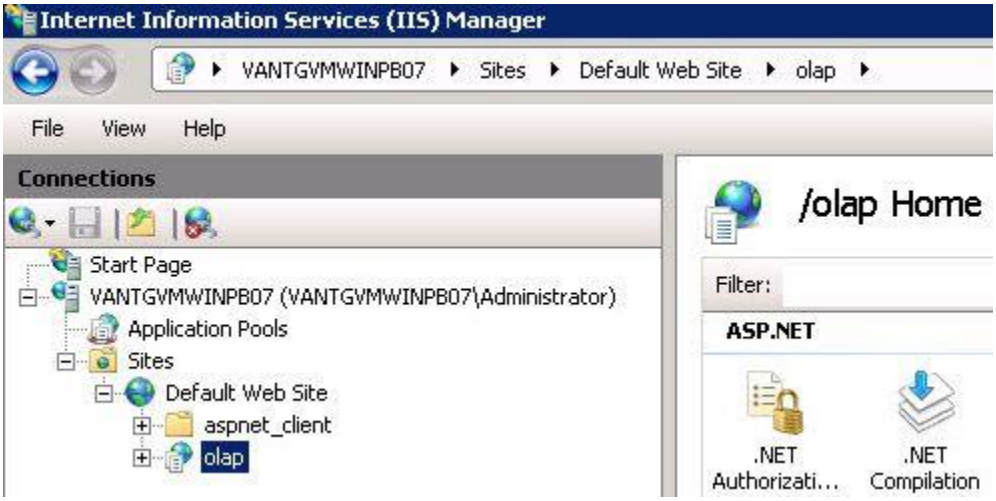


To set up IIS authentication

In this section, you configure further the MSAS virtual directory you just created. You will specify an authentication method, and then add a
script map.

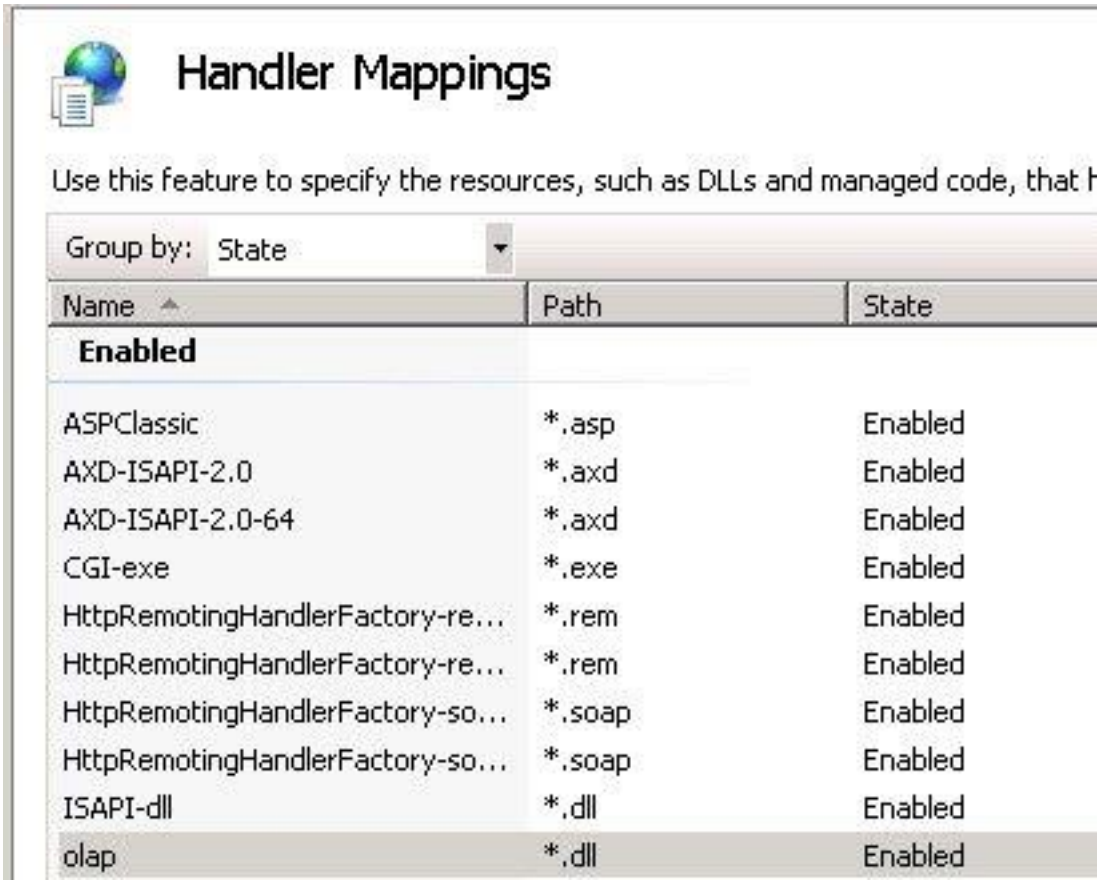
1. In IIS Manager, open **Site**, open **Default Web Site**, and then select the **olap** Virtual directory.

2. In the "IIS" area, double-click **Authentication**.



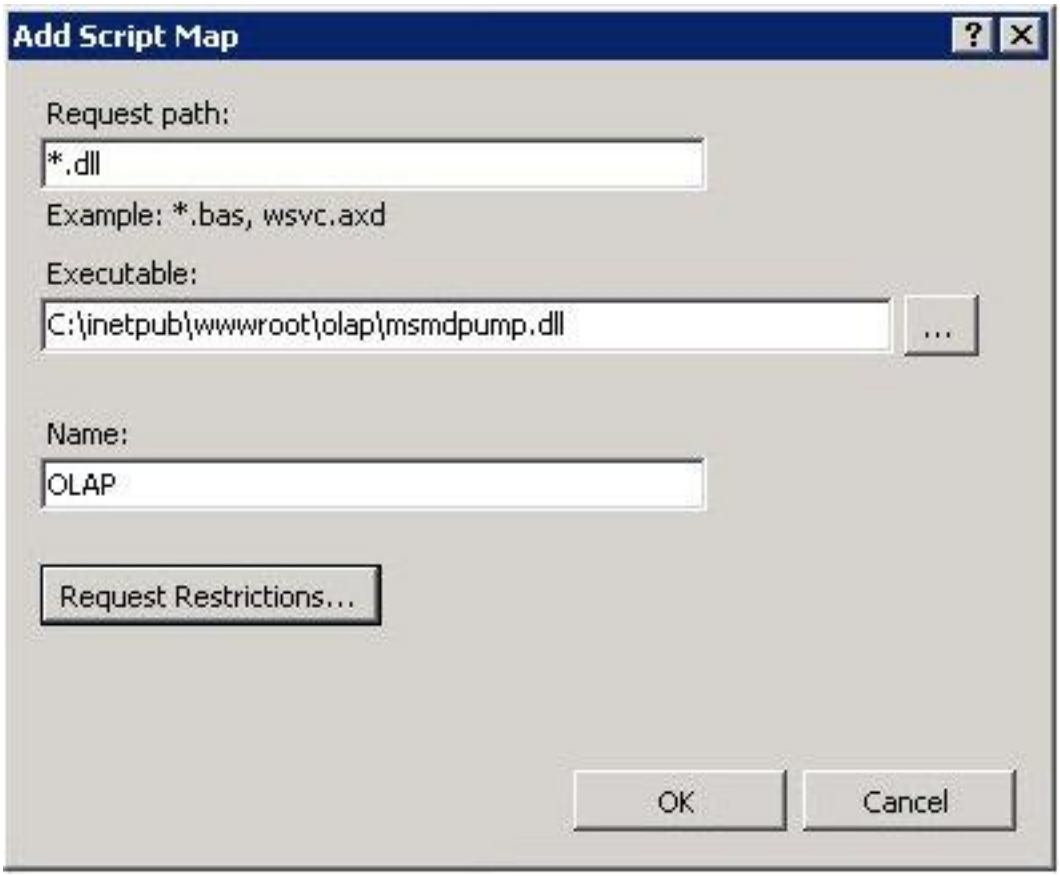
3. Enable **Windows Authentication**.
   Windows authentication is the most secure and recommended authentication. It must be enabled to configure SSO.
   Note: Anonymous Authentication must be set to **disabled**.

4. Click on the **OLAP** virtual directory to open the main page. Double-click **Handler Mappings**.
   The "Handler Mappings" dialog box opens.

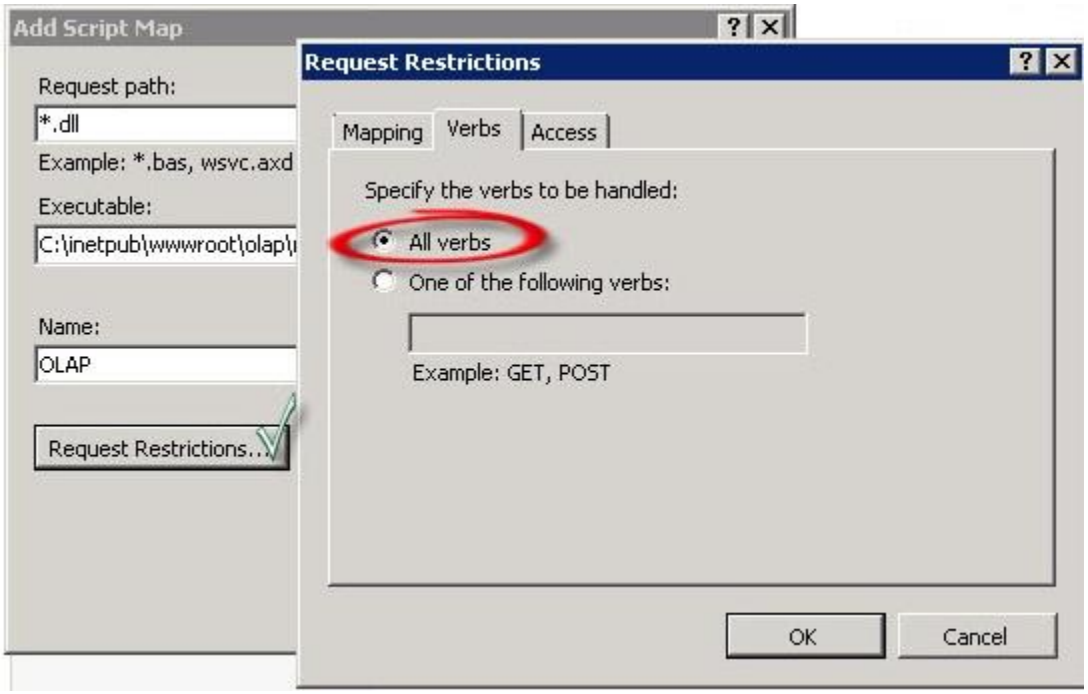


5. Right-click anywhere on the page, and select **Add Script Map**.
   The "Add Script Map" dialog box opens.

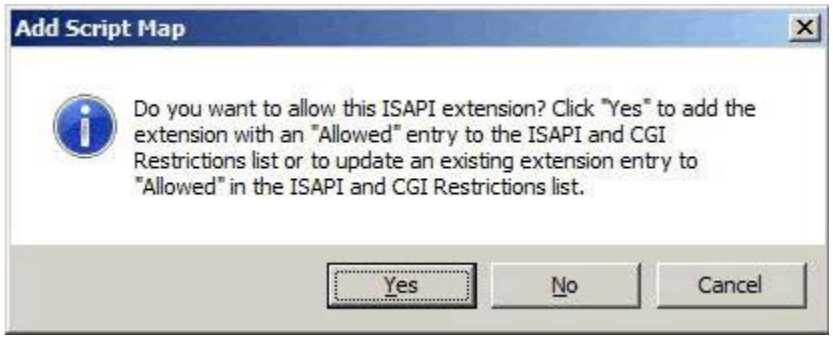
6. In the Add Script Map dialog box, do the following:
   a) In the **Request path** box, type ***.dll**.
   b) In the **Executable** box, type **c:\inetpub\wwwroot\OLAP\msmdpump.dll**
   c) In the **Name** box, type **OLAP**.



7. Click **Request Restrictions.**
   The "Request Restrictions" dialog box opens.
8. On the **Verbs** tab, ensure **All verbs** is selected.



9. Click **OK**, and click **OK** again to finish adding the script mapping.
10. When prompted to allow the ISAPI extension, click **Yes.**



To set up the Service Principal Name (SPN) to enable SSO with MSAS and IIS to Analysis for OLAP

Warning: When a connection is made to a computer that is running Microsoft SQL Server 2008 Analysis Services or Microsoft SQL Server 2005 Analysis Services, and that connection involves a double-hop authentication scenario, you must use Kerberos as the authentication protocol. For example, in a double-hop authentication scenario, a client computer may pass the logon credentials to a computer that is running Microsoft Internet Information Services (IIS). The computer that is running IIS must then pass the logon credentials to the Analysis Services server.

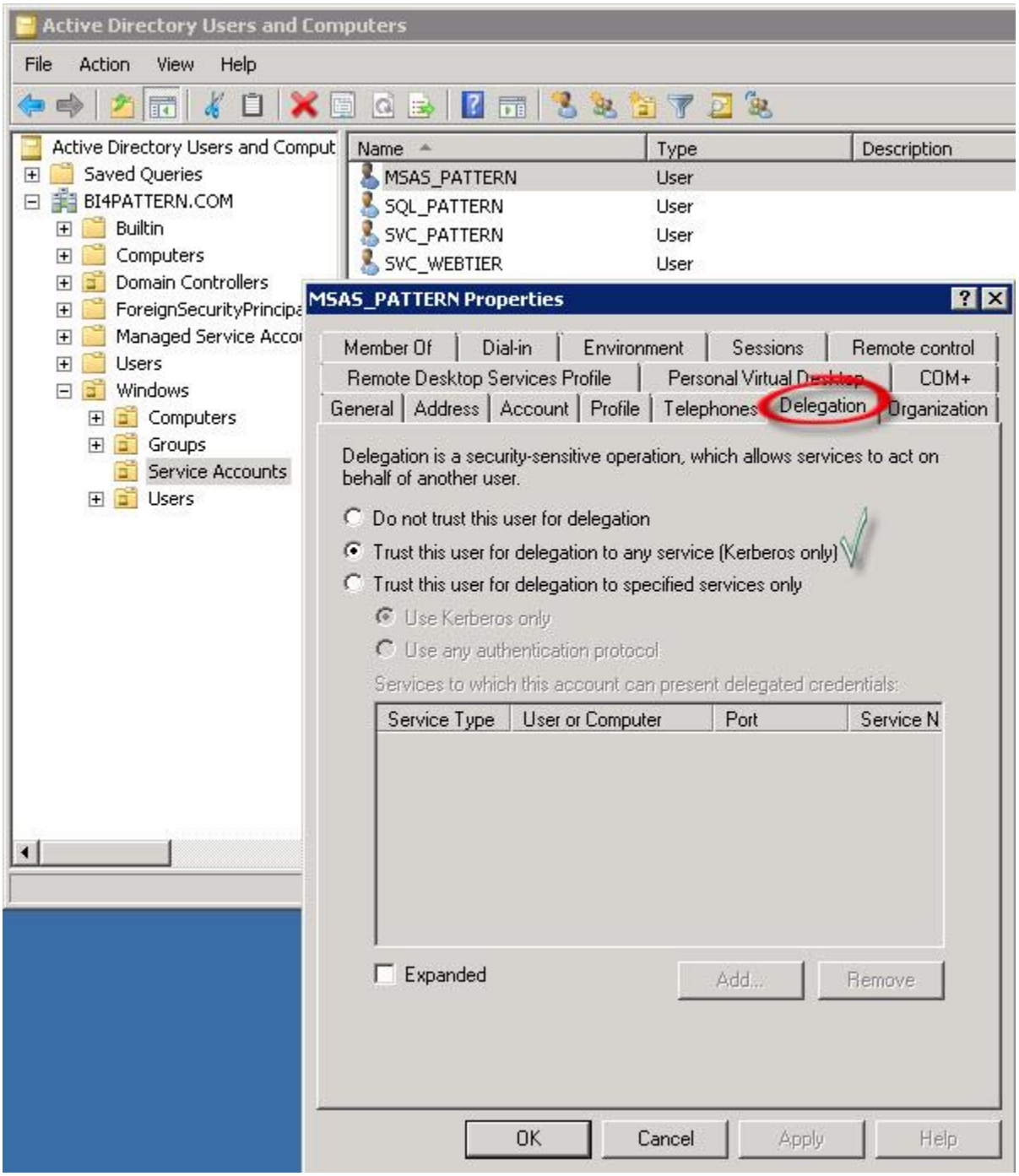
This SPN you create here will establish the Kerberos communication between MSAS and the requests from IIS.

System Prerequisites

- Ensure the servers hosting MSAS and ISS belong to the same Active Directory domain. For example, this pattern has been using
- BI4PATTERN.COM as the domain.
- Ensure a MSAS_PATTERN Service Account is created for running the SSAS Service and for SSO.
- Create an msasuser user account to test for SSAS.
- Ensure the Service Account and the server hosting MSAS are both enabled for Delegation.
- Under the settings for local policy, add the Service Account.
- Ensure Kerberos authentication is set up as shown in this Microsoft KB article: http://support.microsoft.com/kb/917409.

This pattern uses a Service Account named MSAS_PATTERN to run the SSAS service.

1. Click **Start** > **Administrative Tools** > **Active Directory Users and Computers**.
   The "Active Directory Users and Computers" dialog box opens.
2. Click **Service Accounts**.
3. On the Delegation tab, select **Trust this user for delegation to any service (Kerberos only)**.



4. To create the SPN account, in a command prompt window, type the following:

   Setspn.exe -S
   MSOLAPSvc.3/<Fully_Qualified_domainName>.<OLAP_Service_Startup_Account>

5. Replace <Fully_Qualified_domainName> with the fully qualified domain name and <OLAP_Service_Startup_Account> with your
   OLAP Service Account.. This pattern uses the following settings:

* Service Account: MSAS_PATTERN
* MSAS SERVER: vantgvmwinpb07.BI4PATTERN.COM
* IIS SERVER: vantgvmwinpb07.BI4PATTERN.COM

```
C:\>setspn -S  MSOLAPSvc.3/vantgvmwinpb07.BI4PATTERN.COM MSAS_PATTERN
Checking domain DC=BI4PATTERN,DC=COM

Registering ServicePrincipalNames for CN=MSAS_PATTERN,OU=Service Accounts,OU=Win
dows,DC=BI4PATTERN,DC=COM
        MSOLAPSvc.3/vantgvmwinpb07.BI4PATTERN.COM
Updated object
```

6. To create the account for the IIS server, in a command prompt window, type a command for the Fully Qualified Domain Name and a command for the Net Bios Name as follows:

   - setspn -s http/vantgvmwinpb07.BI4PATTERN.COM vantgvmwinpb07.BI4PATTERN.COM
   - setspn -s http/vantgvmwinpb07.BI4PATTERN.COM vantgvmwinpb07

7. To verify that the SPN has been created, do the following:
   a. In a command prompt window, type the following command: setspn -L vantgvmwinpb07

```
Administrator: C:\Windows\system32\cmd.exe

C:\Users\Administrator>setspn -L vantgvmwinpb07
Registered ServicePrincipalNames for CN=VANTGVMWINPB07,OU=Computers,OU=Windows,D
C=BI4PATTERN,DC=COM:
        http/vantgvmwinpb07.BI4PATTERN.COM
        http/vantgvmwinpb07
        TERMSRV/VANTGVMWINPB07
        TERMSRV/vantgvmwinpb07.BI4PATTERN.COM
        WSMAN/vantgvmwinpb07
        WSMAN/vantgvmwinpb07.BI4PATTERN.COM
        RestrictedKrbHost/VANTGVMWINPB07
        HOST/VANTGVMWINPB07
        RestrictedKrbHost/VANTGVMWINPB07.BI4PATTERN.COM
        HOST/VANTGVMWINPB07.BI4PATTERN.COM
```

   b. In a command prompt window, type the following command: setspn -L MSAS_PATTERN

```
C:\>setspn -L MSAS_PATTERN
Registered ServicePrincipalNames for CN=MSAS_PATTERN,OU=Service Accounts,OU=Wind
ows,DC=BI4PATTERN,DC=COM:
        MSOLAPSvc.3/vantgvmwinpb07.BI4PATTERN.COM
```

   c. You are now able to create an OLAP Connection from the CMC to MSAS 2005-08 for use with SSO, provided you have set up SSO with BI Launchpad. You can otherwise test your configuration by using Windows AD Authentication manually.

To configure MDAS and the hosting Adaptive Processing Server (APS)

To set up end-to-end SSO with Microsoft Analysis Server and BI 4.0 Analysis Edition for OLAP you need to create keytab file and APS hosting the MDAS server on BI platform. Modifications need to be made to ensure the APS hosting to the MDAS recognizes the following files: bscLogin.conf and Krb5.ini. You will add extra parameters to the bsclogin.conf file.

Warning: The keytab file needs to be copied to C:\Windows Folders where the MDAS server is being deployed.

This section shows how to do the following steps:

- Create the keytab file with the ktpass command.
- Add the server parameters to bsclogin.conf.
- Ensure the APS that is hosting the MDAS recognizes the bscLogin.conf and Krb5.ini files.

To create the keytab file using the ktpass command

In a command prompt window, type the following:

```
ktpass -out bosso.keytab -princ service-account-spn@REALM -mapuser service-account-<name@REALM --pass service-account-
password
-ptype KRB5_NT_PRINCIPAL -crypto RC4-HMAC-NT
```

The keytab for the Windows pattern will look as follows:

```
ktpass -out bosso.keytab -princ BICMS/svc_pattern.BI4PATTERN.COM@BI4PATTERN.COM
-mapuser svc_pattern@BI4PATTERN.COM -pass Pattern123 -ptype KRB5_NT_PRINCIPAL
-crypto RC4-HMAC-NT /target BI4PATTERN.COM
```

To ensure the APS that is hosting the MDAS recognizes bscLogin.conf and Krb5.ini

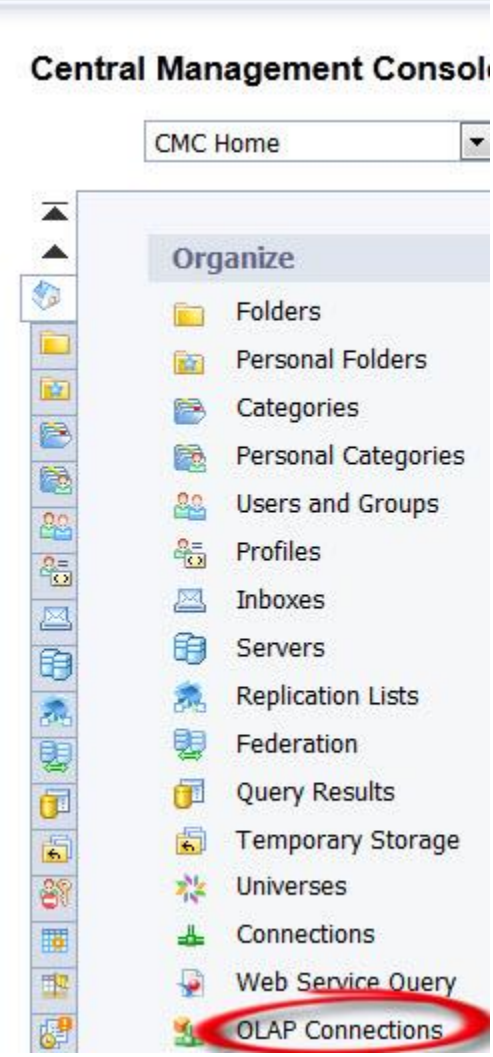
The Adaptive Processing Server (APS) running the Multi-Dimensional Analysis Service (MDAS) must be set to recognize the configuration files bscLogin.conf and krb5.ini. The path to bscLogin.conf must always be specified, and by default the APS searches for krb5.iniin C:\Windows. However, it is recommended to explicitly specify the search locations, in case the default search location is changed by third-party software.

1. Add the following argument to the command line of APSs running the MDAS service: -Djava.security.auth.login.config=C:/Windows/bscLogin.conf -Djava.security.krb5.conf=C:/Windows/krb5.ini

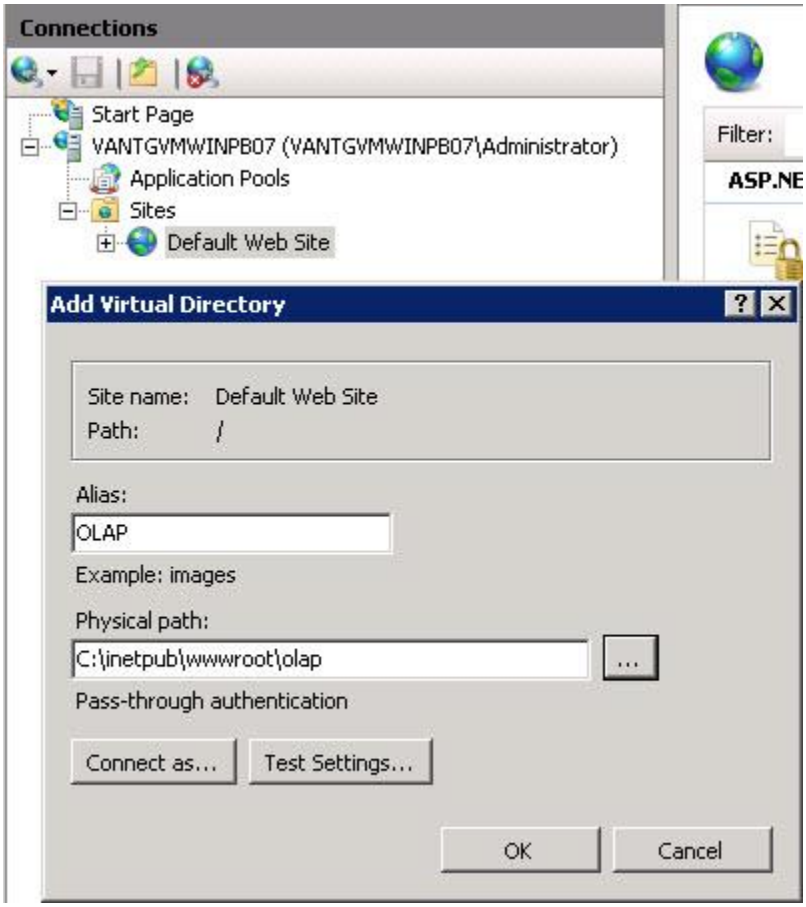
To verify the SSO connection from BI Launchpad

Test the connection from the BI Platform CMC OLAP connection.

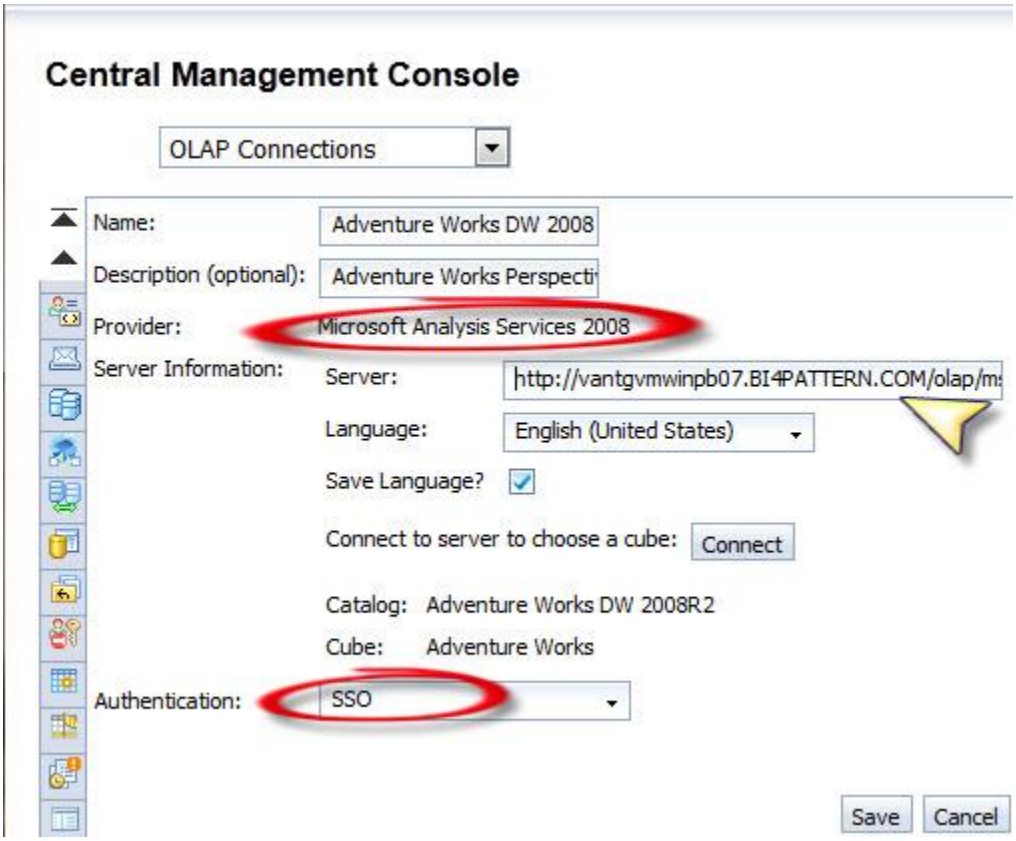
1. To open the CMC, click **Start** > **All Programs** > **SAP BusinessObjects BI platform 4.0** > **SAP BusinessObjects BI platform** > **SAP BusinessObjects BI platform Central Management Console**.
   The login page appears.
2. After you have logged in to the CMC, in the **Organize** list, click **OLAP Connections**.



3. Click the New connection icon.



4. In the Name box, type a name for the connection, and in the Description box provide additional details.
5. In the Provider list, choose a data provider.
   For SSAS, currently Microsoft Analysis Services 2005 and Microsoft Analysis Services 2008 are supported.



6. In the **Server Information** box, enter the URL path to msmdpump.dll.
   If you have been using the examples suggested in this pattern, the URL will be http:<IIS servername>/olap/msmdpump.dll, where <IIS servername> is the name of the IIS server that has been configured.

Setting up Single Sign on (SSO) with MSSQL Server OLTP

Perquisites and Workflow

Before setting up SSO with SQL Server 2008 Release 2, you will need the following:

Prerequisites
Windows Server 2008 R2
Microsoft SQL Server 2008 R2 installed
A "**SQL_PATTERN"** service Account specifically set up for this pattern

Prerequisites
A machine that hosts SQL Server 2008 Release 2 and that is on the same domain as your BI platform deployment
The following machine name: **vantgvmwinpb07.dhcp.pgdev.sap.corp**

Workflow

Setting up SSO with SQL Server 2008 Release 2 involves the following tasks:

- Changing the MSSQLSERVER account to "SQL_PATTERN
- Setting up a Service Principle Name (SPN).
- Enabling the Delegation settings for the SPN.
- Verifying through the local security policy settings that the account impersonation is in effect.

Verifying the service account through a connection test

To check which account is running the MSSQLSERVER, on the machine that is running SQL Server 2008 Release 2. # In the Start menu, click **Run** then type *services.msc* in the dialog prompt, click **OK**. The Services screen opens.

1. Look up and double-click the Service SQL Server (MSSQLSERVER) service.

2. Select the **Log On** tab.
3. Click this account: option and provide the information for the "SQL_PATTERN" service account.

To create the SPN account

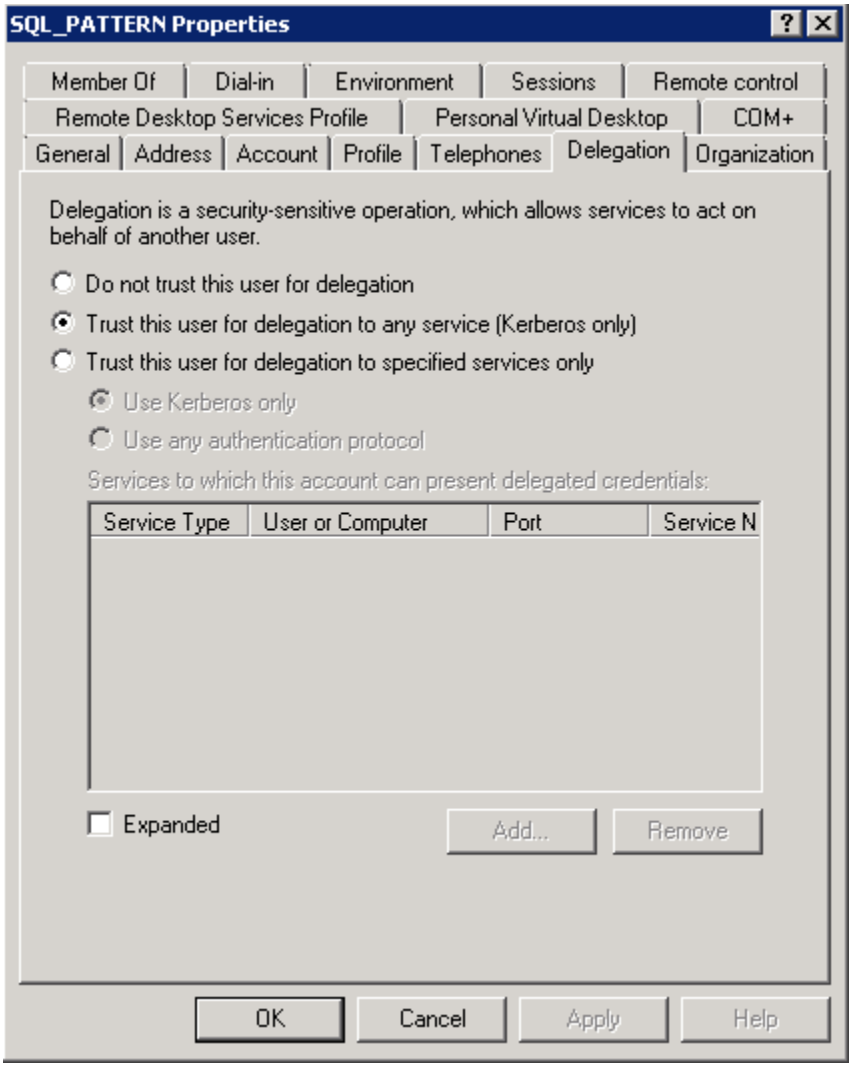
Open a Command Prompt window, and type the following:
C:\Users\Administrator>**setspn.exe -A MSSQLSvc/vantgvmwinpb07.BI4PATTERN.COM:1433 SQL_PATTERN**

1. Run the command, the following output should appear:

```
C:\Users\Administrator>setspn.exe -A MSSQLSvc/vantgvmwinpb07.BI4PATTERN.COM:1433
 SQL_PATTERN
Registering ServicePrincipalNames for CN=SQL_PATTERN,OU=Service Accounts,OU=Wind
ows,DC=BI4PATTERN,DC=COM
        MSSQLSvc/vantgvmwinpb07.BI4PATTERN.COM:1433
Updated object
```

To set up trust delegation for the service account

1. Click on **Active Directory Users and Computer** and navigate to**Service Accounts** Properties.
2. Double-click "**SQL_PATTERN Properties**". The following dialog opens:
3. Click the Delegation tab.
4. Select **Trust this user for delegation to any service (Kerberos only)**, and click **OK.**



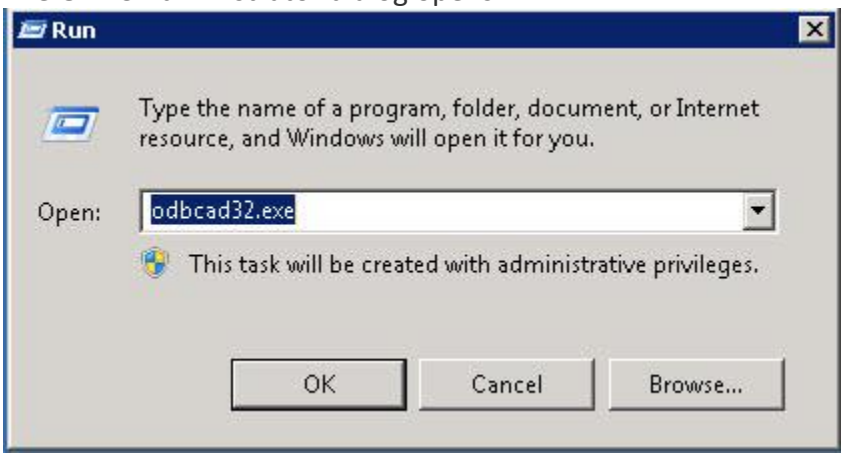
To check that account impersonation is in effect

1. Open a command prompt and type:
   mmc >
2. Click the File menu, select Open and navigate to:
   C**:\Windows\System32\secpol.msc**
   The Local Security Policy dialog opens.
3. Click Local Policies>User Rights Assignment.
4. Locate and select the **Impersonate a client after impersonation** right.

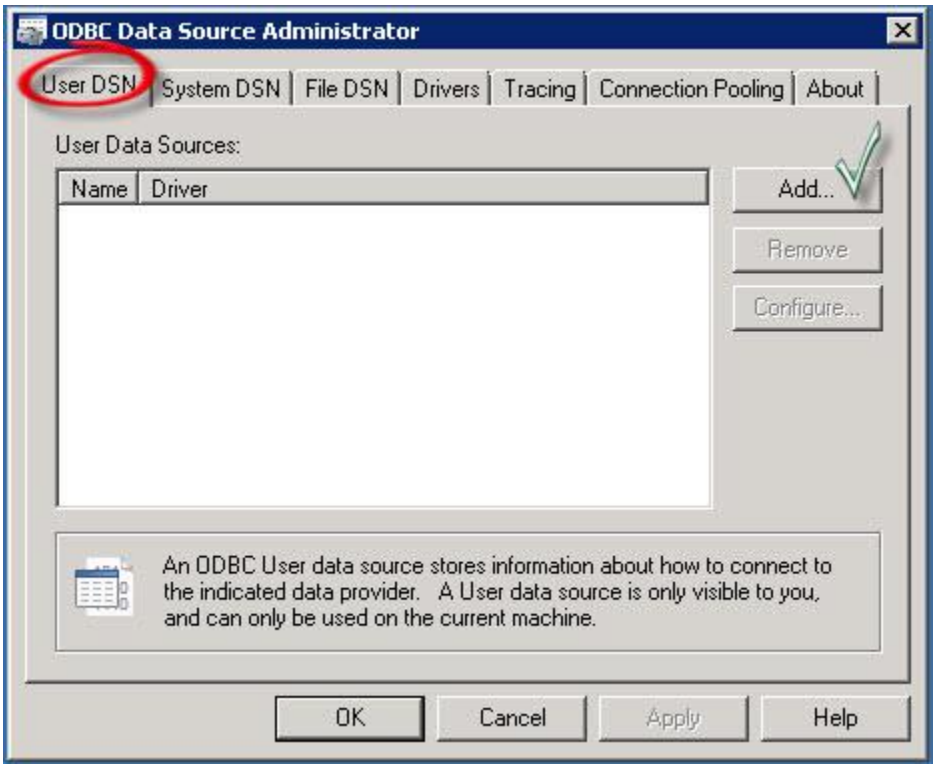
5. Check that the **Service Account** has been added to the list.

To perform a connection test with the service account

1. In a command prompt type *odbcad32.exe* and click **OK.**
   The ODBC Administrator dialog opens.

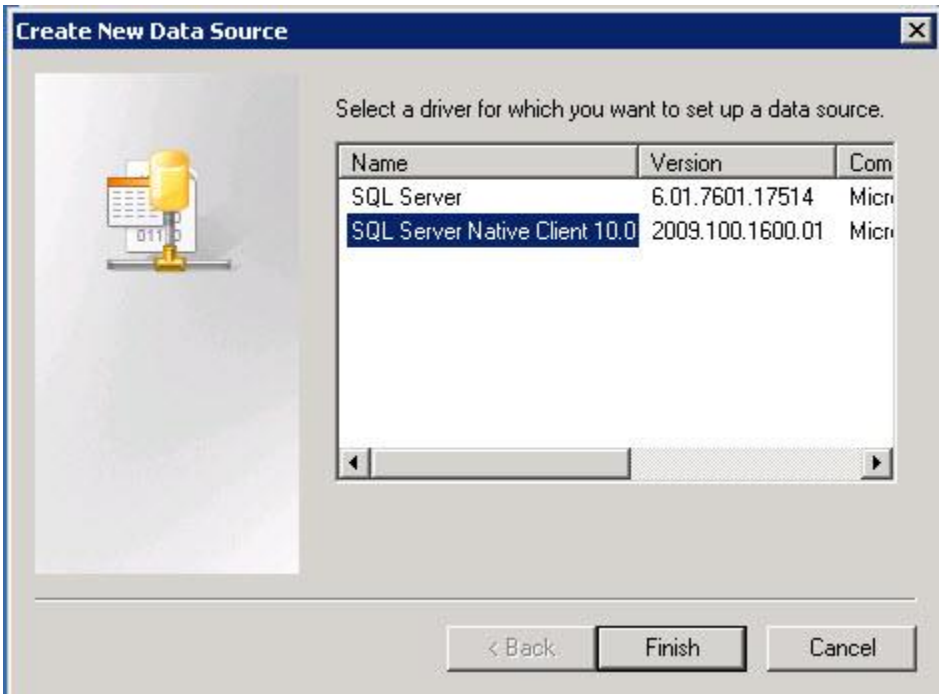


2. Click the **User DSN** tab and select **Add**.

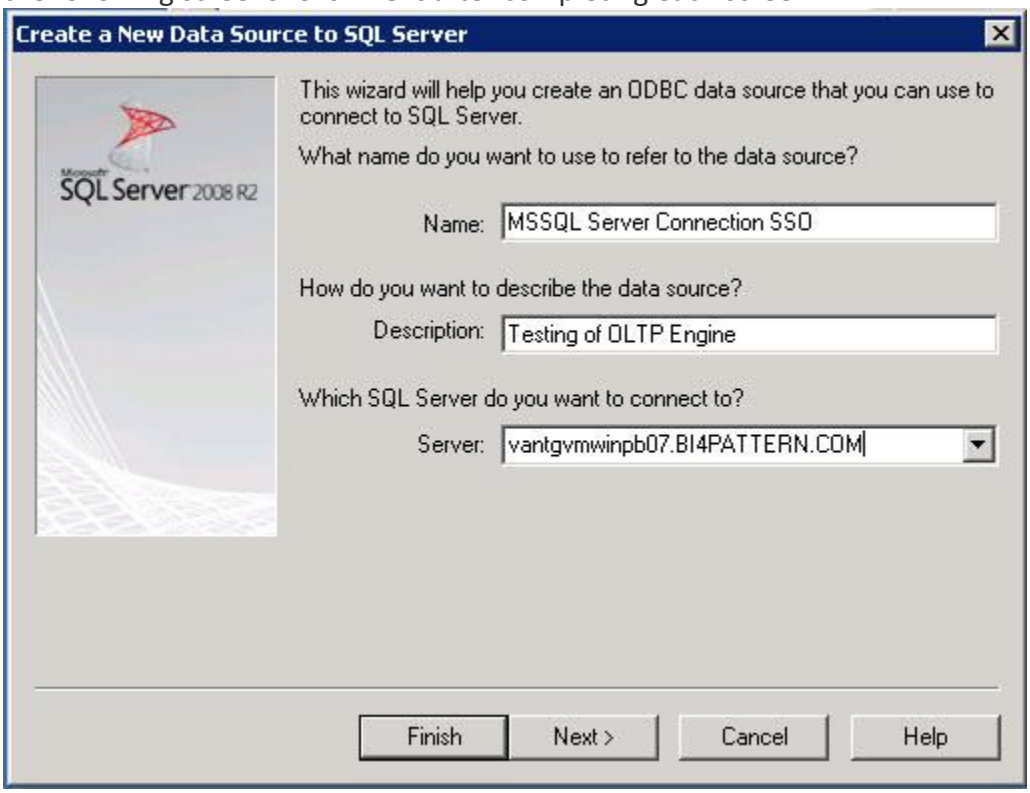


   The "**Create New DataSource"** dialog opens.

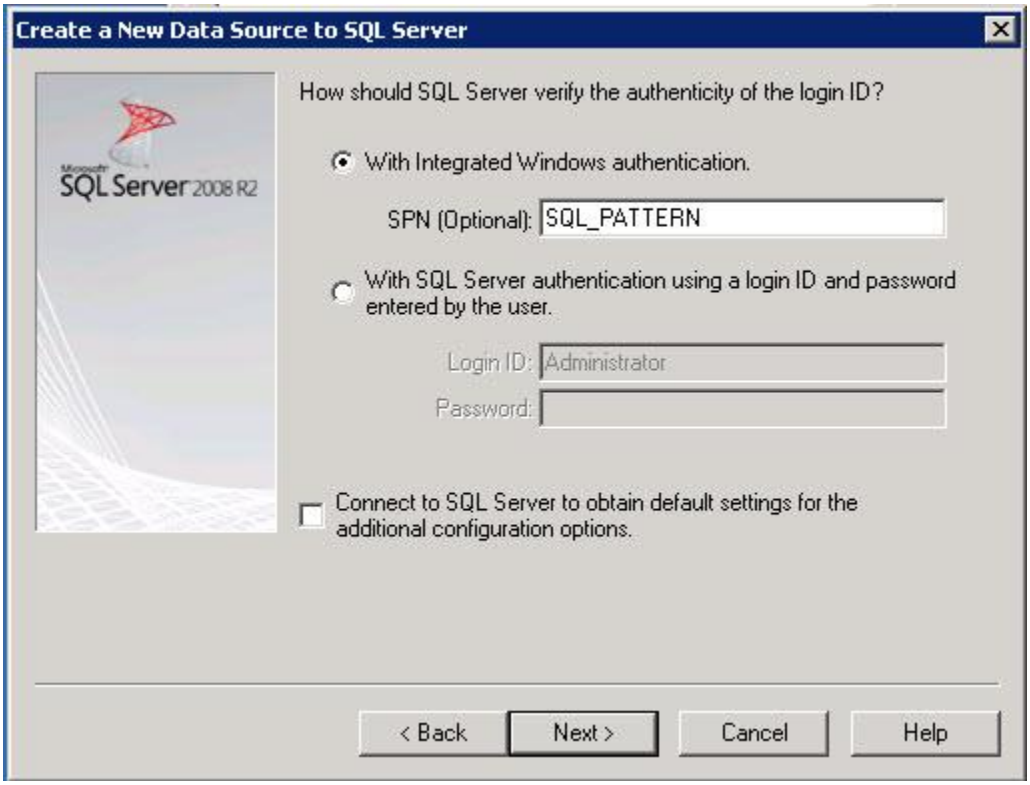
3. Select **SQL Server Native Client 10.0** and click **Finish.**



4. To create a data source connection specify the configuration information provided in the following screens. Click **Next** after completing each screen.



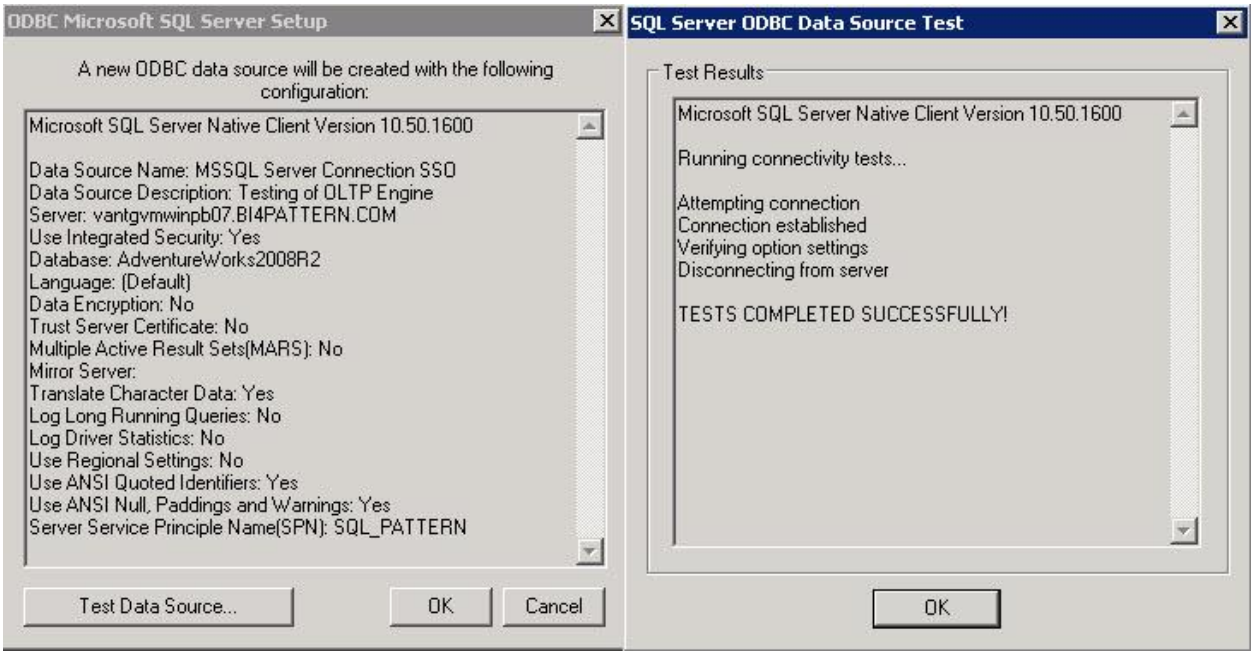
5. Select **With Integrated Windows authentication** and type SQL _PATTERN in the **SPN (Optional)** field as shown below:



6. Click **Next**.

Testing the connection

Now that our **Data Source** has been created, it can be tested by clicking **Test Data Source.**



Your service account and connection has been successfully tested.

Configuring the File Repository Server (FRS)

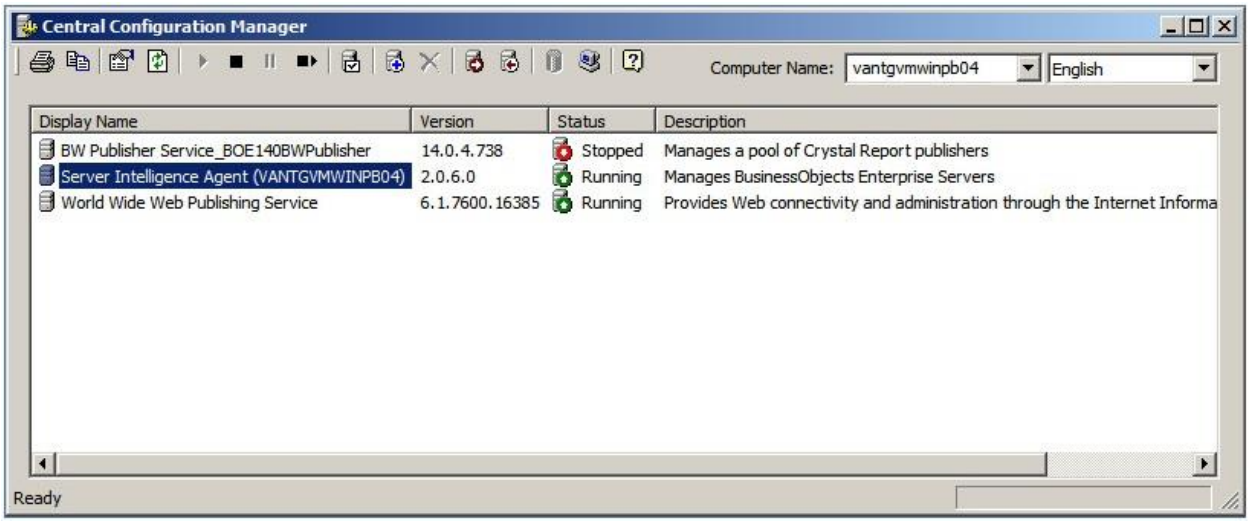
Workflow

1. In the CCM, change the default location of the FRS to a share.
2. In the CMC, update the Input and Output FRS servers on the BI platform servers to the shared location.

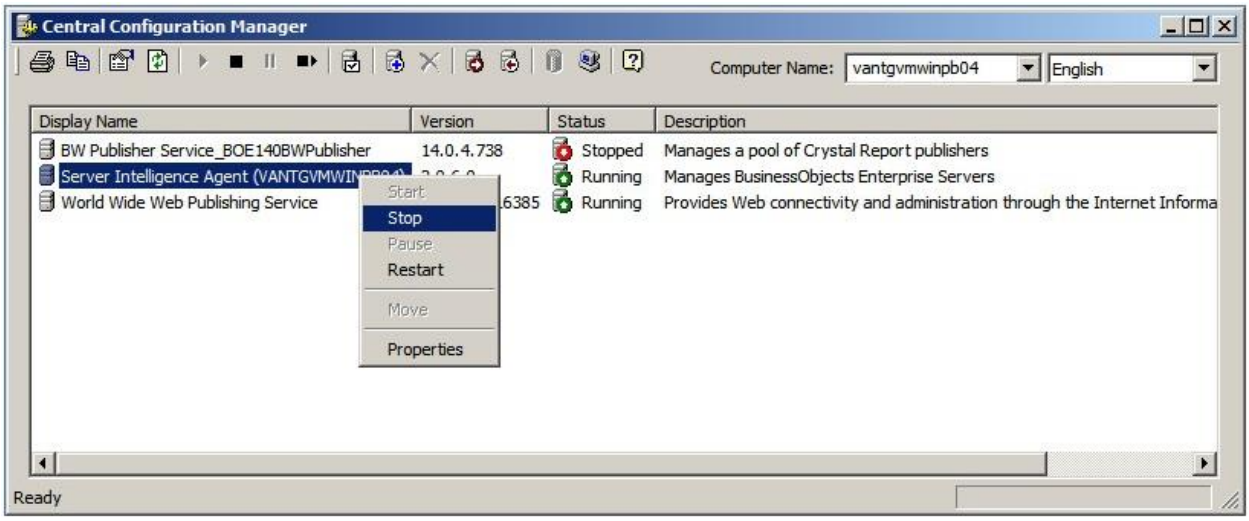
To change the FRS location in the CCM

By default, the FRS is located here C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\FileStore. It needs to be moved to share on the WINFRS01 machine.

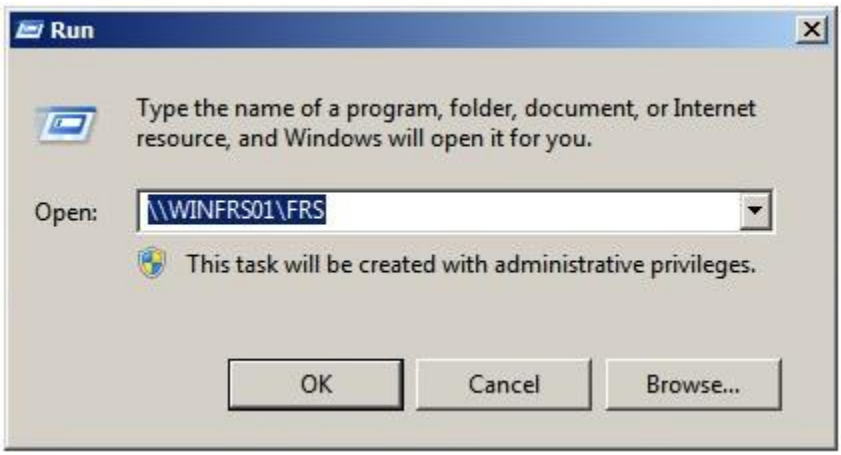
1. Log in to the machine Vantgvmpb04 using an administrator account.
2. To open the CCM, click **Start** > **All Programs** > **SAP BusinessObjects BI Platform 4** > **SAP BusinessObjects BI platform** > **Central Configuration Manager(CCM)**.



3. Right-click **Server Intelligence Agent**, and click **Stop**.



4. When the SIA has stopped, to access the FRS share, click **Start** > **Run**, and in the "Run" dialog box, type the path to the FRS share:\WINFRS01\FRS.

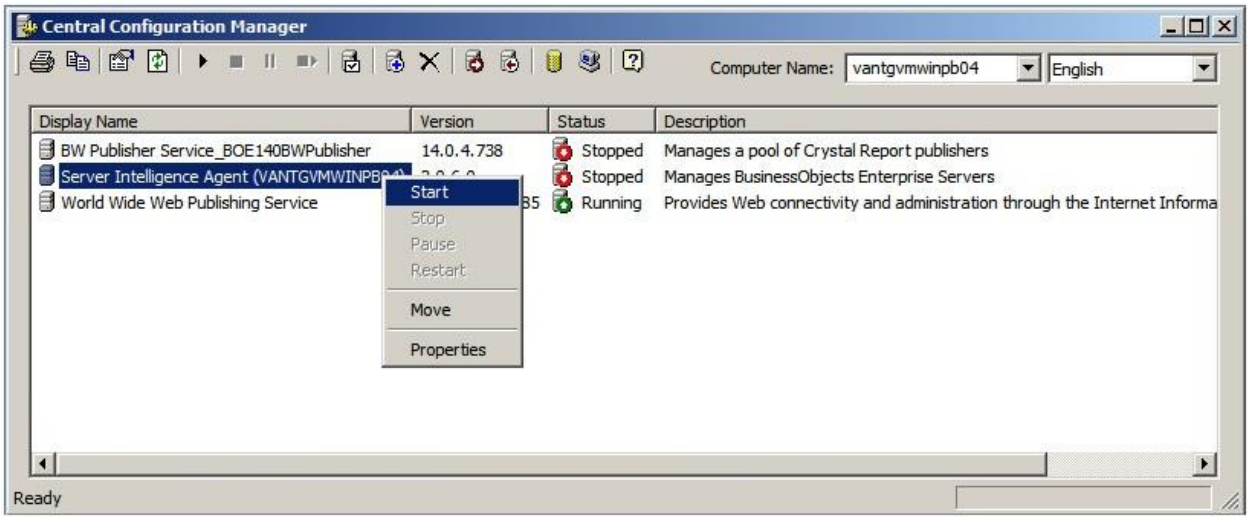


5. Copy the Input folder and Output folder from C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\FileStore to \\WINFRS01\FRS
6. Once the files are copied, count the folders and files in both locations to ensure they match in number.

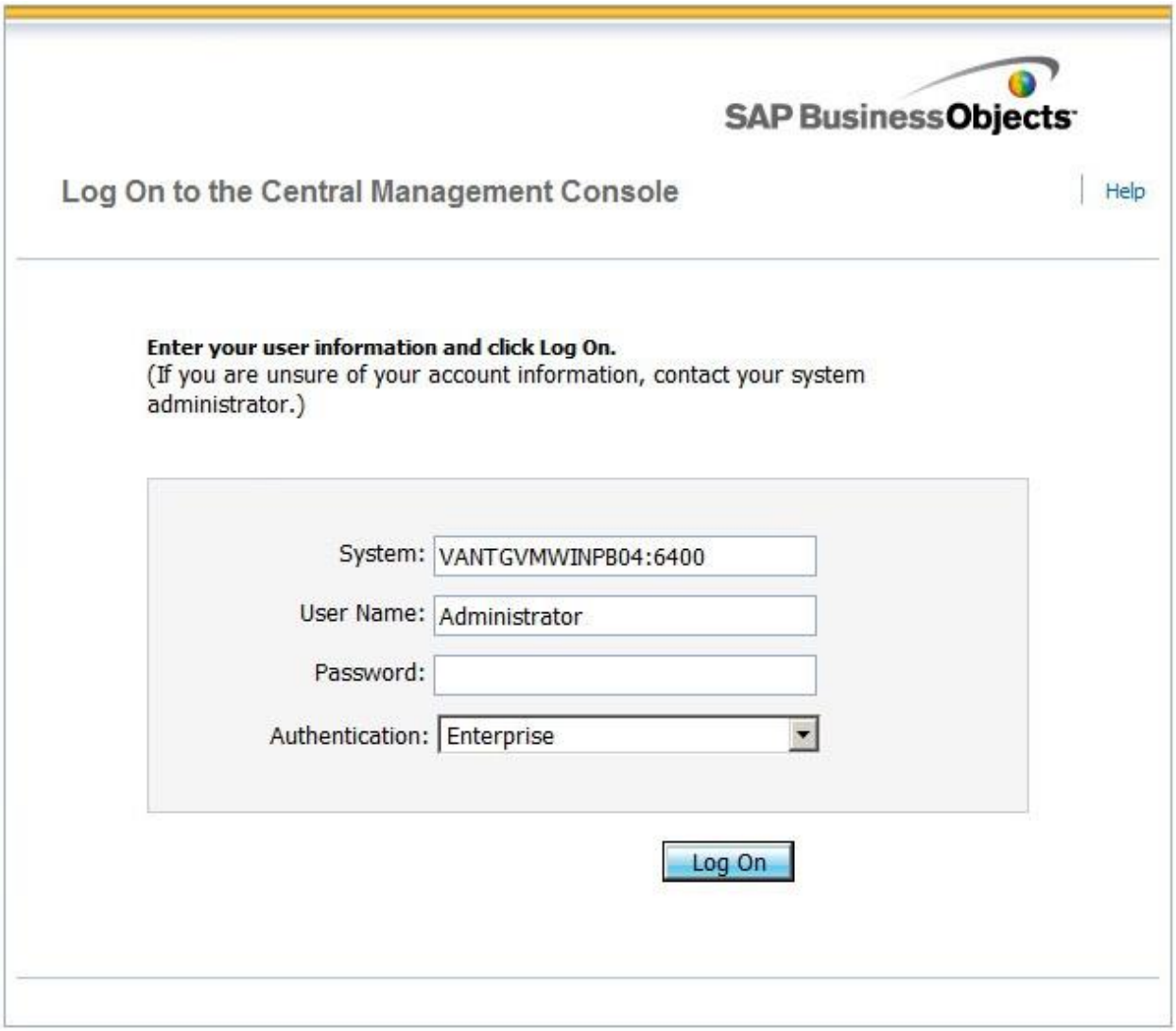
To update the Input and Output FRS servers on BIP servers to the shared location

Follow these steps to update the Input and Output FRS servers on the BI platform servers to the shared location.

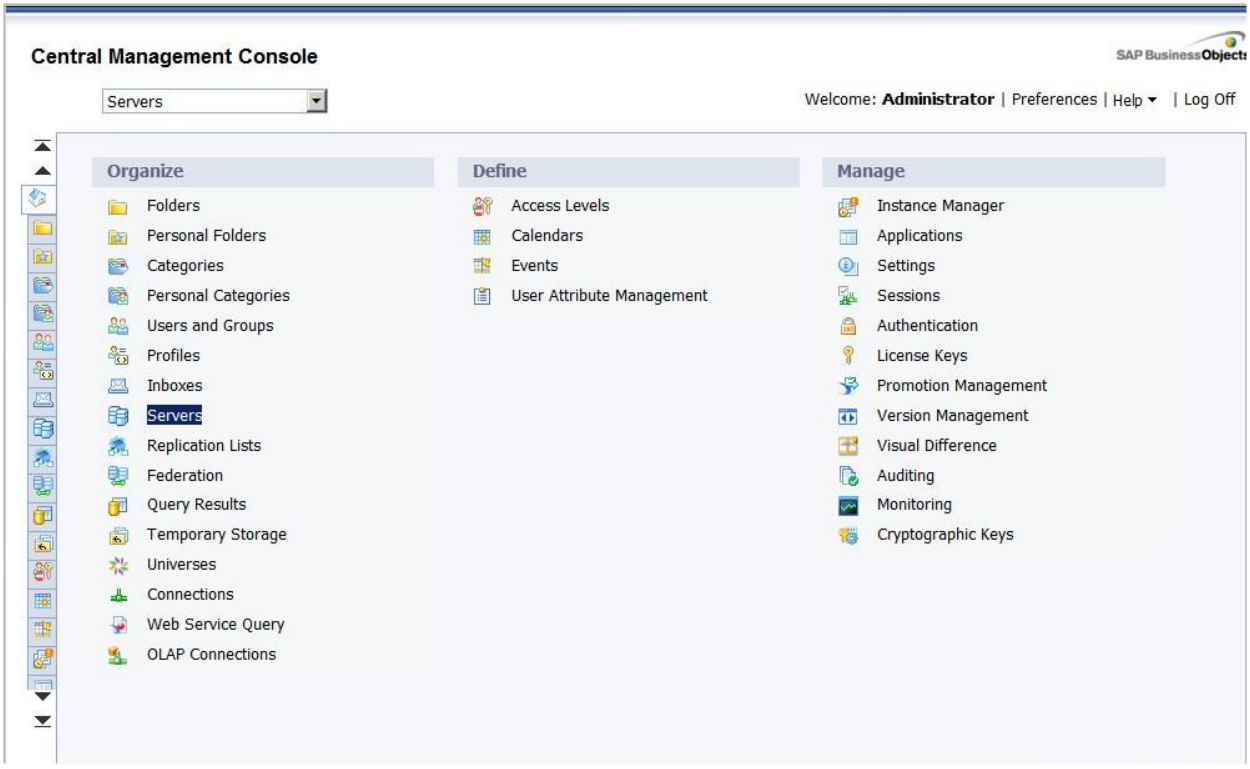
1. To start the SIA service, in the CCM, right-click **Server Intelligence Agent**, and click **Start**.



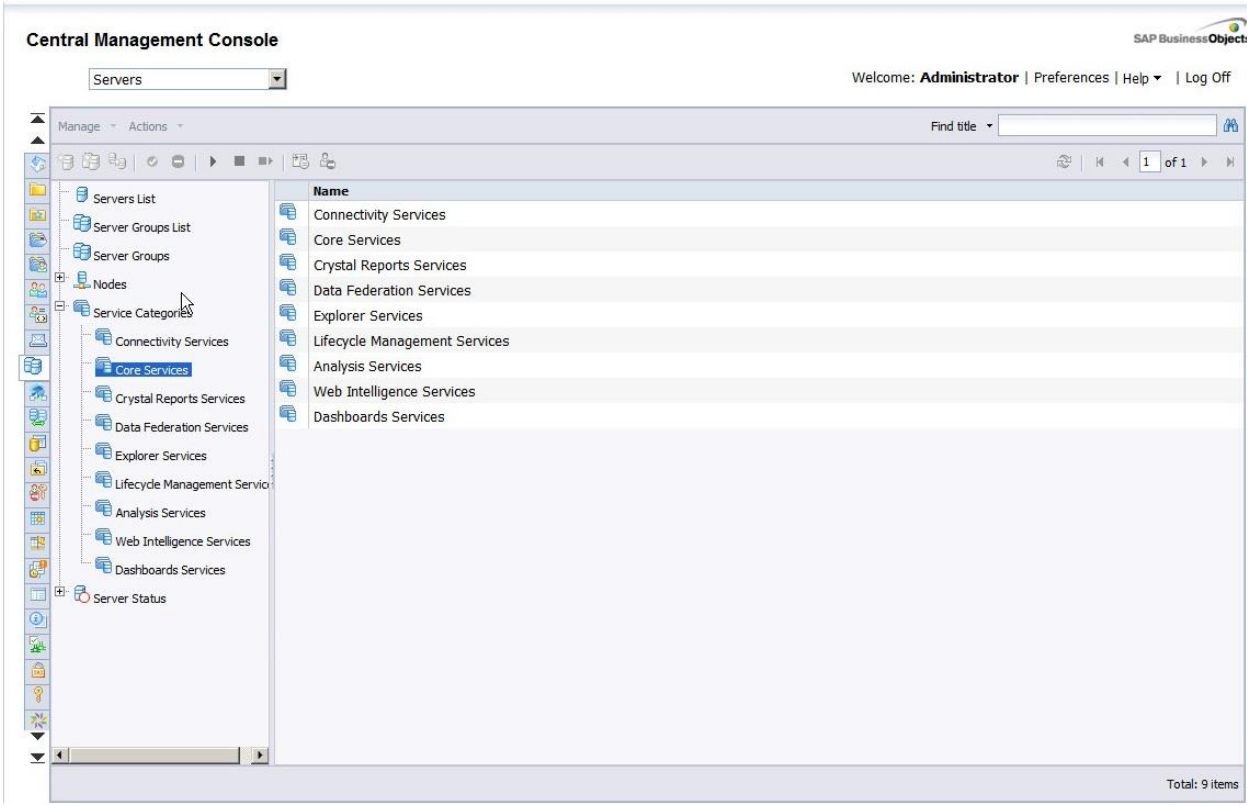
2. Log in to the Central Management Console (CMC) as an Administrator.



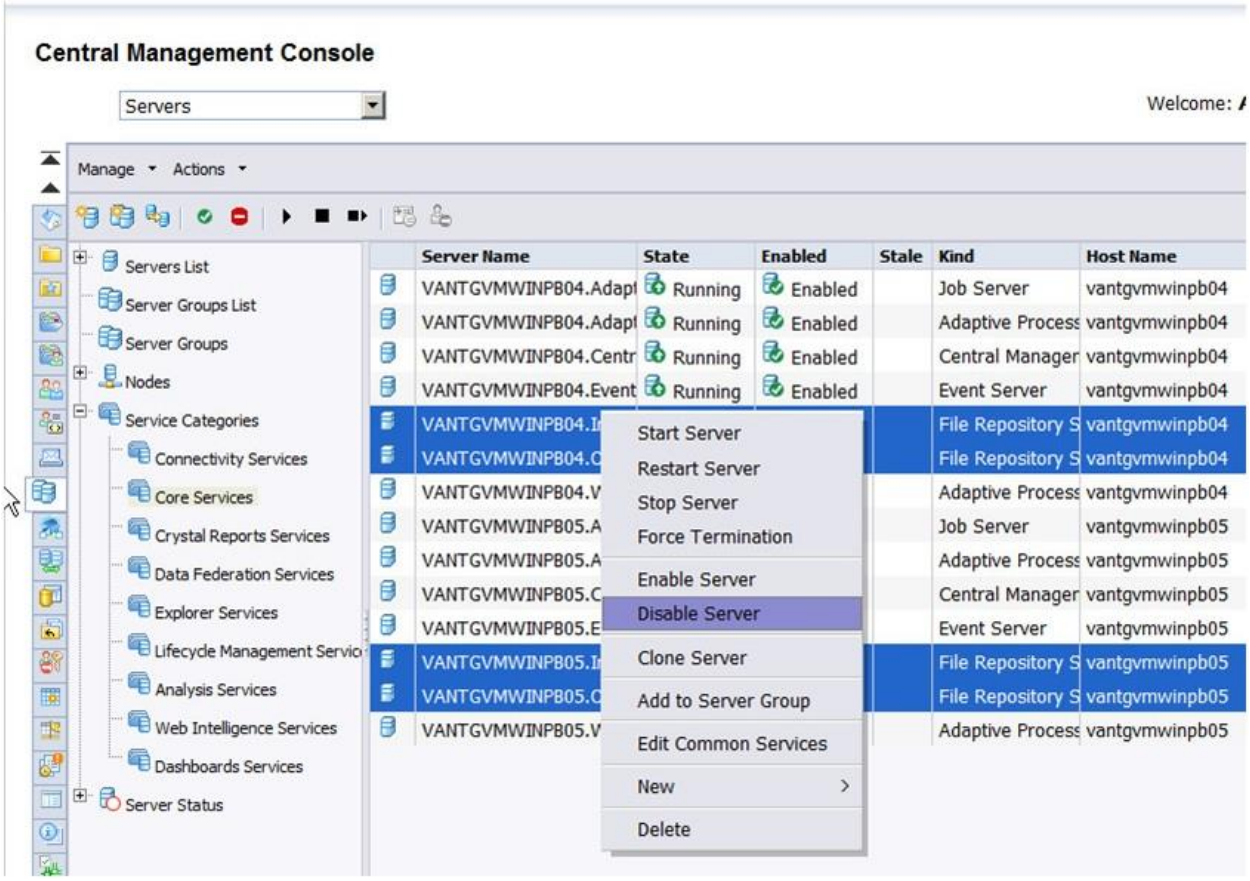
3. Click **Servers**.



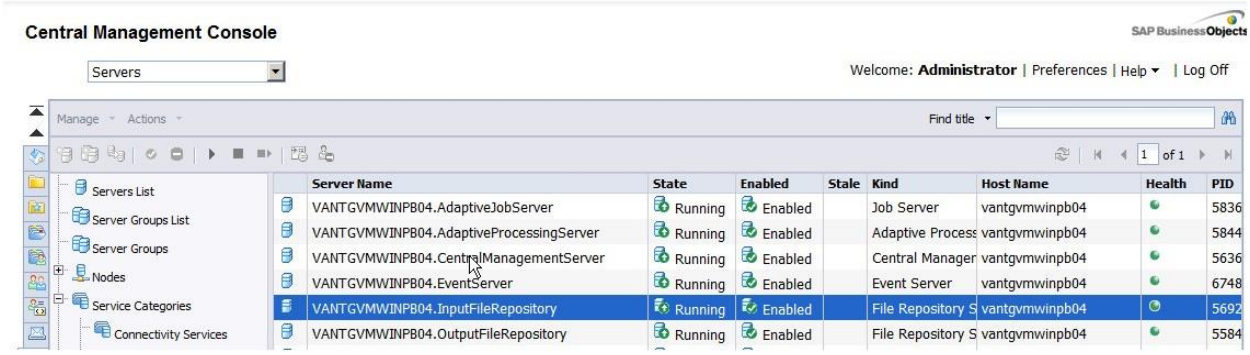
4. Click **Core services**.



5. Hold down the CRTL key, and click on the following Input and Output servers:
    - VANTGVMWINPB04.InputFileRepository
    - VANTGVMWINPB05.InputFileRepository
    - VANTGVMWINPB04.OutputFileRepository
    - VANTGVMWINPB05.OutputFileRepository.
6. Right-click any of the selected servers, and click **Disable Server**.



7. Double-click VANTGVMWINPB04.InputFileRepository.



8. In the "Input Filestore Service" area, in the **File Store Directory** box type the following text:\\WINFRS01\FRS\Input

9. In the **Temporary Directory** box, type \\WINFRS01\FRS\Input\temp.

10. To save the changes, click **Save** & **Close**.

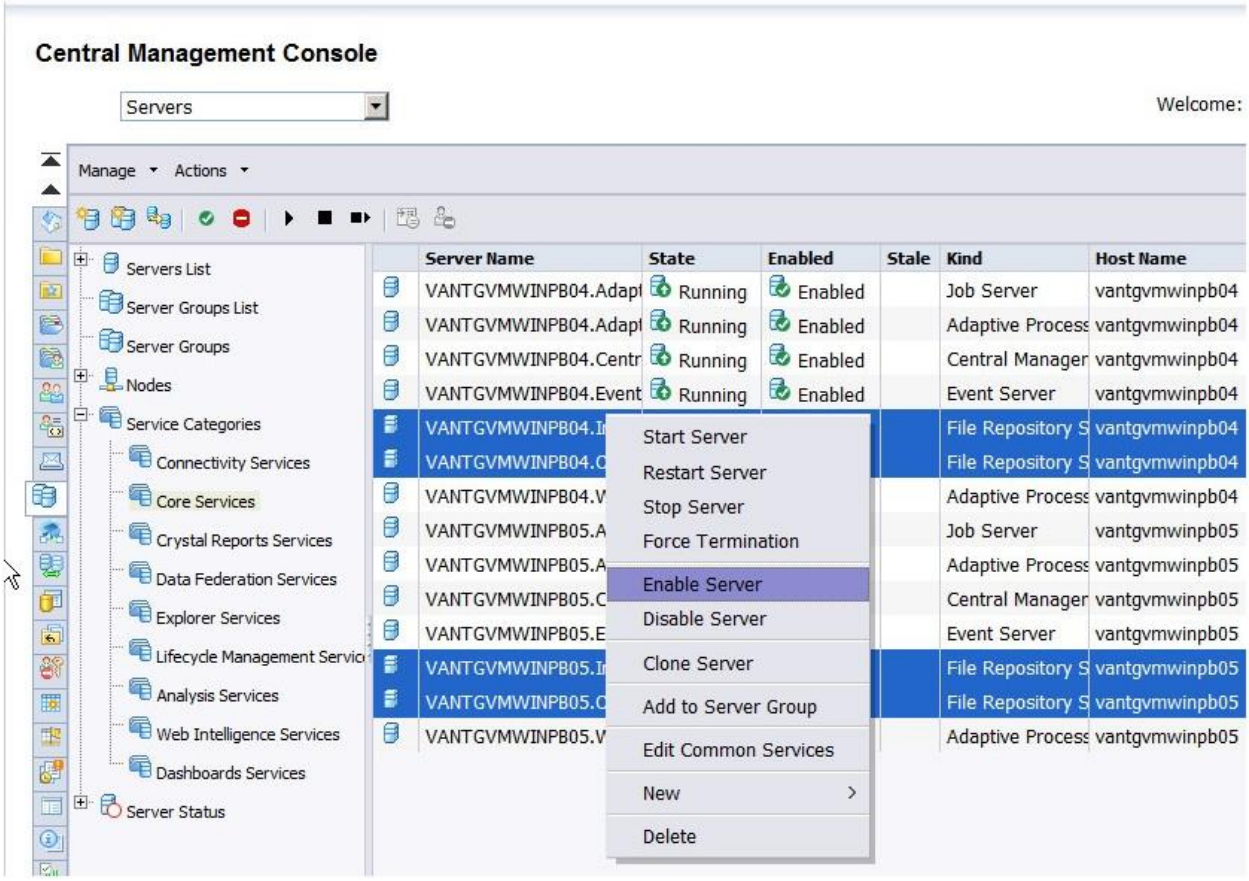
11. Repeat Steps 7 to 10 for the VANTGVMBIP05.InputFileRepository server.

12. Repeat steps 7 to 10 for Output FRS servers VANTGVMWINPB04.OutputFileRepository and VANTGVMWINPB05.OutputFileRepository.
    Ensure that the following path is used: \\WINFRS01\FRS\Output

13. Restart each of the modified servers to commit the changes: hold down the CRTL key, and click on the following Input and Output servers:

    - VANTGVMWINPB04.InputFileRepository
    - VANTGVMWINPB05.InputFileRepository
    - VANTGVMWINPB04.OutputFileRepository
    - VANTGVMWINPB05.OutputFileRepository.

14. Right-click any of the selected servers, and click **Enable Server**.



You have successfully updated the input and output FRS servers in the CMC.

BI platform 4.0 cluster configuration

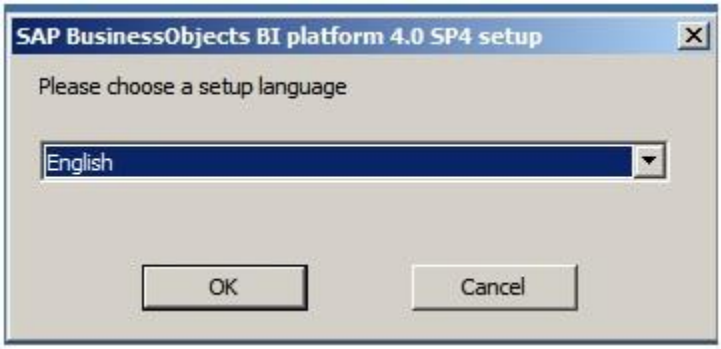
To set up the cluster, install the BI platform servers on two machines and cluster them. The following topics provide step-by-step instructions for setting up the cluster:

- Configuring and installing BI platform on server 1
- Configuring and installing BI platform on server 2
- Changing the cluster name
- Splitting Adaptive Processing Server (APS)

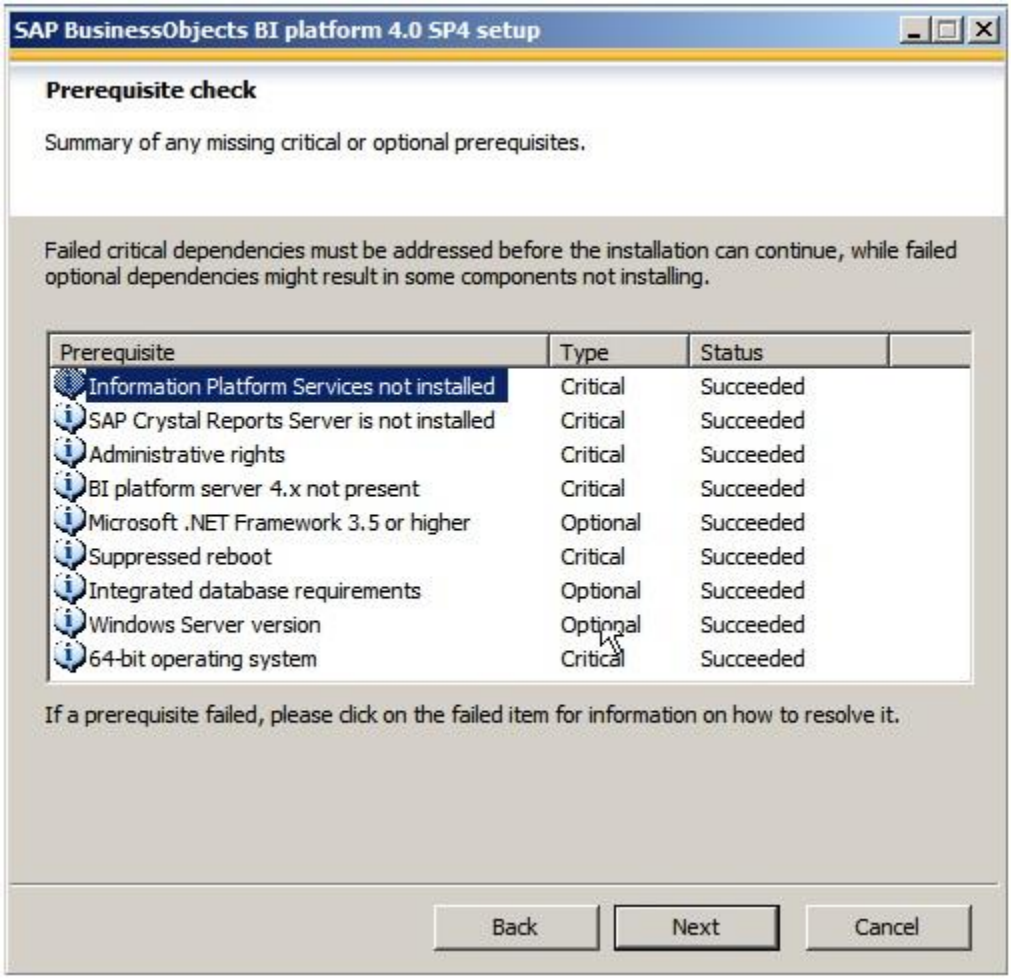
Configuring and installing BI platform on server 1

To install BI platform on server 1

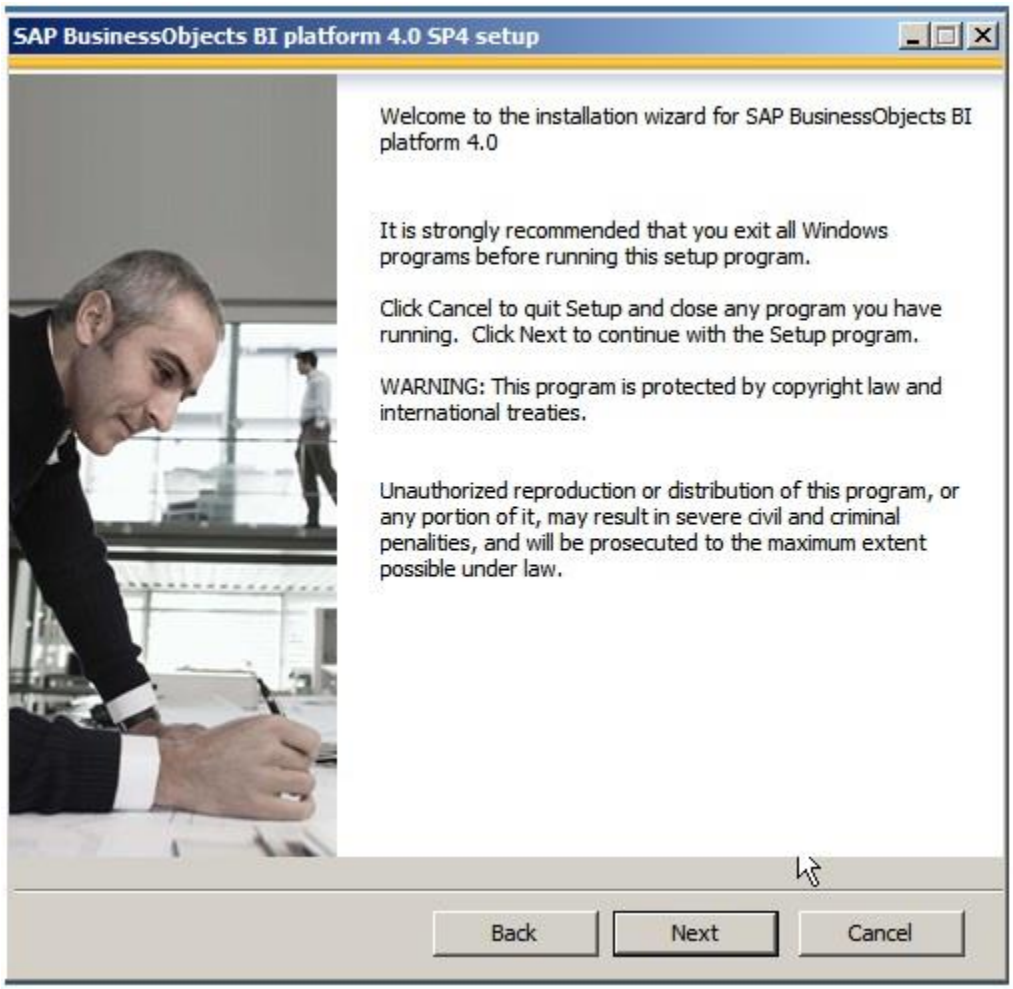
1. Log in to VANTGVMWINPB04.pgdev.sap.corp as Administrator.
2. Go to the "SAP BusinessObjects" folder, open it, and double-click Setup.exe.
3. On the "SAP BusinessObjects BI platform 4.0 SP4 setup" page, select **English**, and then click **OK**.



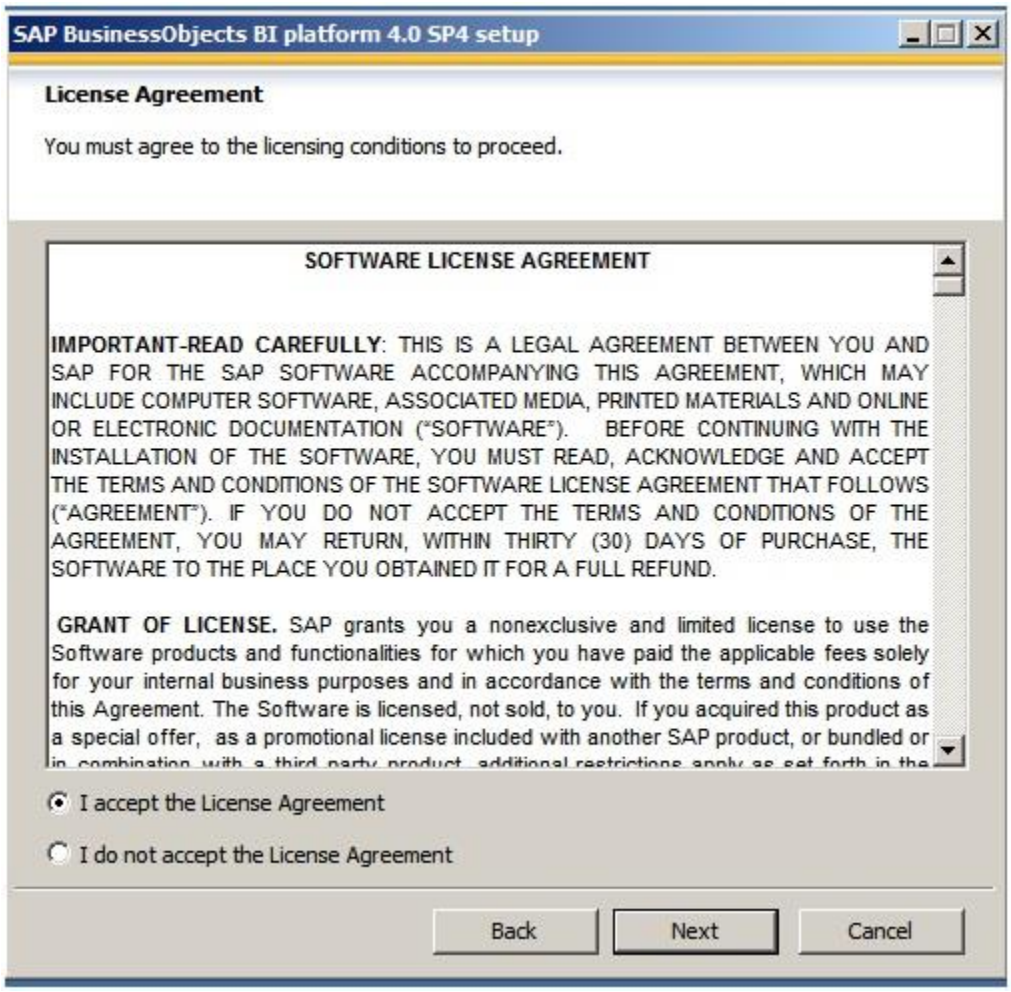
4. When the prerequisite system check completes successfully, click **Next**.



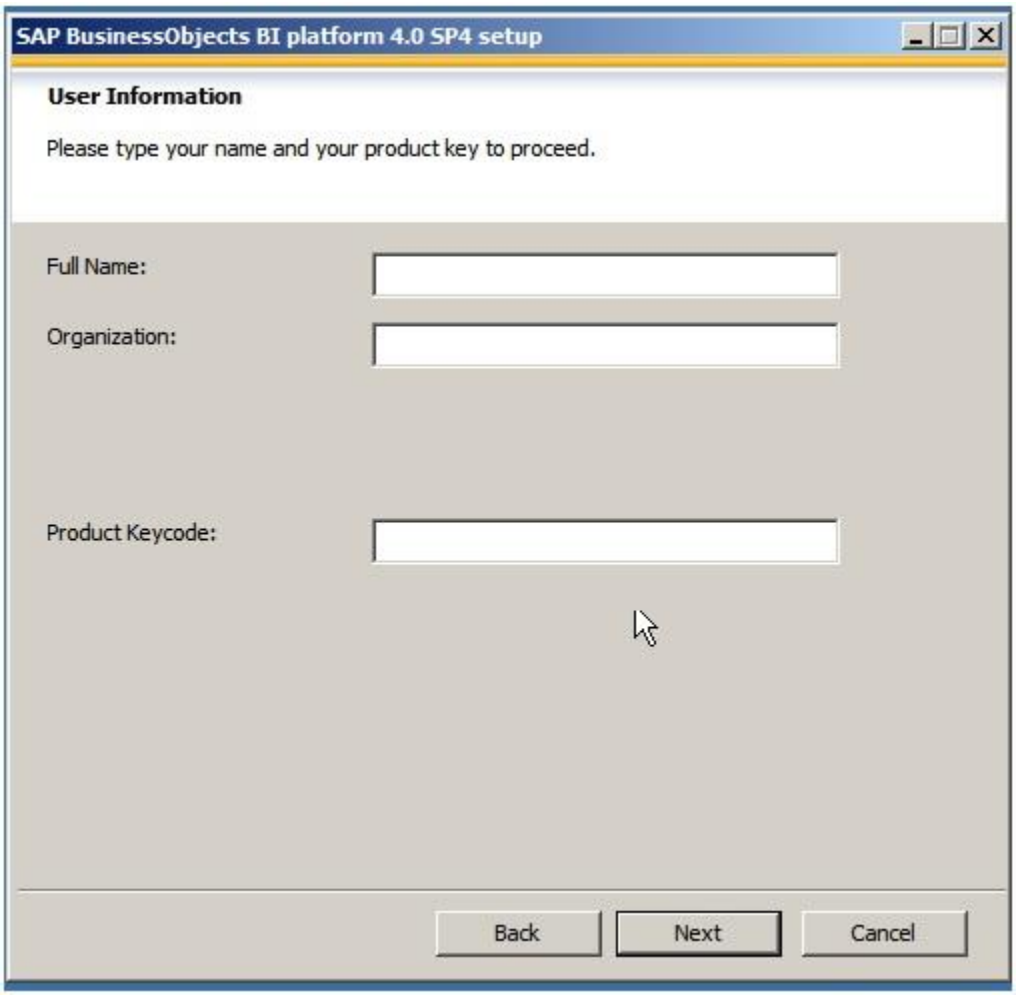
5. On the "SAP BusinessObjects BI platform 4.0 SP4 setup" page, click **Next**.



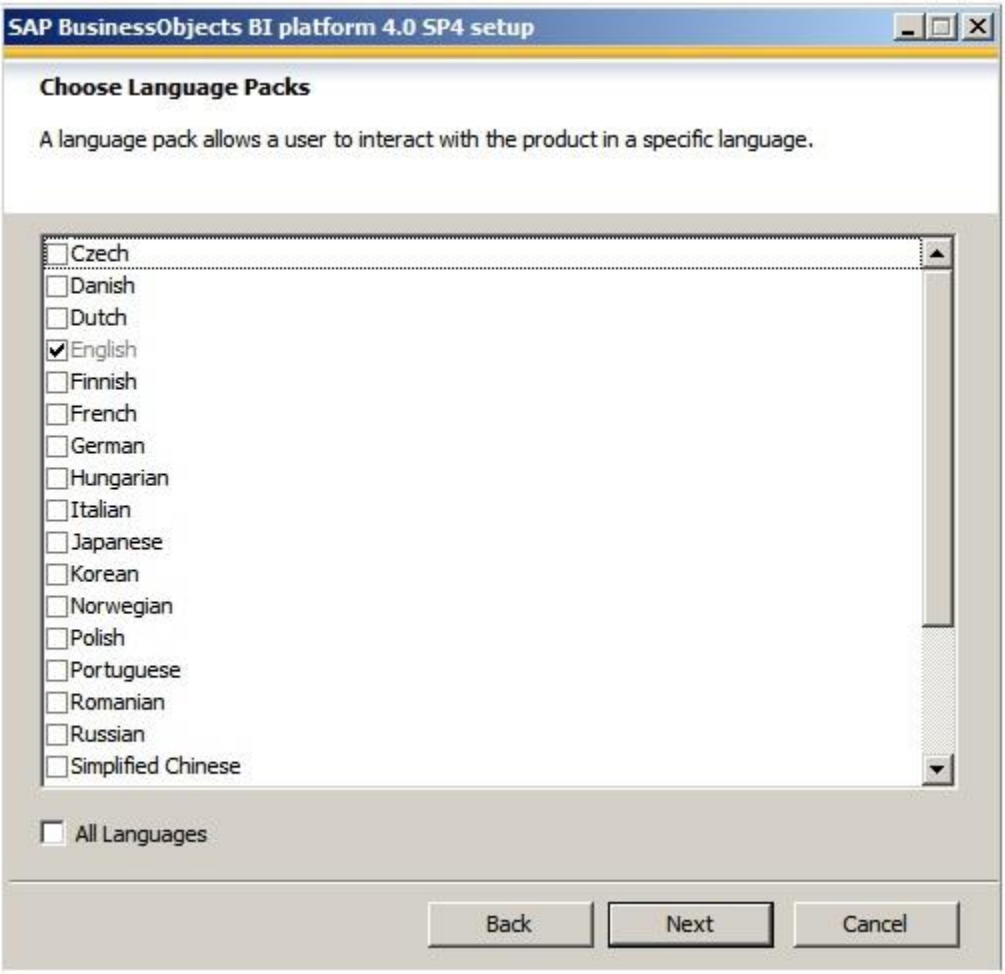
6. Accept the License Agreement, and click **Next**.



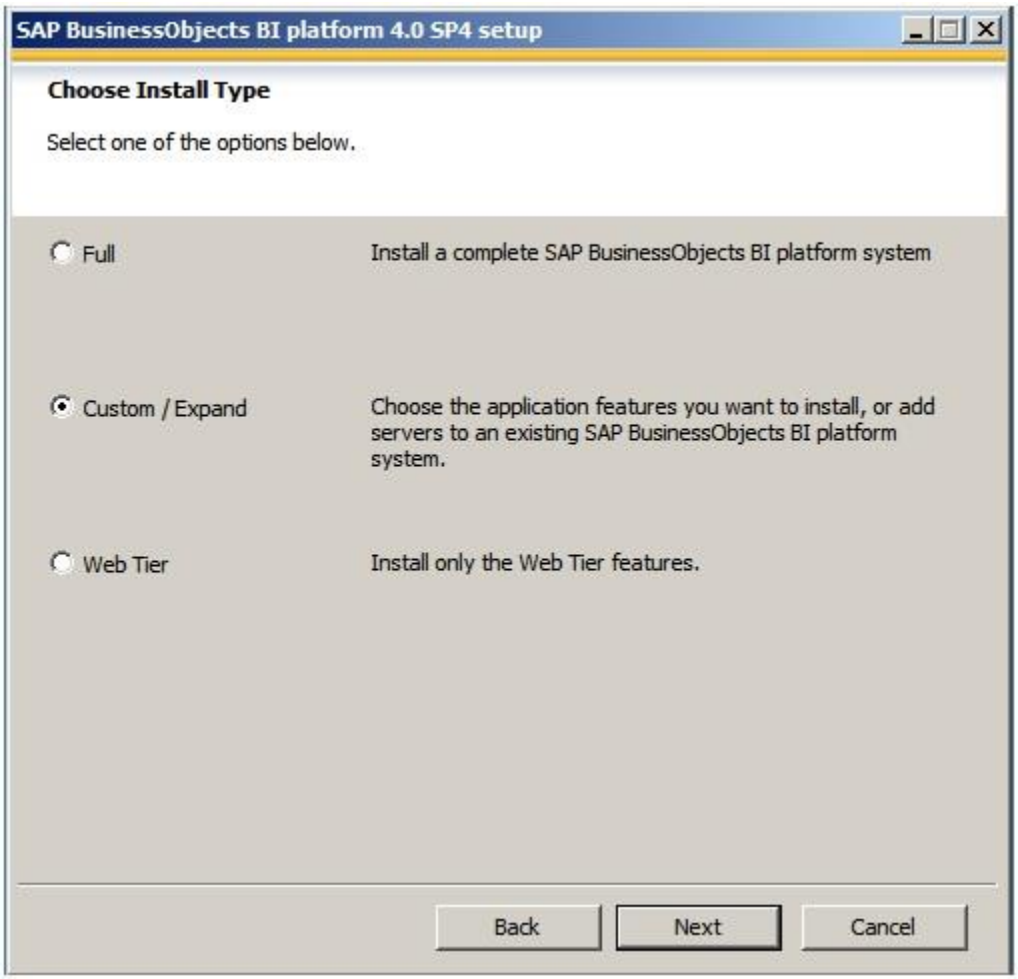
7. Type the information required for the **Full Name**, **Organization**, and **Product Keycode** boxes, and then click **Next**.



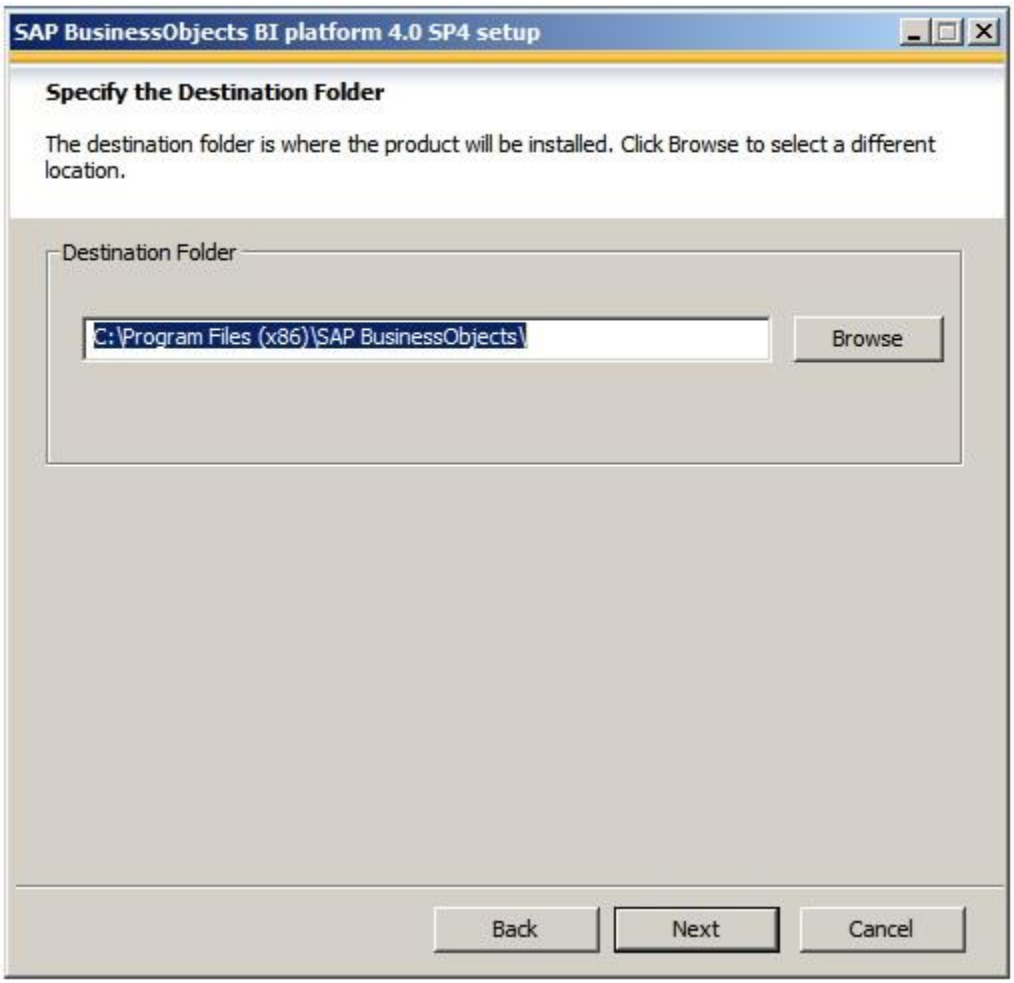
8. Click **Next** to accept the default language (English).



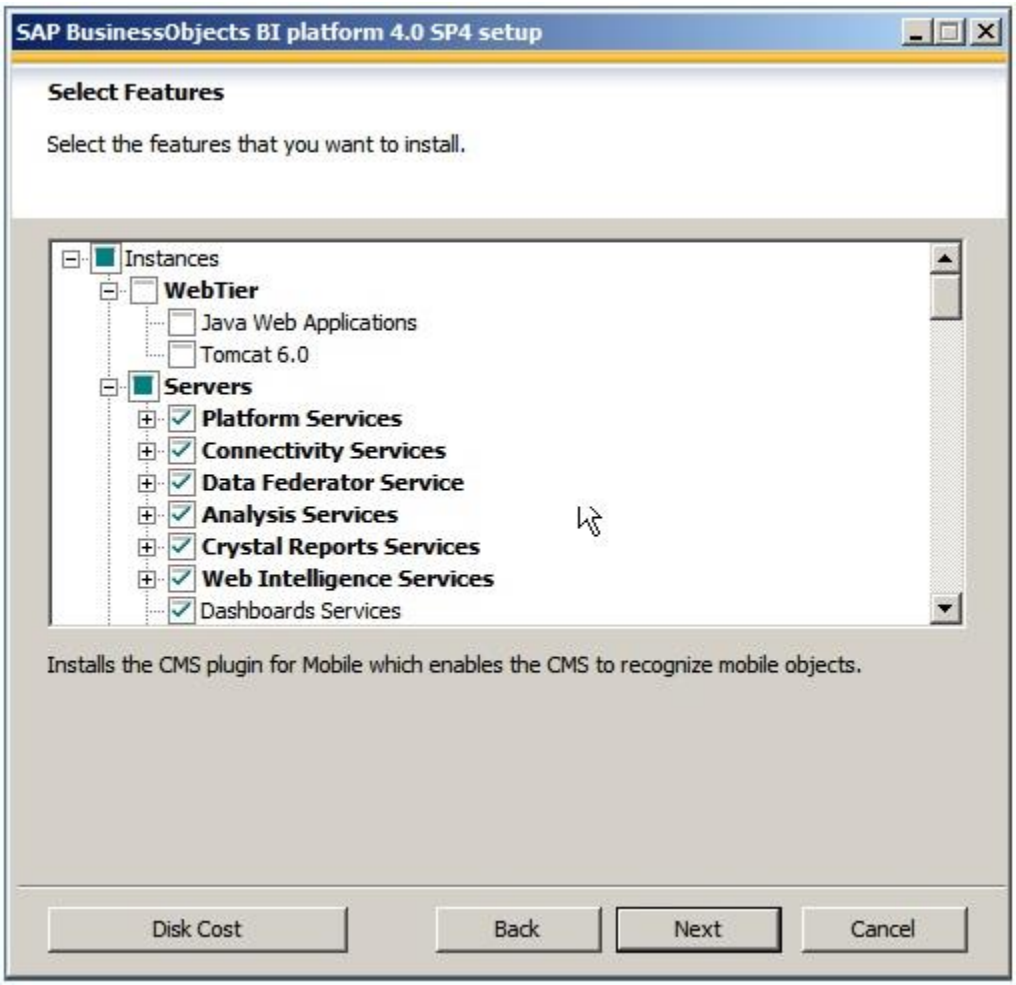
9. Click **Custom/Expand**, and click **Next**.



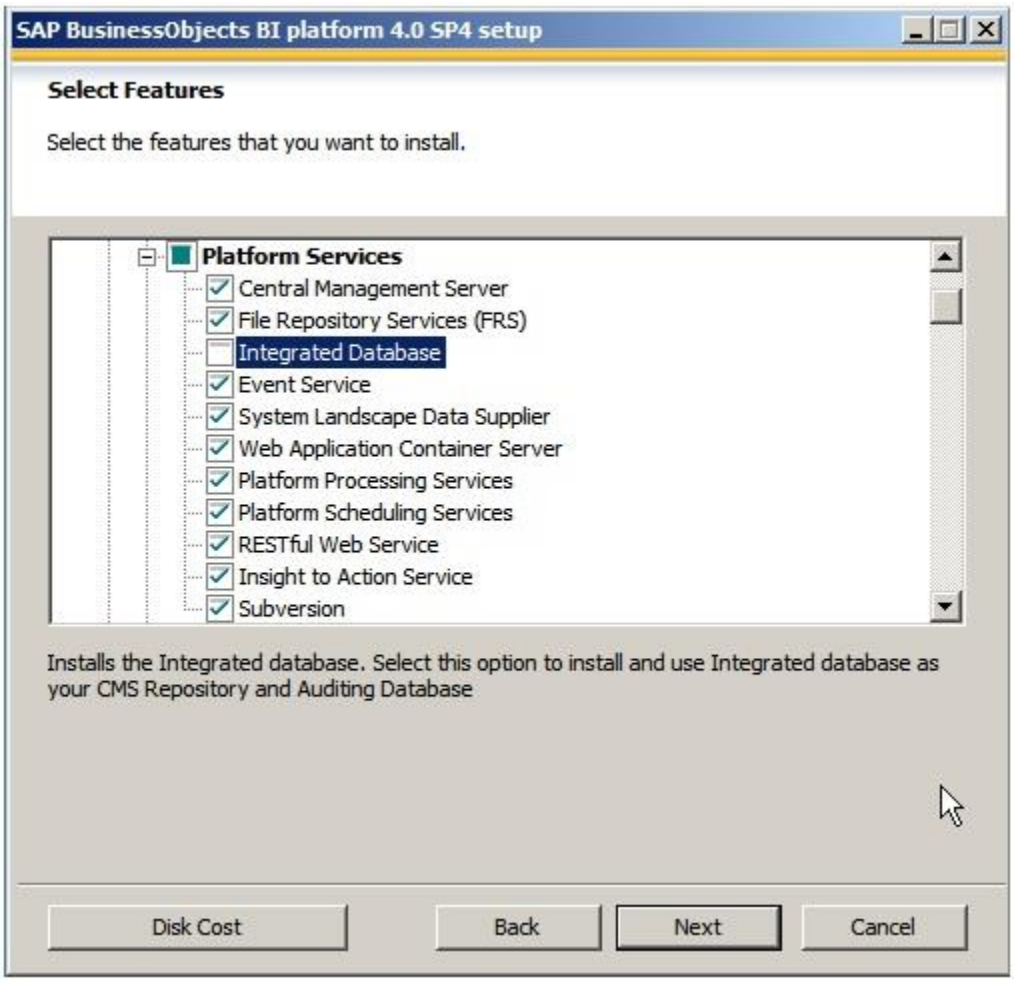
10. Click **Next** to accept the default path to the folder where the program will be installed.



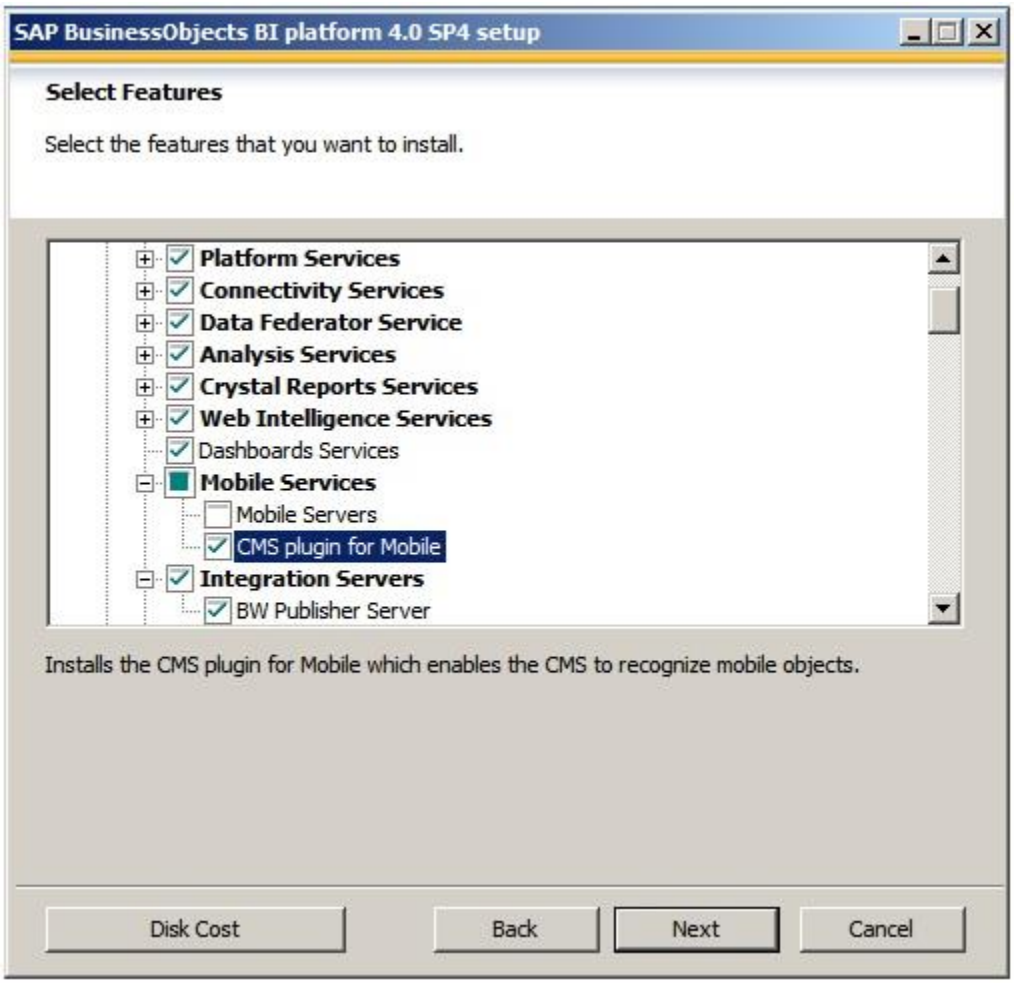
11. Clear the check boxes under **Web Tier**.



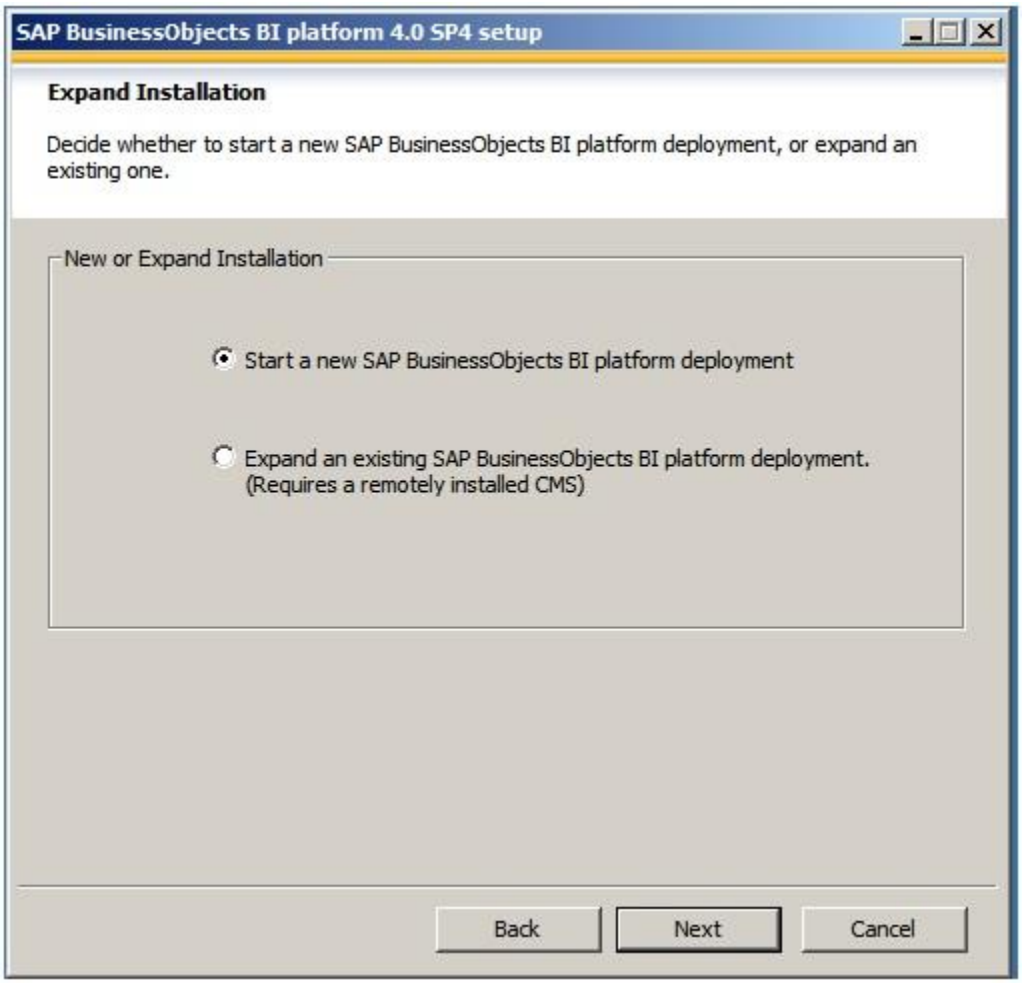
12. Expand **Platform Services**, and clear the **Integrated Database** check box.



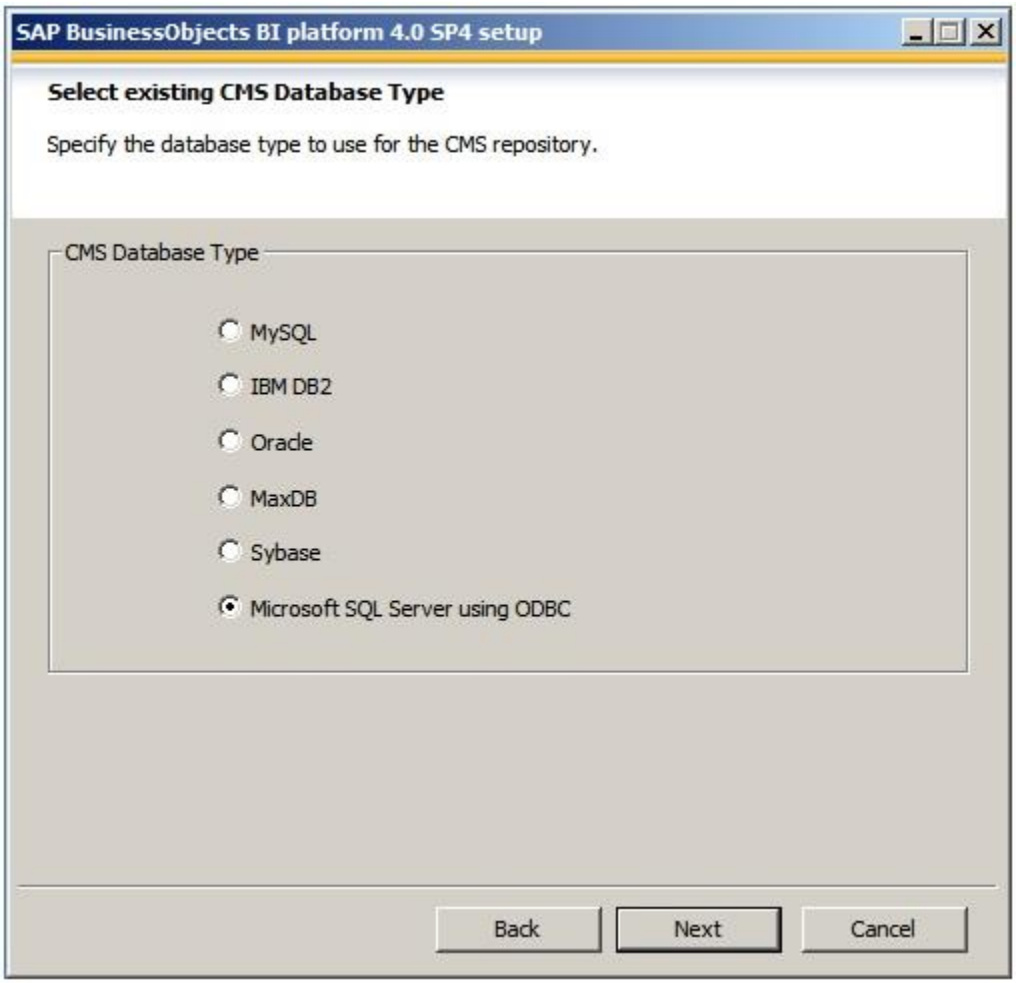
13. Expand **Mobile Services**, clear the **Mobile Servers** check box, (leave the **CMS plugin for Mobile** check box selected), and then click **Next**.



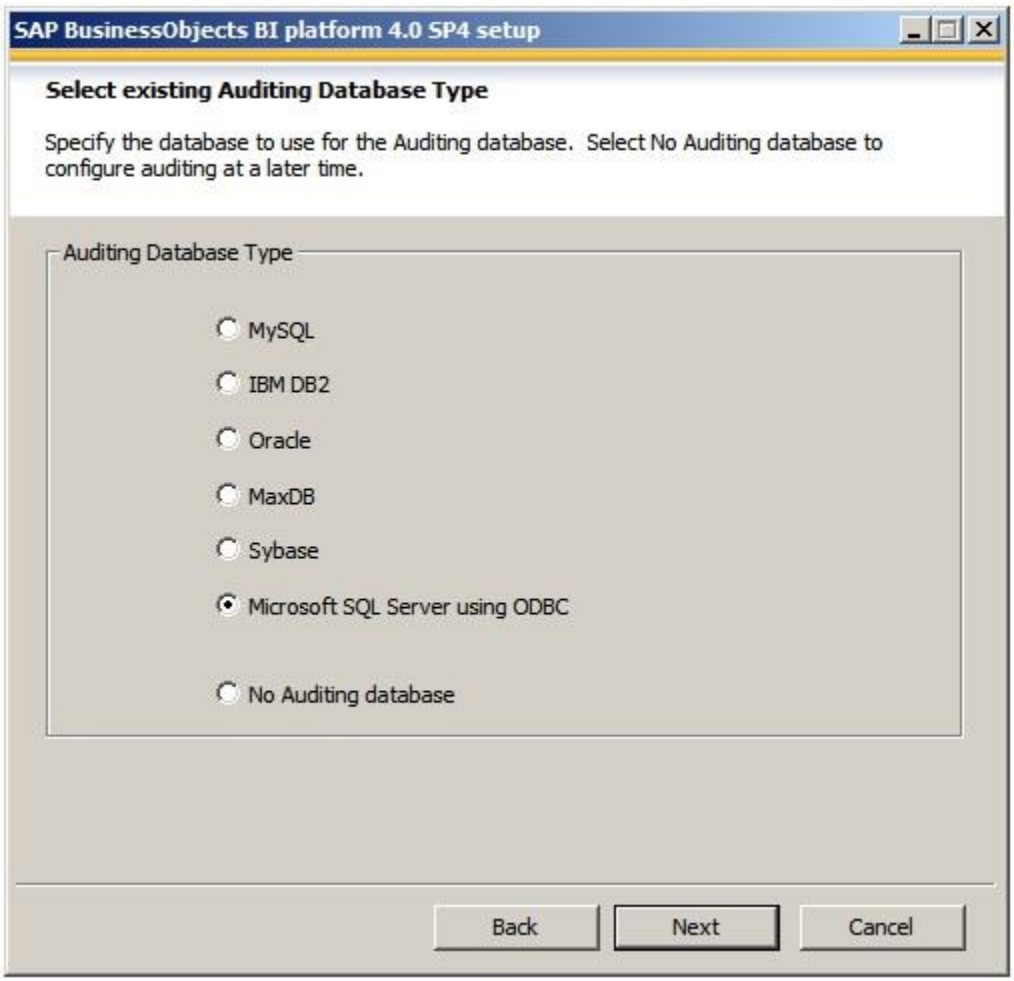
14. On the "Expand Installation" page, click **Start a new SAP BusinessObjects BI Platform deployment**, and click **Next**.



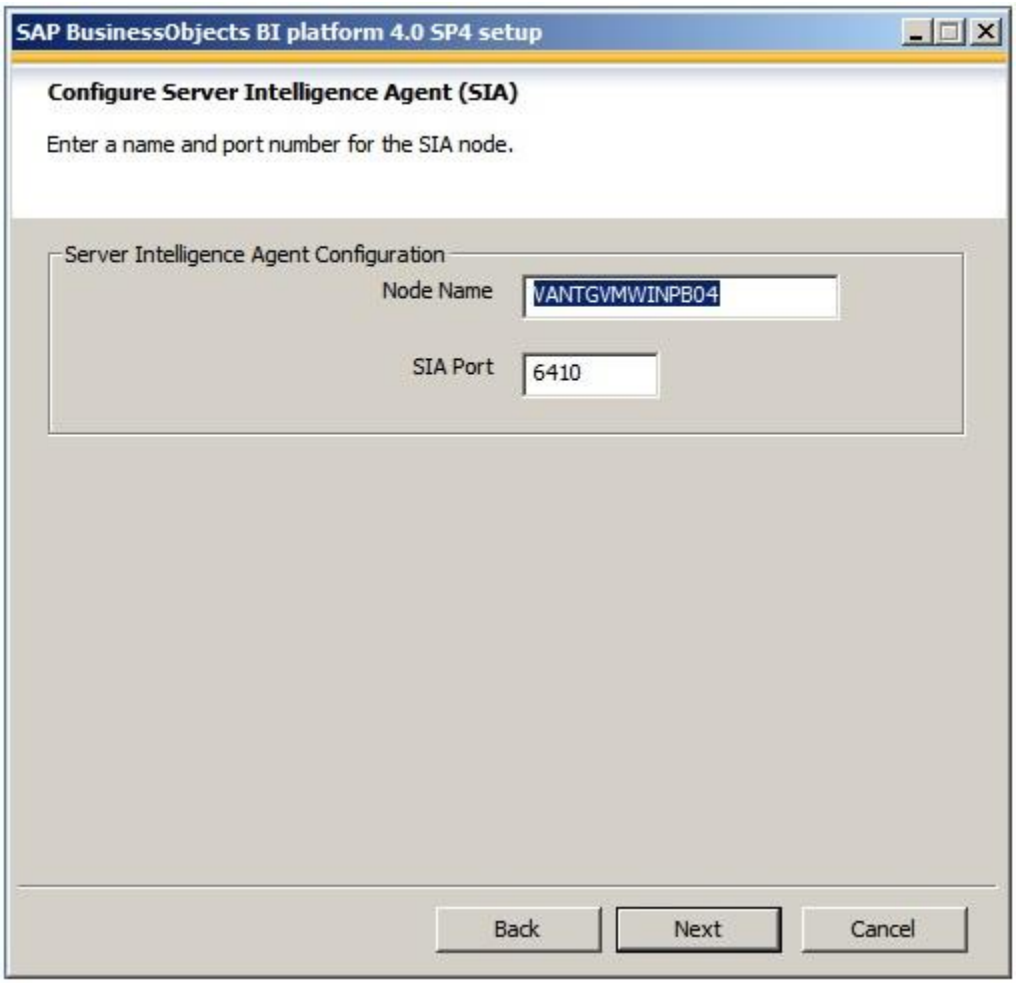
15. For use as the CMS database, click **Microsoft SQL Server using ODBC**, and click **Next**.



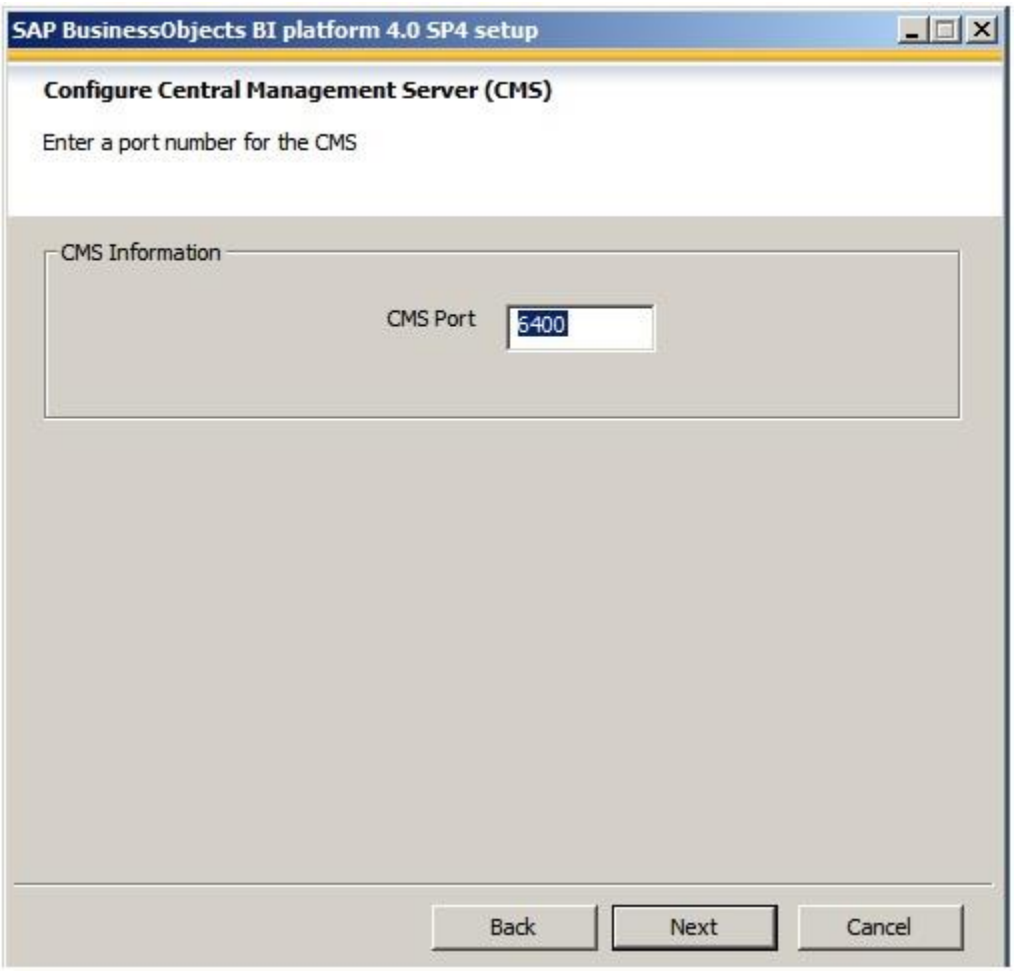
16. For use as the auditing database, click **Microsoft SQL Server using ODBC**, and click **Next**.



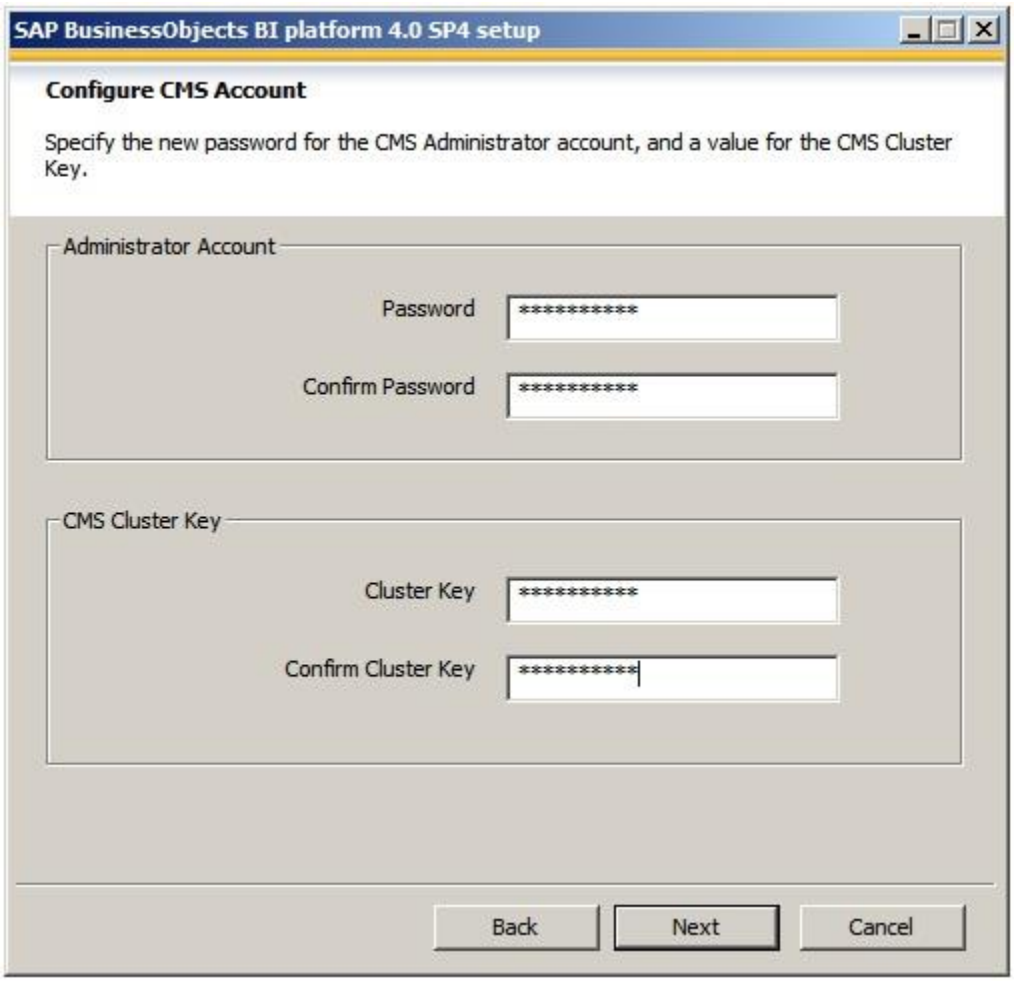
17. In the **Node Name** box, type the SIA name, leave the default SIA port to 6410, and then click **Next**.



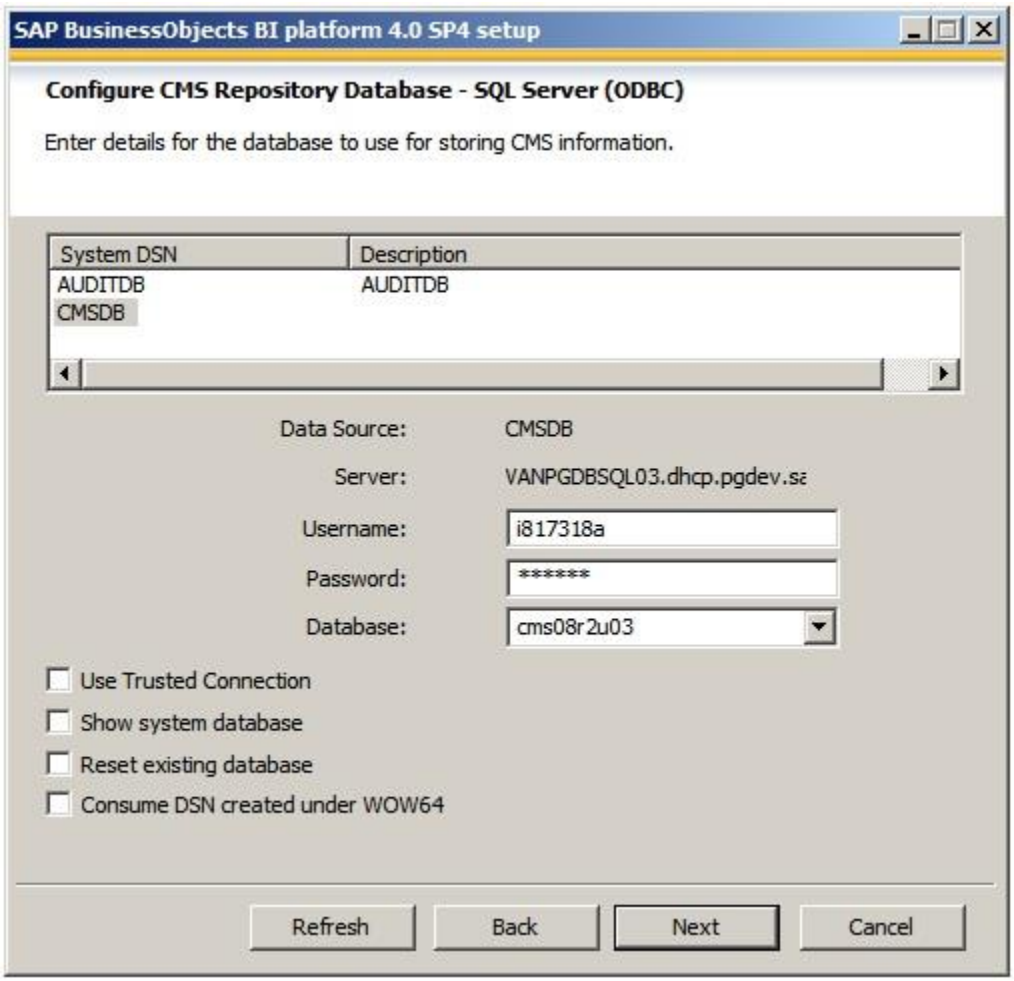
18. Leave the default port for the CMS to 6400, and click **Next**.



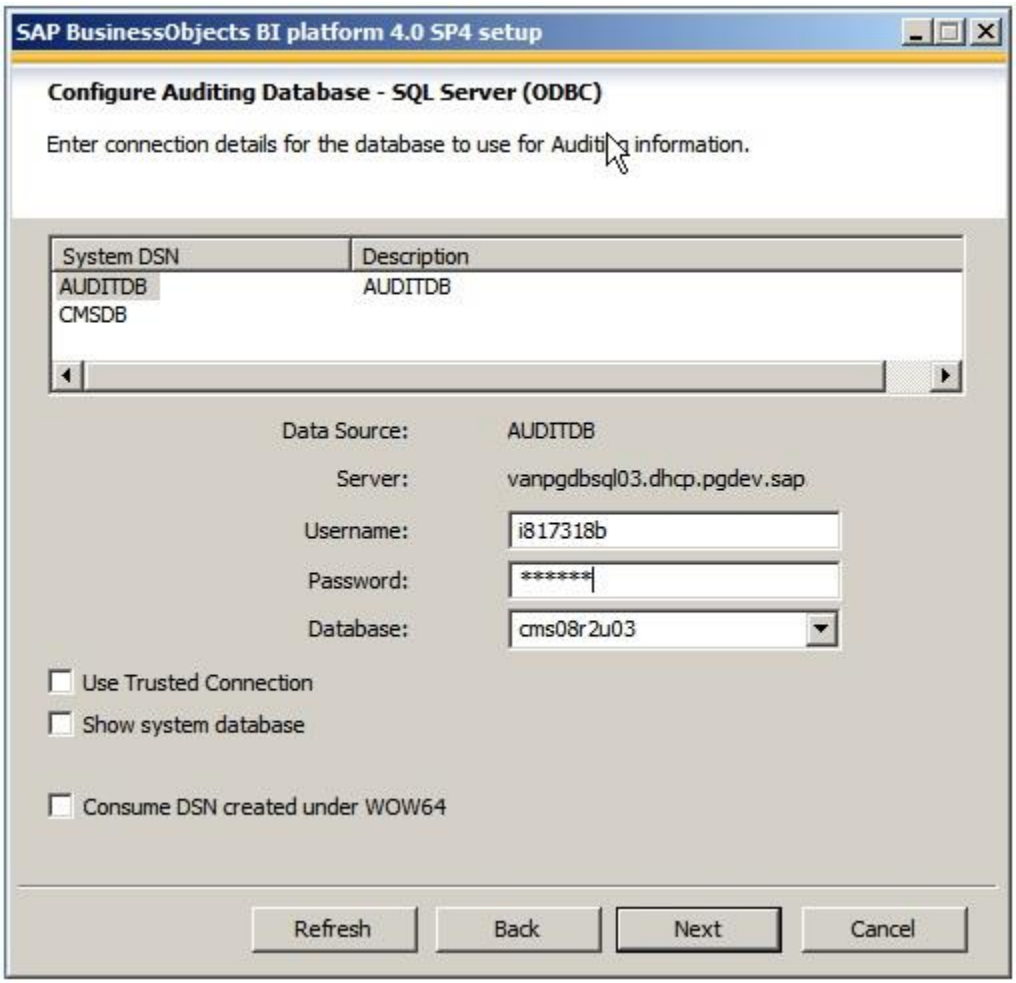
19. Type a password for the CMS Administrator account, type the cluster key, and click **Next**.



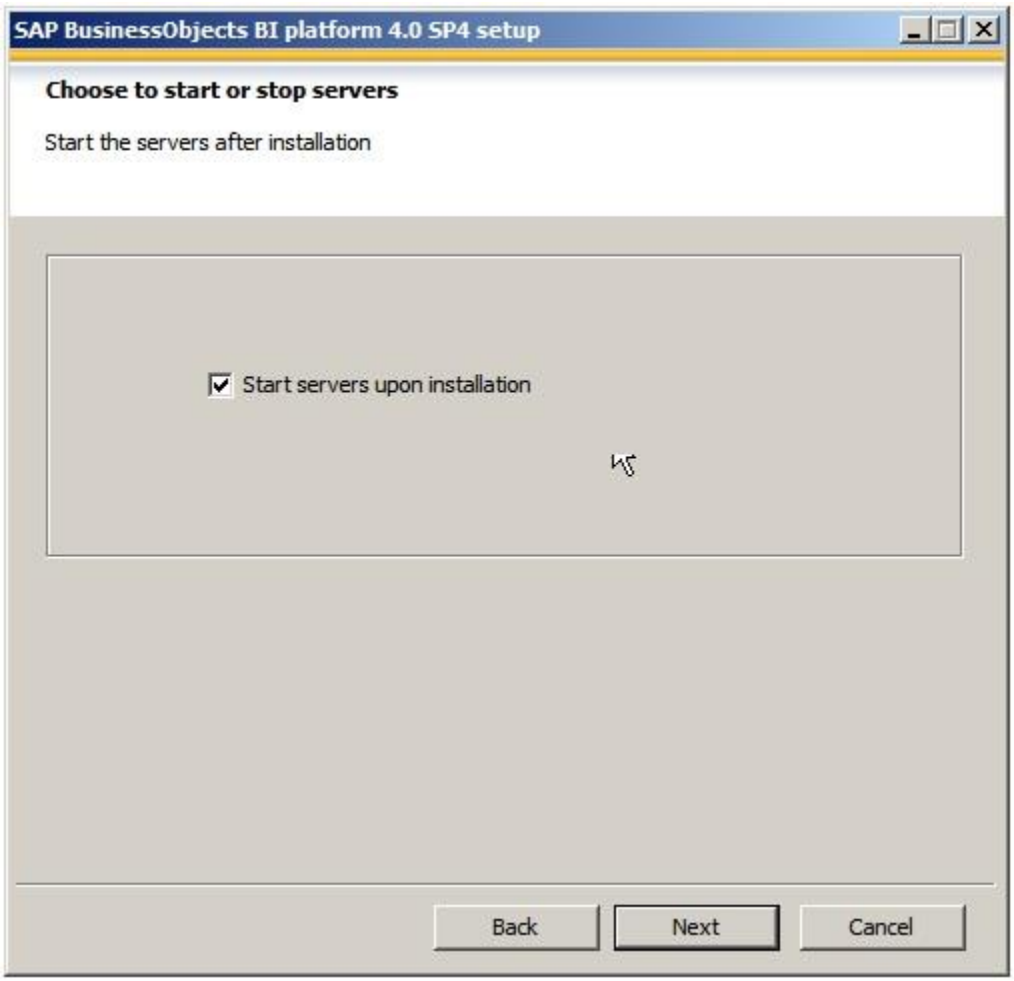
20. Type the login credentials for the CMS database, and click **Next**.



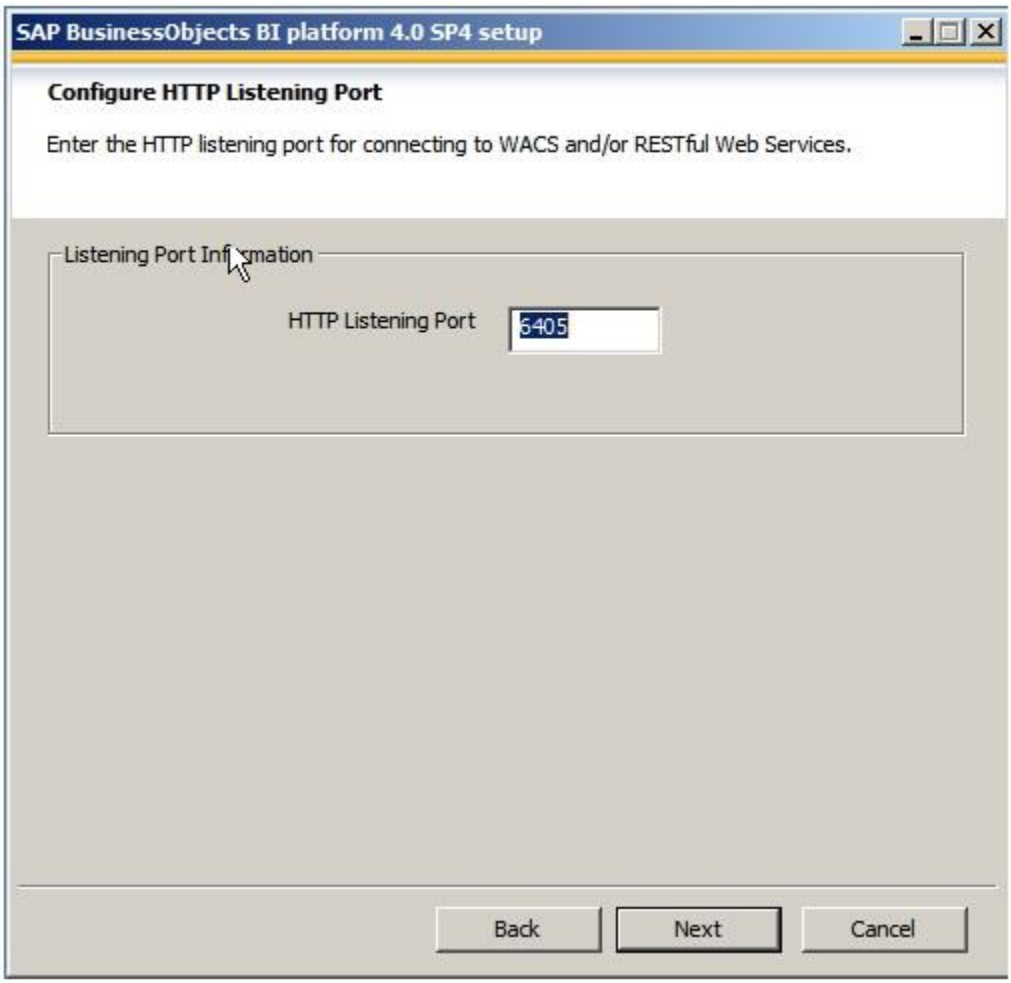
21. Type the login credentials for the Audit Database, and click **Next**.



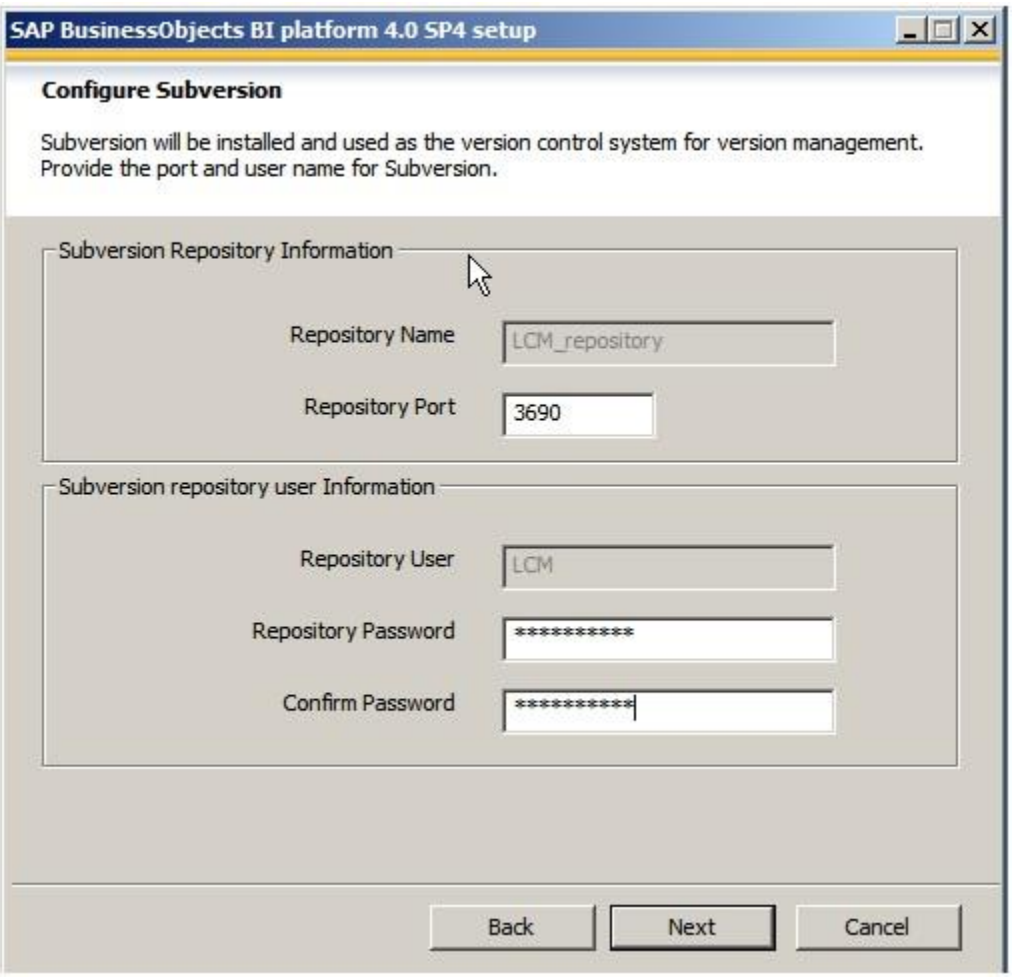
22. Make sure the **Start server upon installation** check box is selected, and click **Next**.



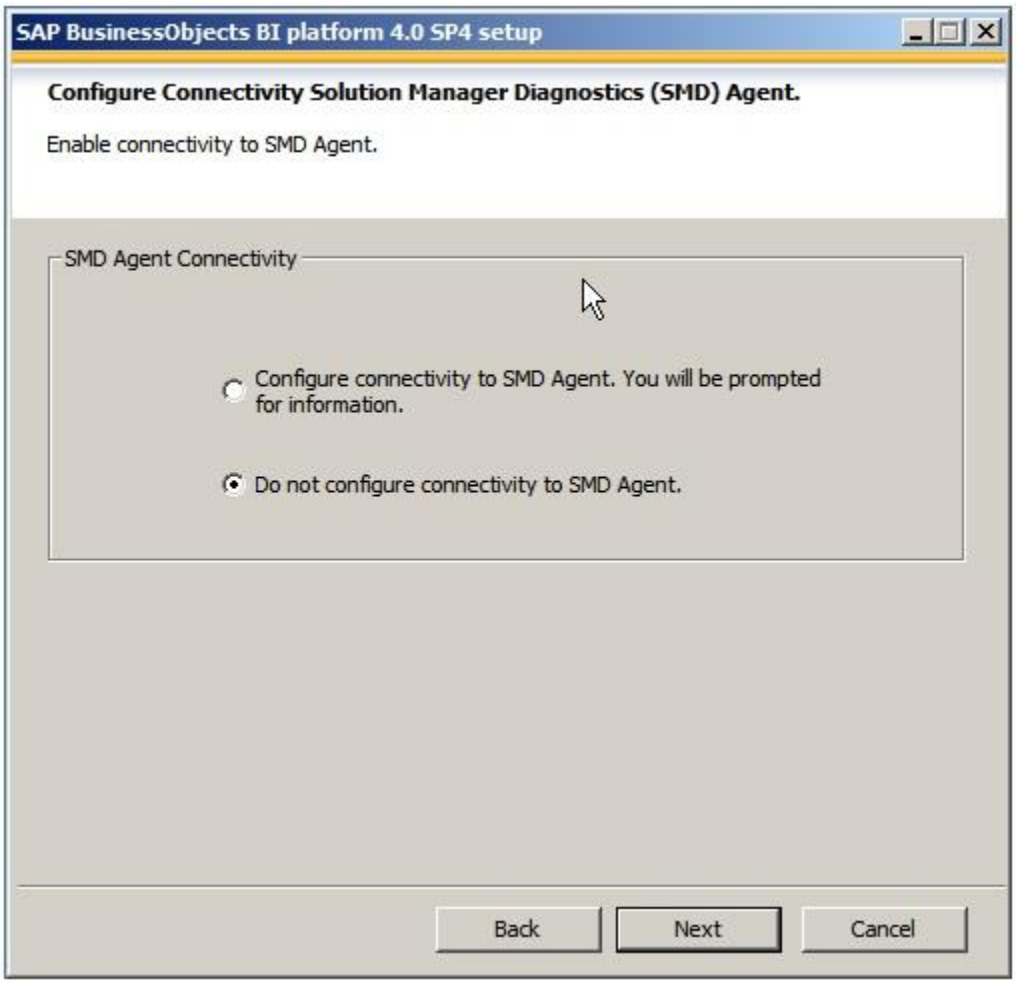
23. Leave the default port for the HTTP listening Port to 6405, and click **Next.**



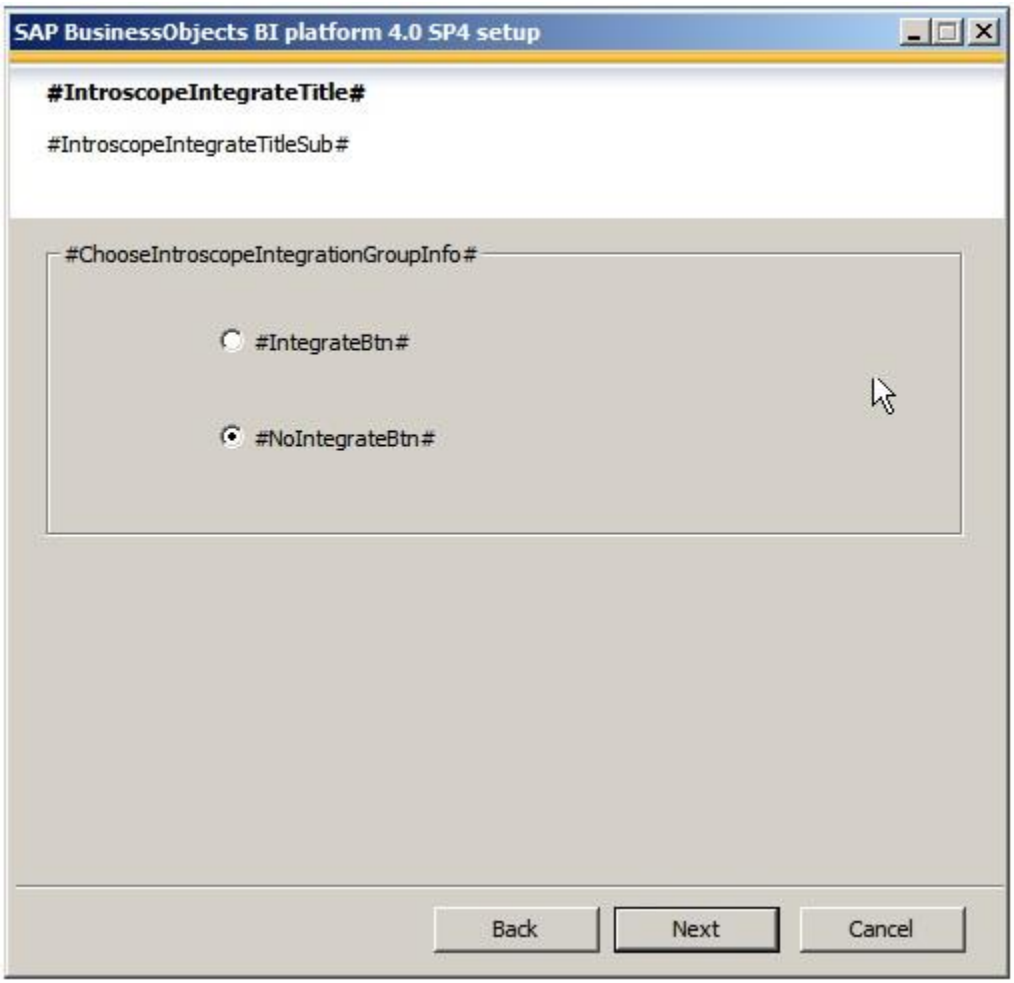
24. Specify a port for the LCM repository, type the password for the Repository User account, and then click **Next**.



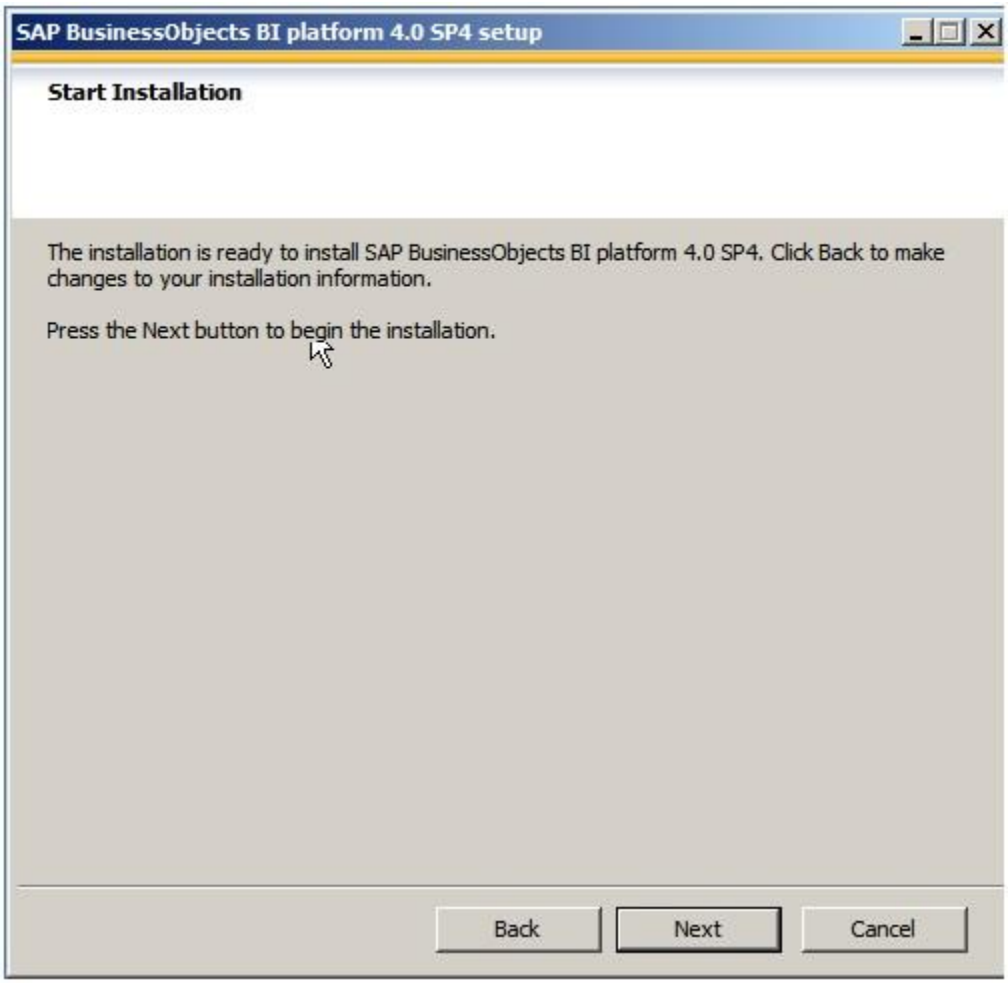
25. Click **Do not configure connectivity to SMD Agent**, and click **Next**.



26. Click **#NoIntegrateBtn#**, and click **Next**.



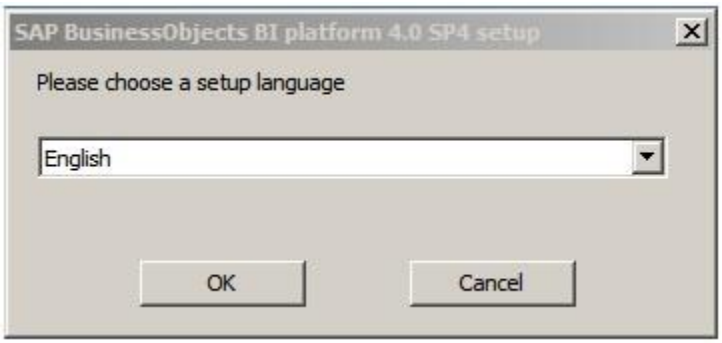
27. To start the installation, click **Next**.



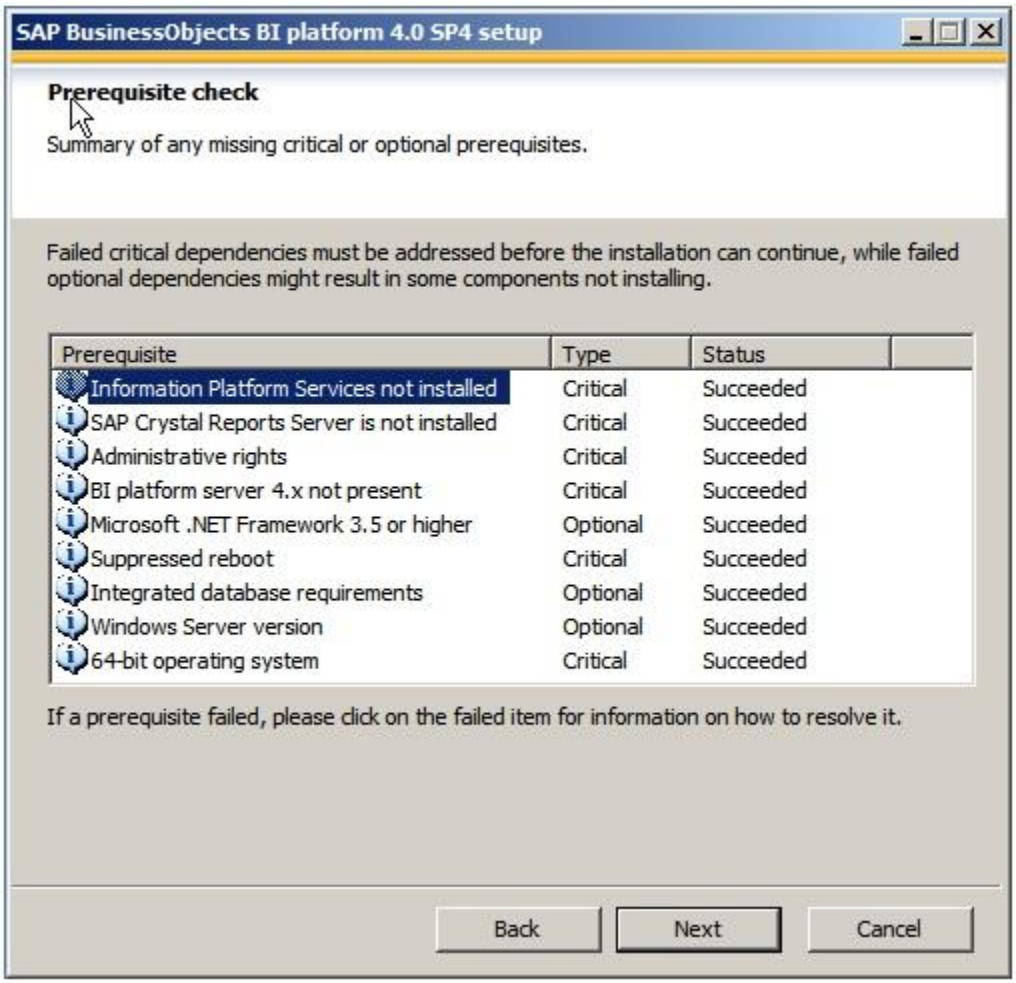
Configuring and installing BI platform on server 2

To install BI platform on server 2

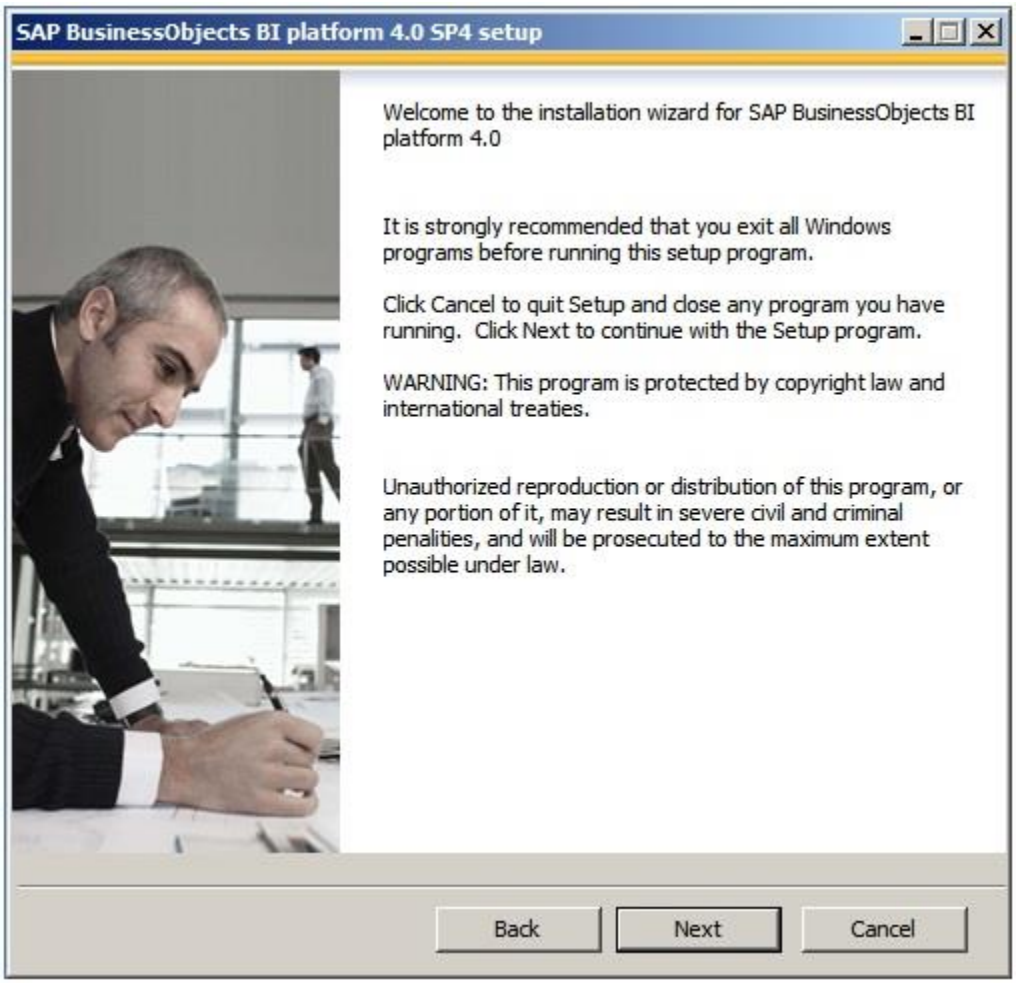
1. Log in to VANTGVMWINPB05.pgdev.sap.corp as Administrator.
2. Go to the "SAP BusinessObjects" folder, open it, and double-click Setup.exe.
3. On the "SAP BusinessObjects BI platform 4.0 SP4 setup" page, select **English**, and then click **OK**.



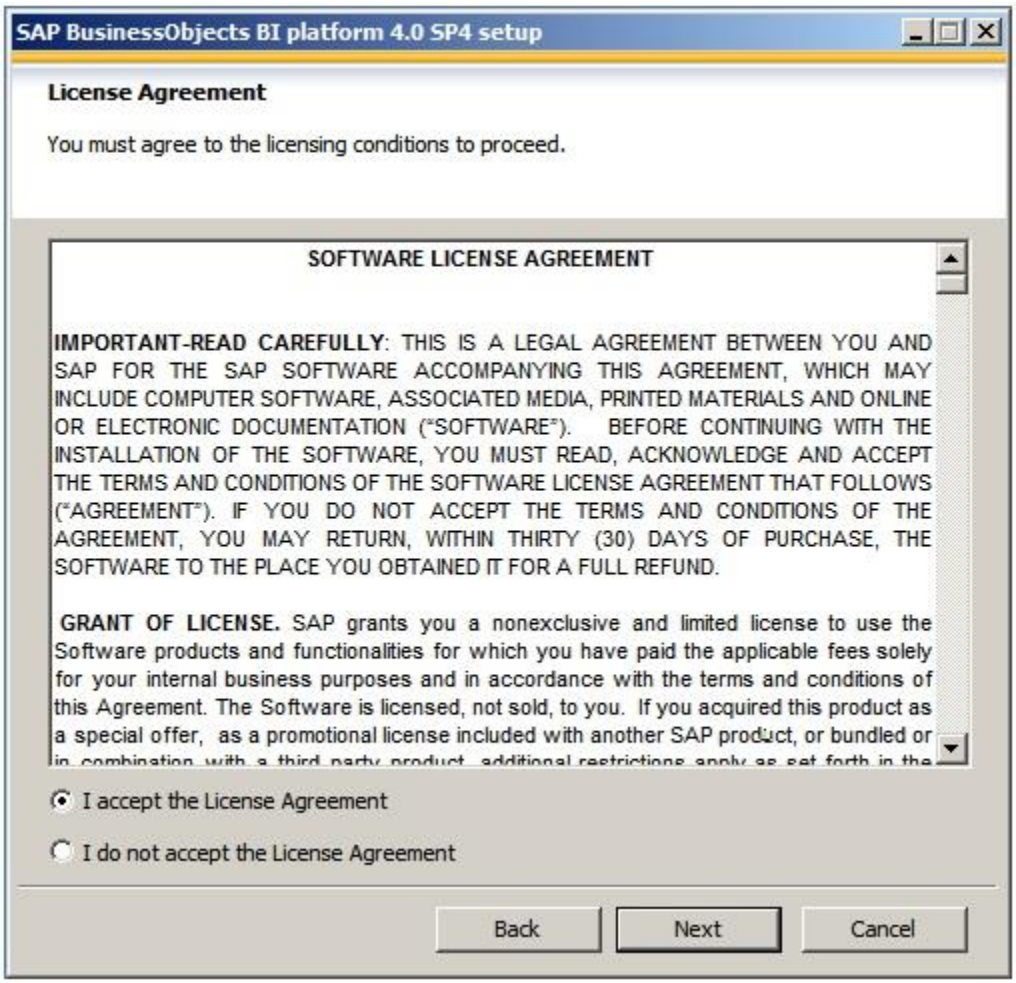
4. When the prerequisite system check completes successfully, click **Next**.



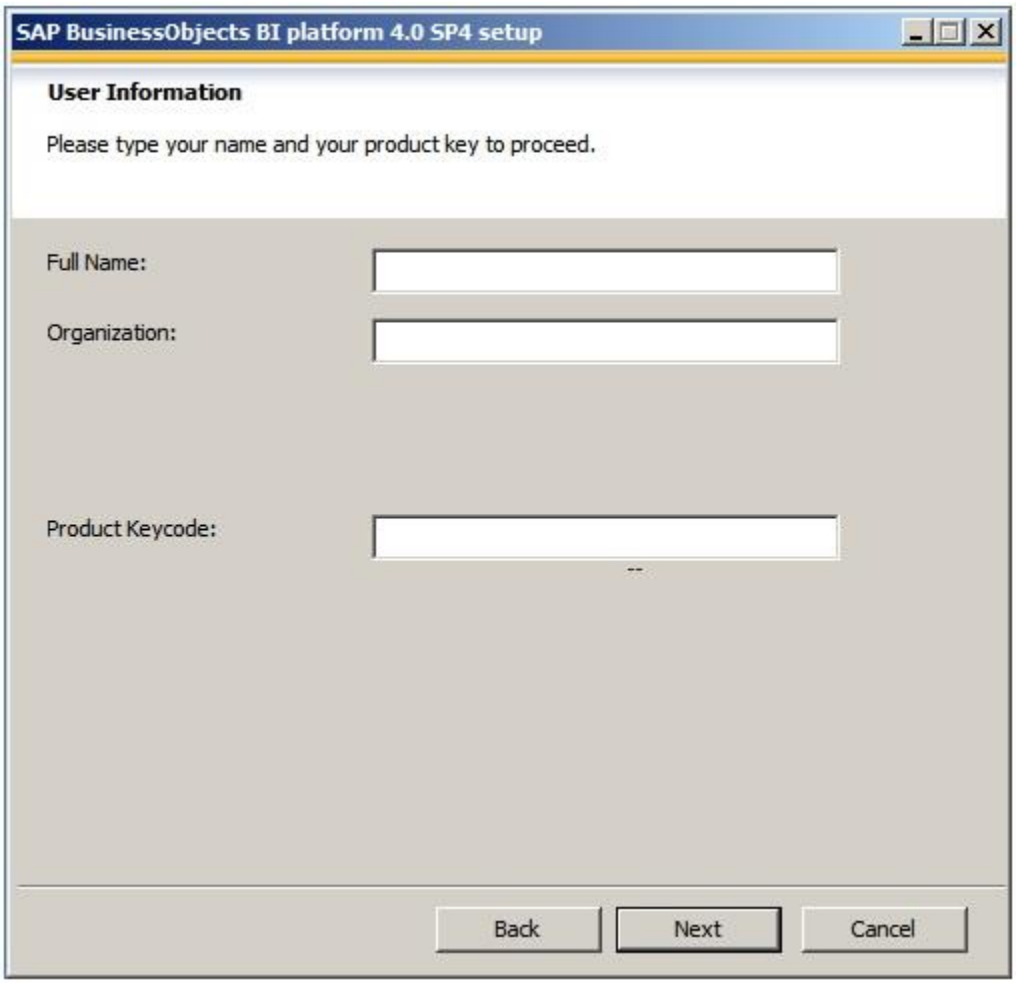
5. On the "SAP BusinessObjects BI platform 4.0 SP4 setup" page, click **Next**.



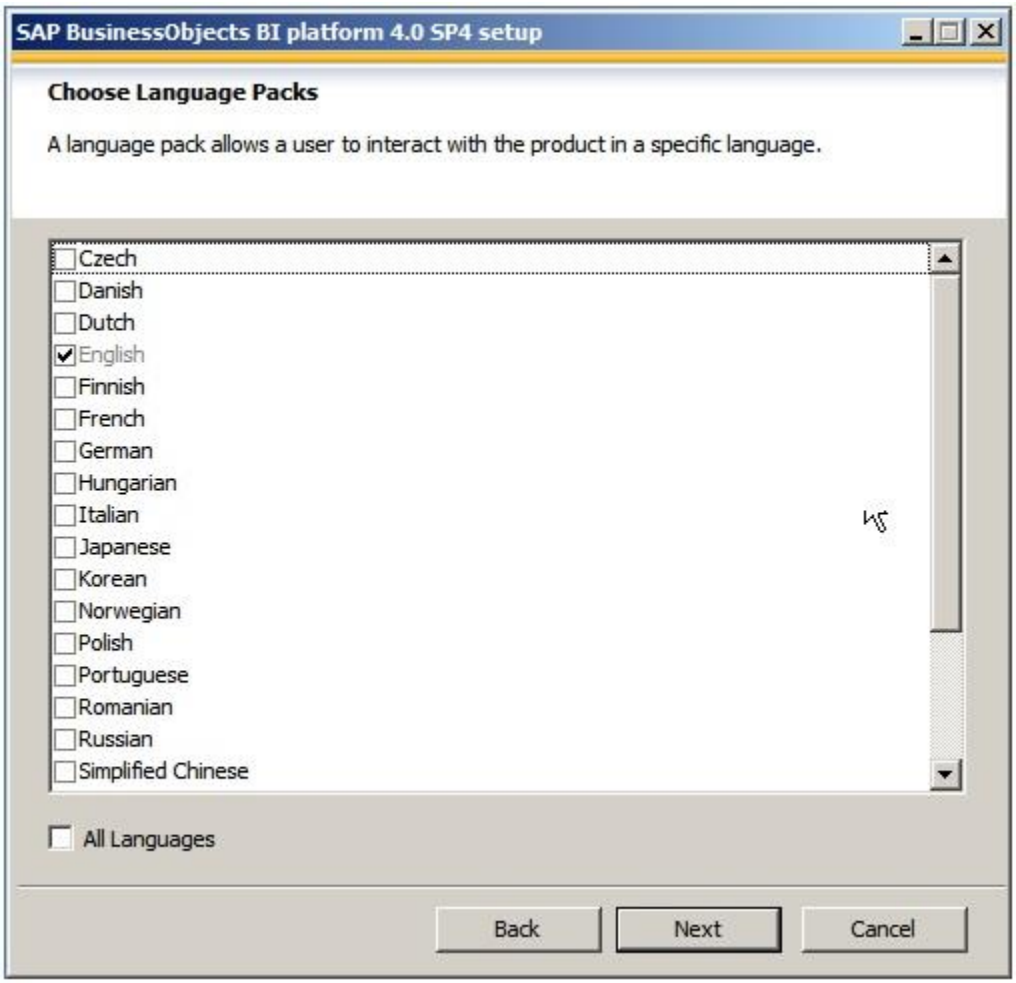
6. Accept the License Agreement, and click **Next**.



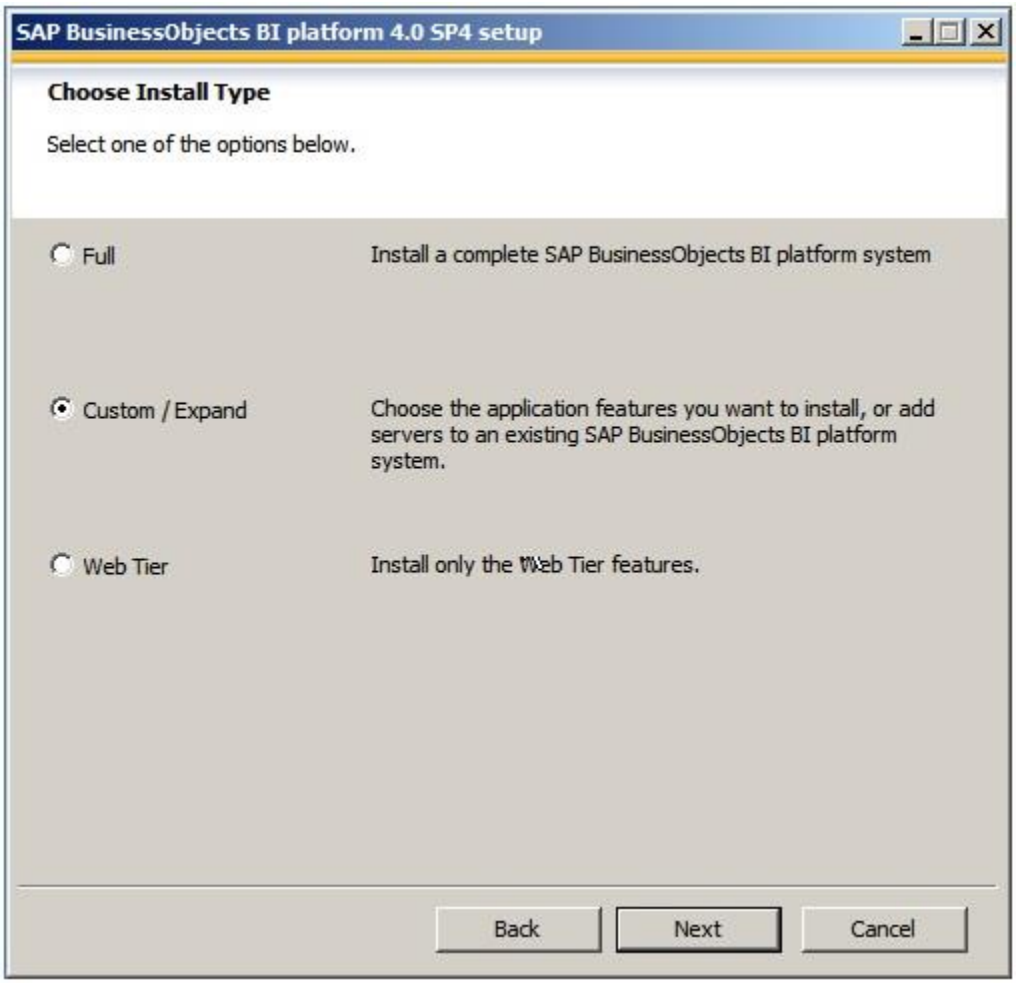
7. Type the information required for the **Full Name**, **Organization**, and **Product Keycode** boxes, and then click **Next**.



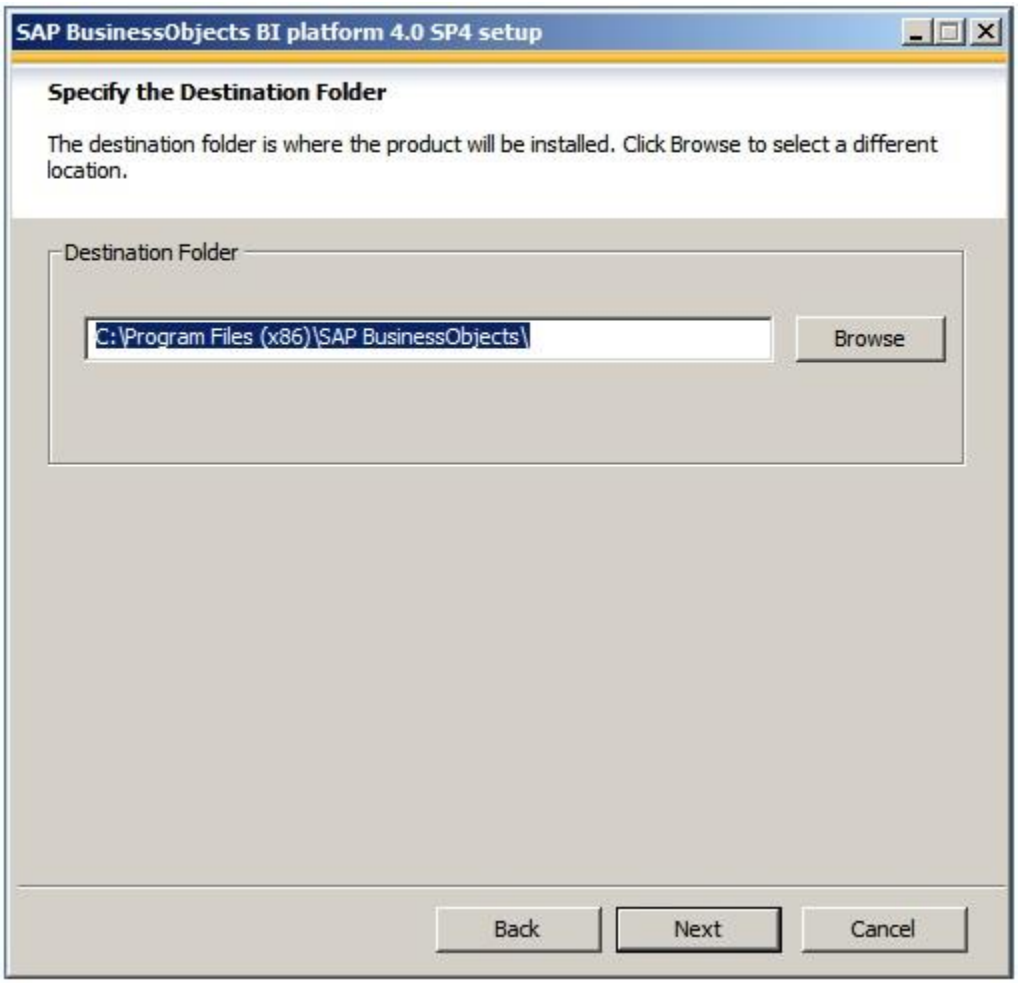
8. Click **Next** to accept the default language (English).



9. Click **Custom/Expand**, and click **Next**.

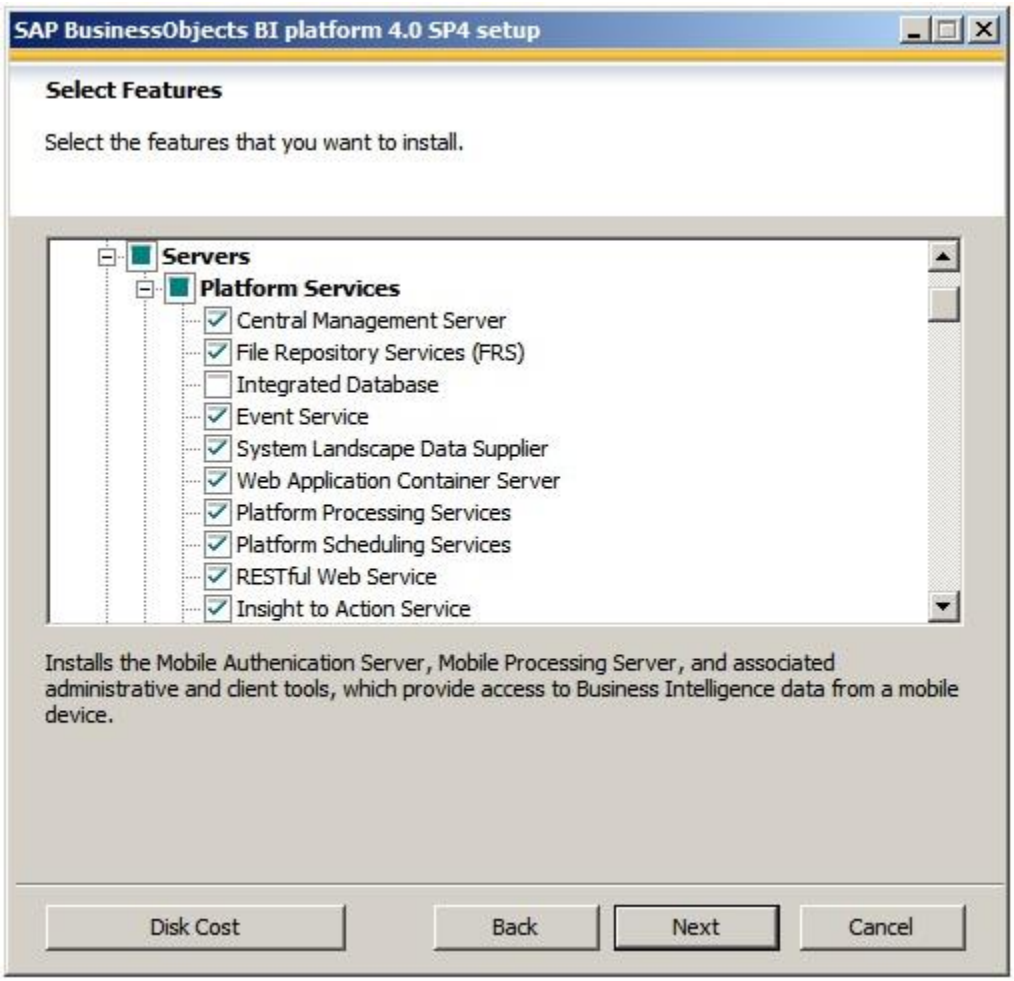


10. Click **Next** to accept the default path to the folder where the program will be installed.

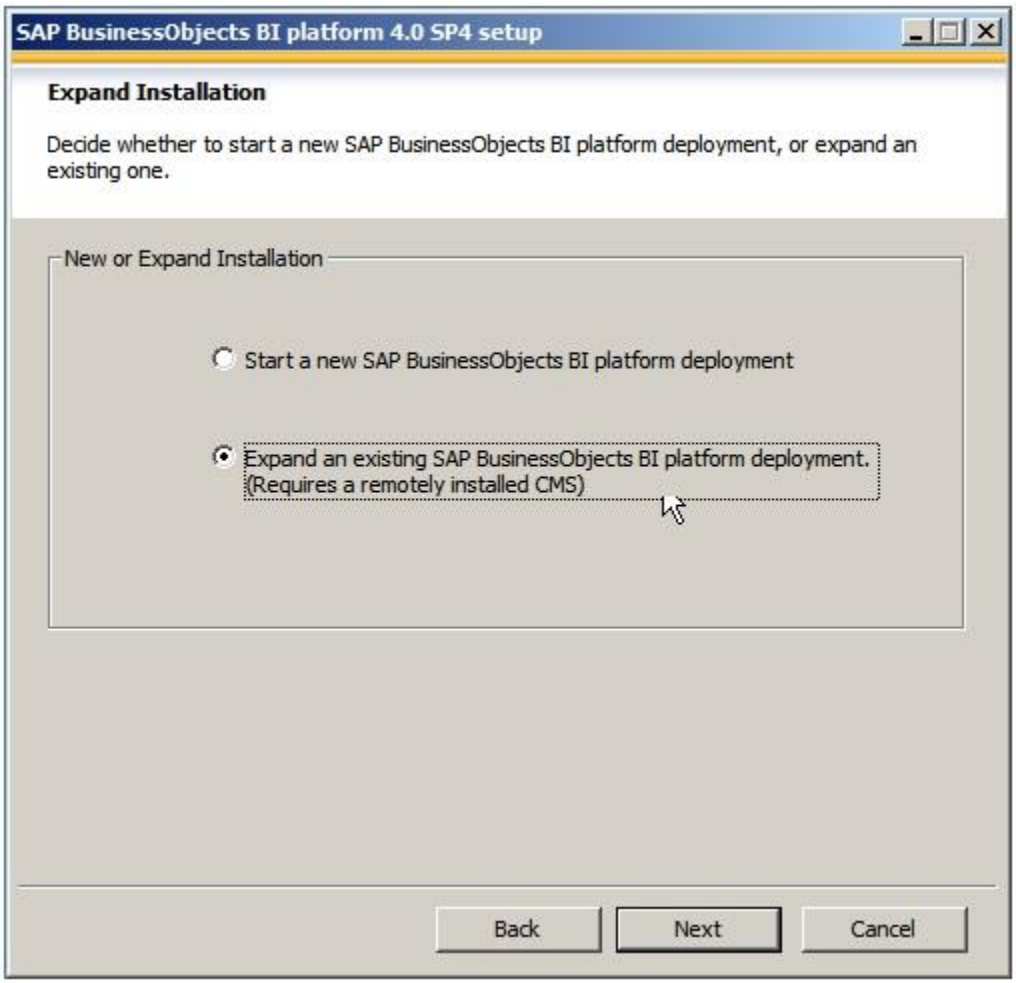


11. Clear the check boxes under **Web Tier**.

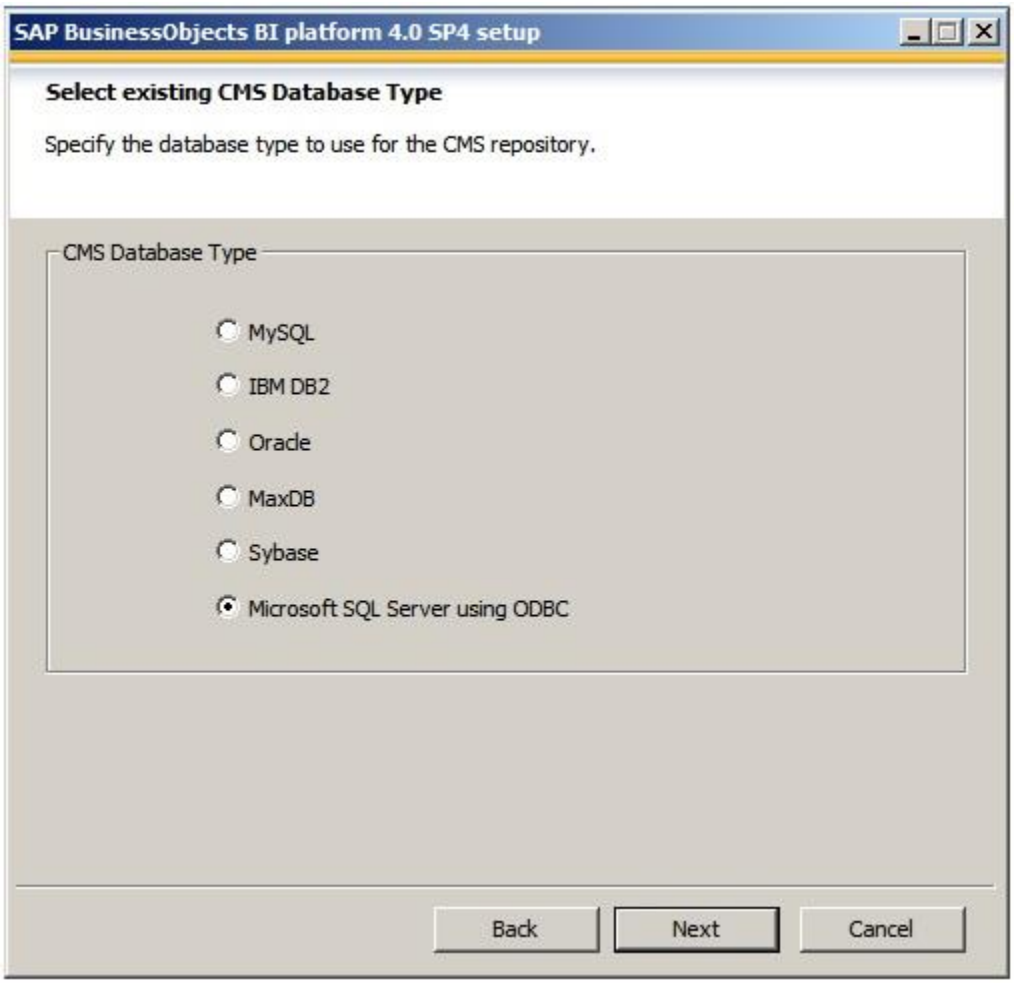
12. Expand **Platform Services**, and clear the following check boxes: **Web Tier**, **Integrated Database**, **Subversion**, and **Mobile Servers**, and then click **Next**



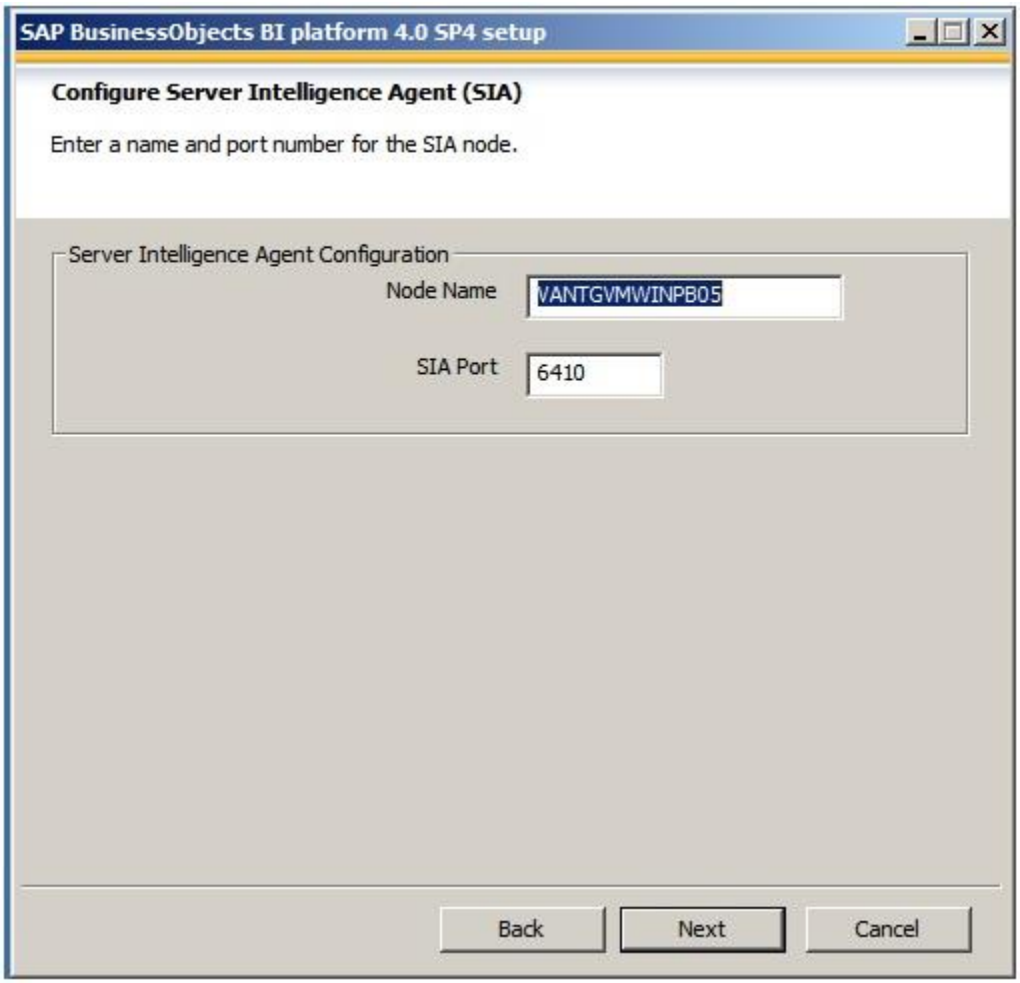
13. On the "Expand Installation" page, click **Start a new SAP BusinessObjects BI Platform deployment**, and click **Next**.



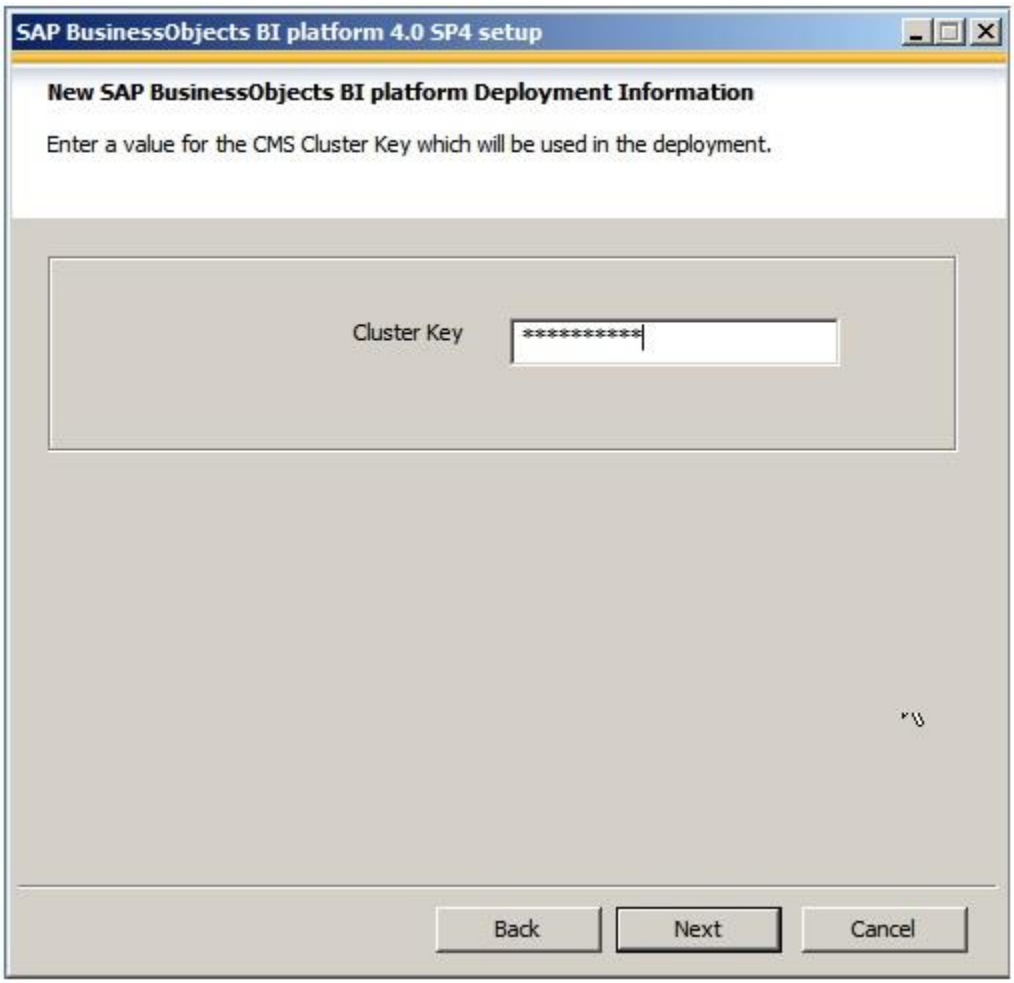
14. For use as the CMS database, click **Microsoft SQL Server using ODBC**, and click **Next**.



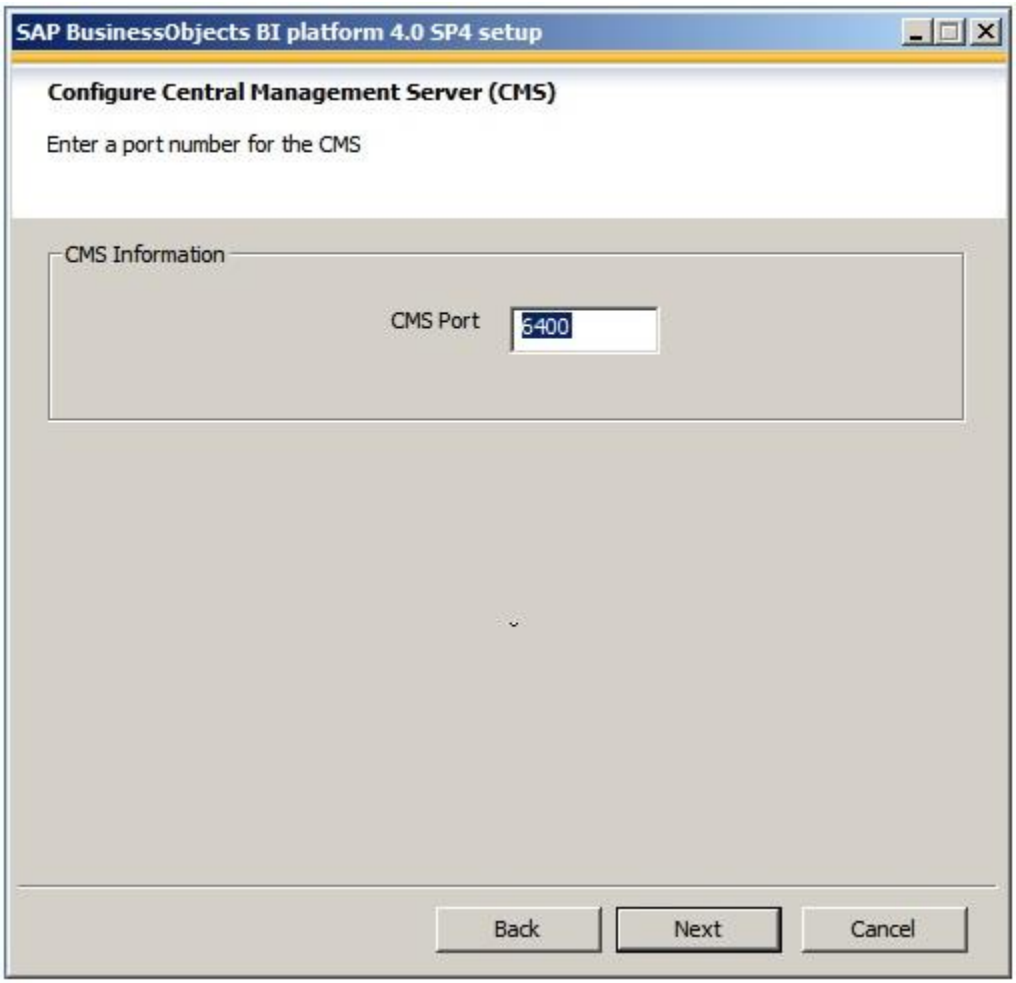
15. In the **Node Name** box, type the SIA name, leave the default SIA port to 6410, and then click **Next**.



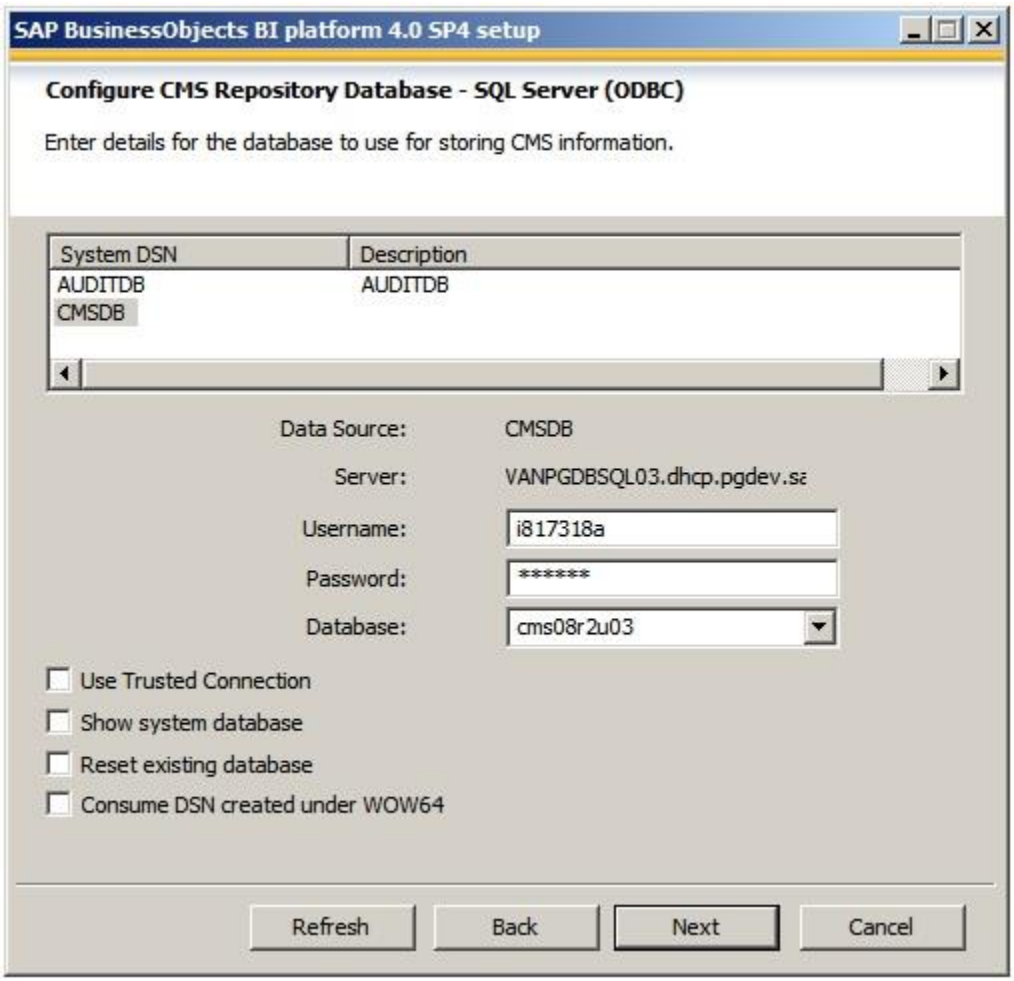
16. Type the Cluster key that you used to install server one, and click **Next**.



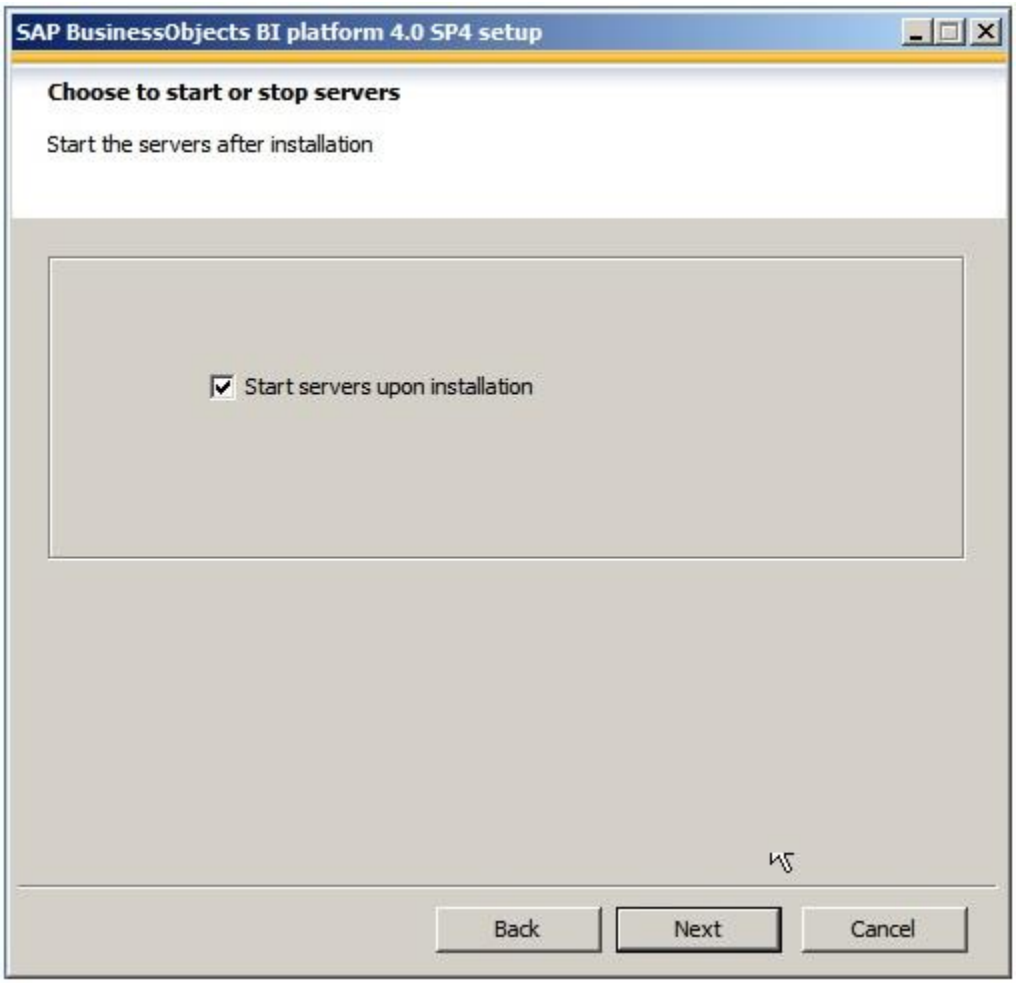
17. Leave the default port for the CMS to 6400, and click Next.



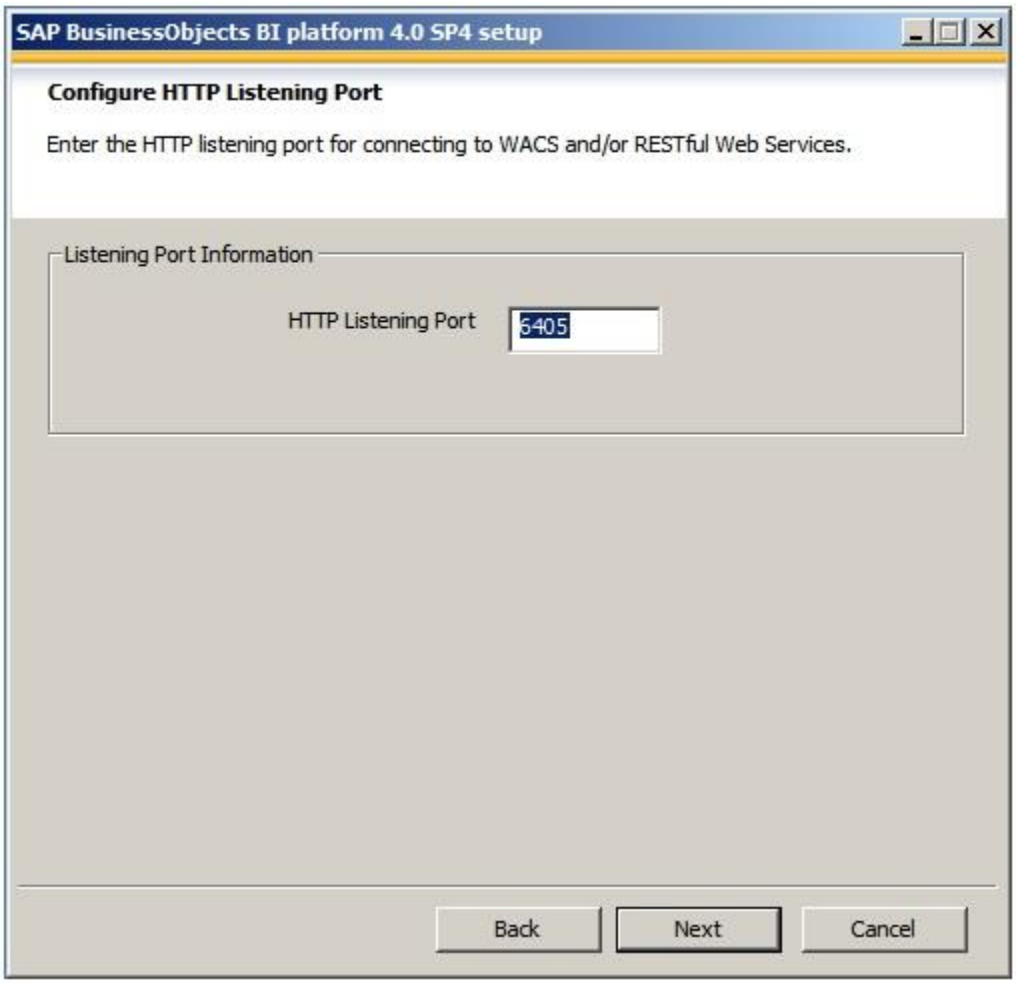
18. Type the login credentials for the CMS database, and click **Next**.



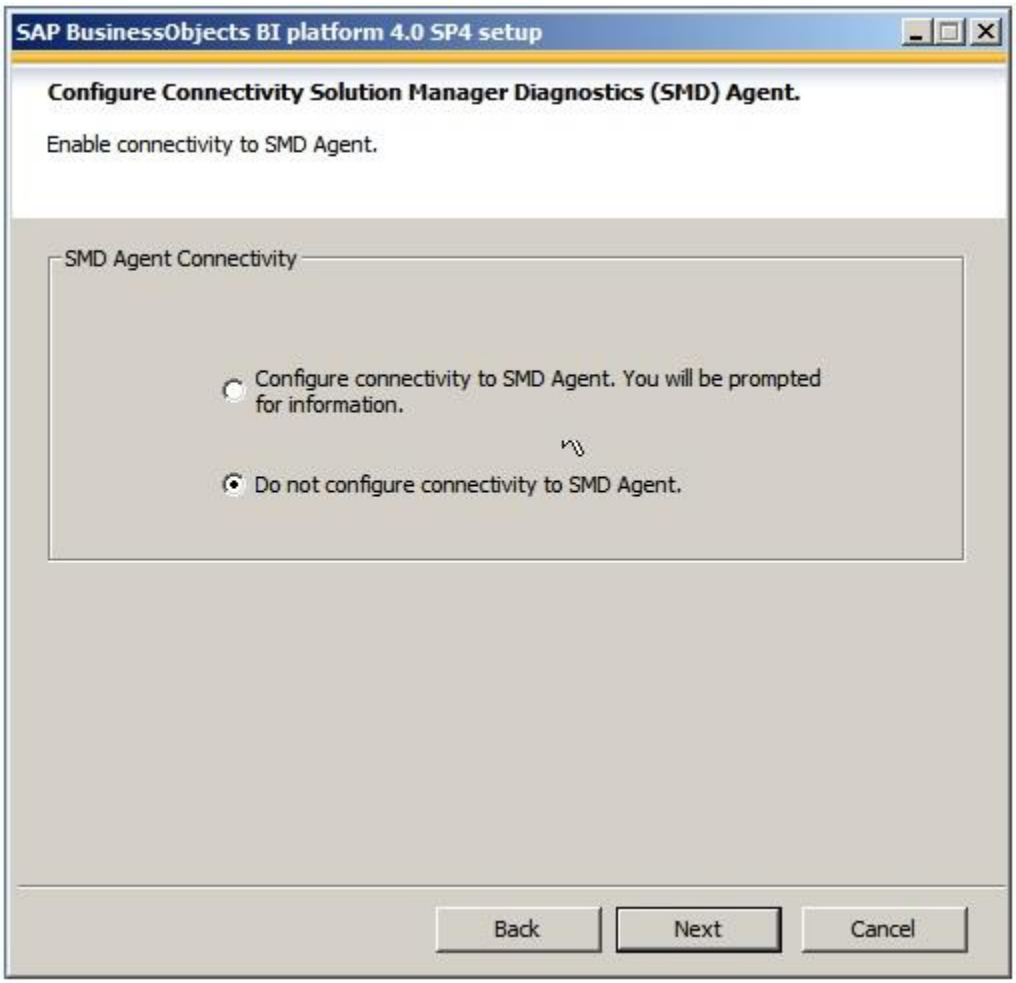
19. Make sure the **Start server upon installation** check box is selected, and click **Next**.



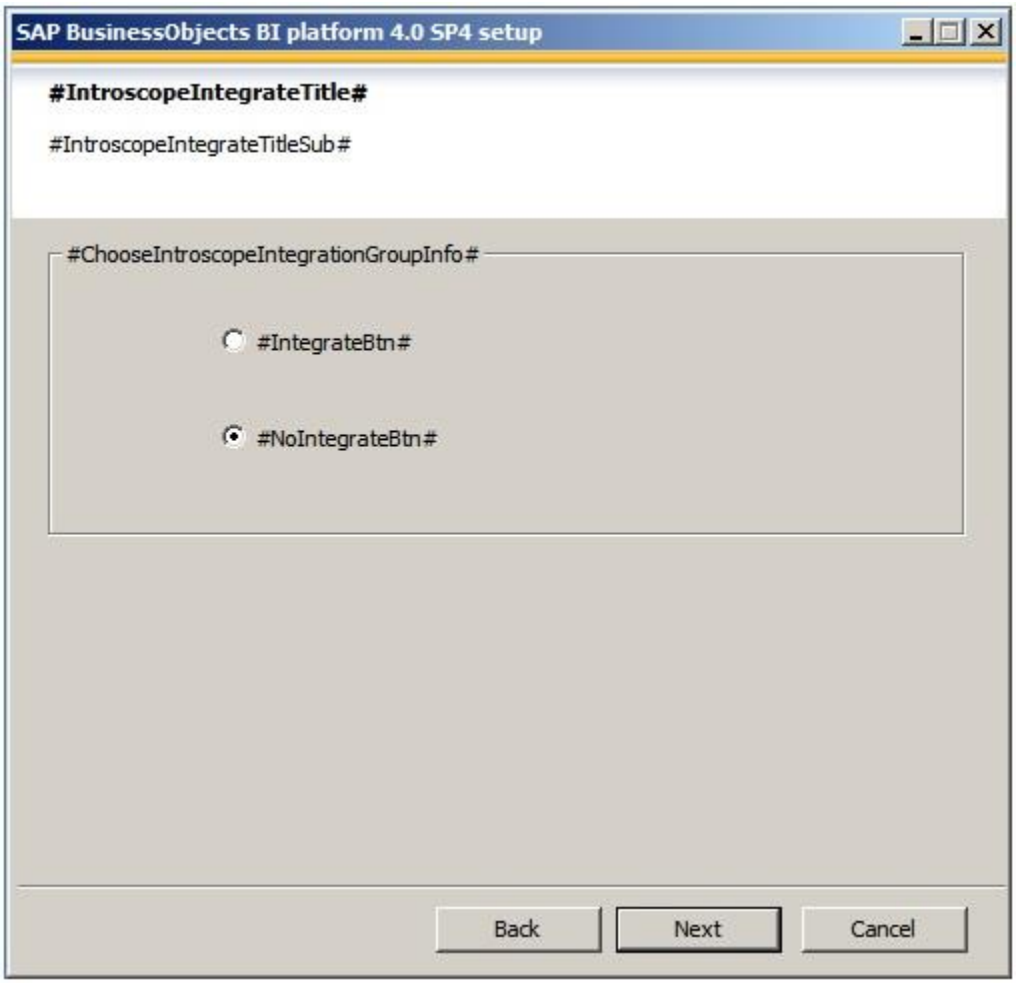
20. Leave the default port for the HTTP listening Port to 6405, and click **Next**.



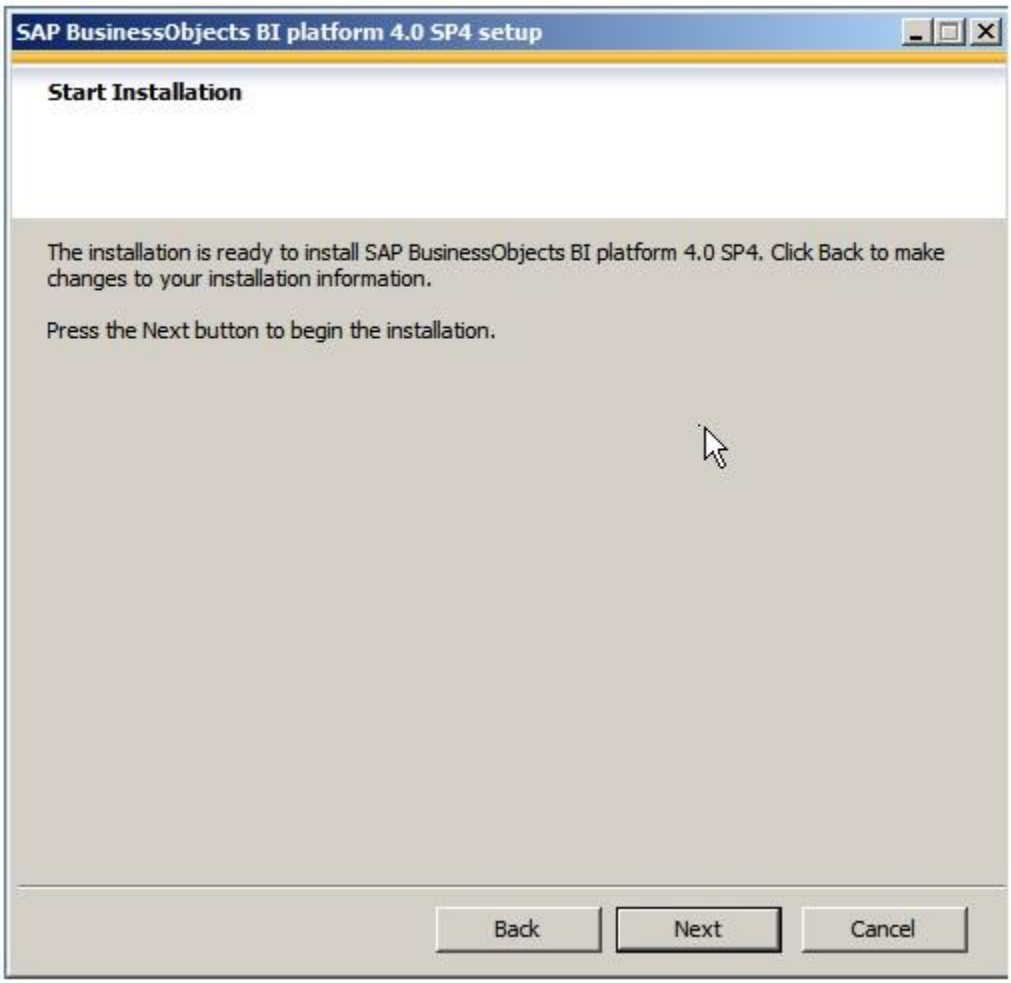
21. Click **Do not configure connectivity to SMD Agent**, and click **Next**.



22. Click **#NoIntegrateBtn#**, and click **Next**.



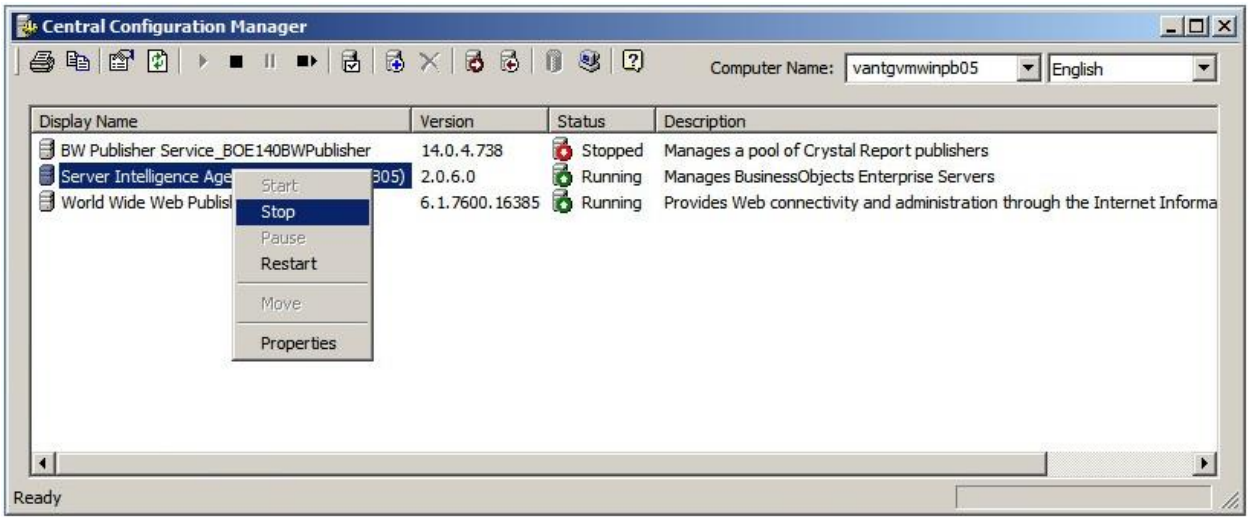
23. To start the installation, click **Next**.



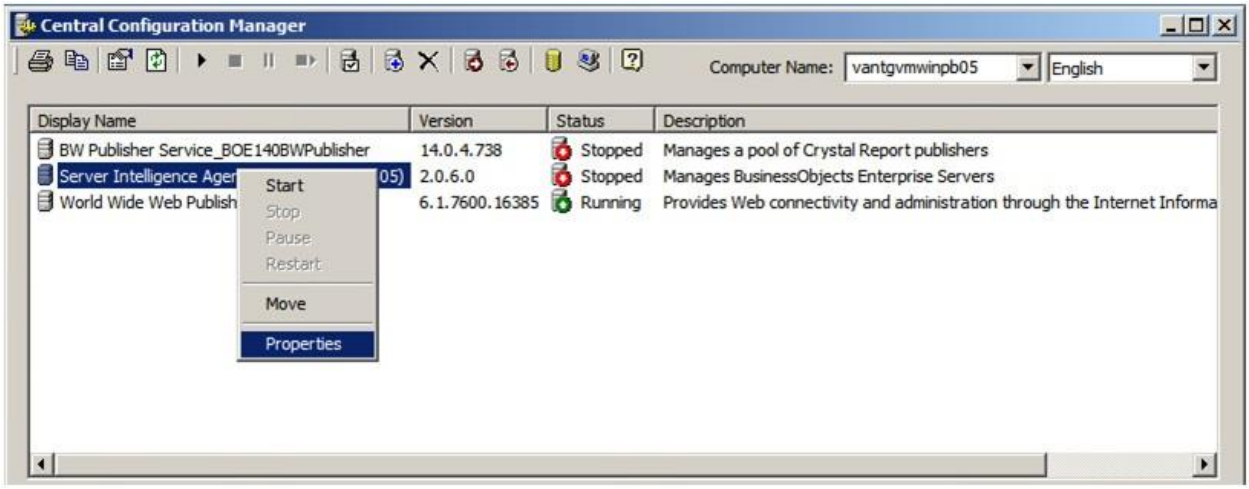
Changing the cluster name

To change the cluster name

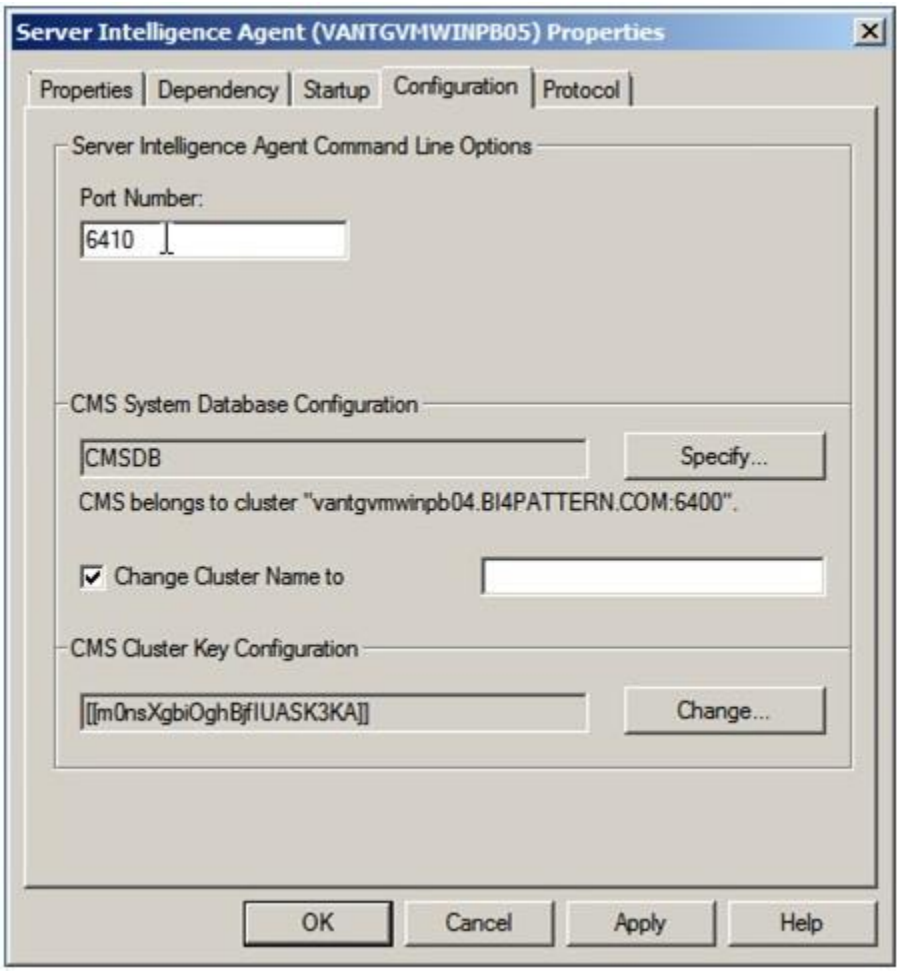
1. Log in to Vantgvmwinpb05.
2. Click **Start** > **All Programs** > **SAP BusinessObjects BI Platform 4** > **SAP BusinessObjects BI platform** > **Central Configuration Manager**.
3. Right-click **Server Intelligence Agent**, and click **Stop**.



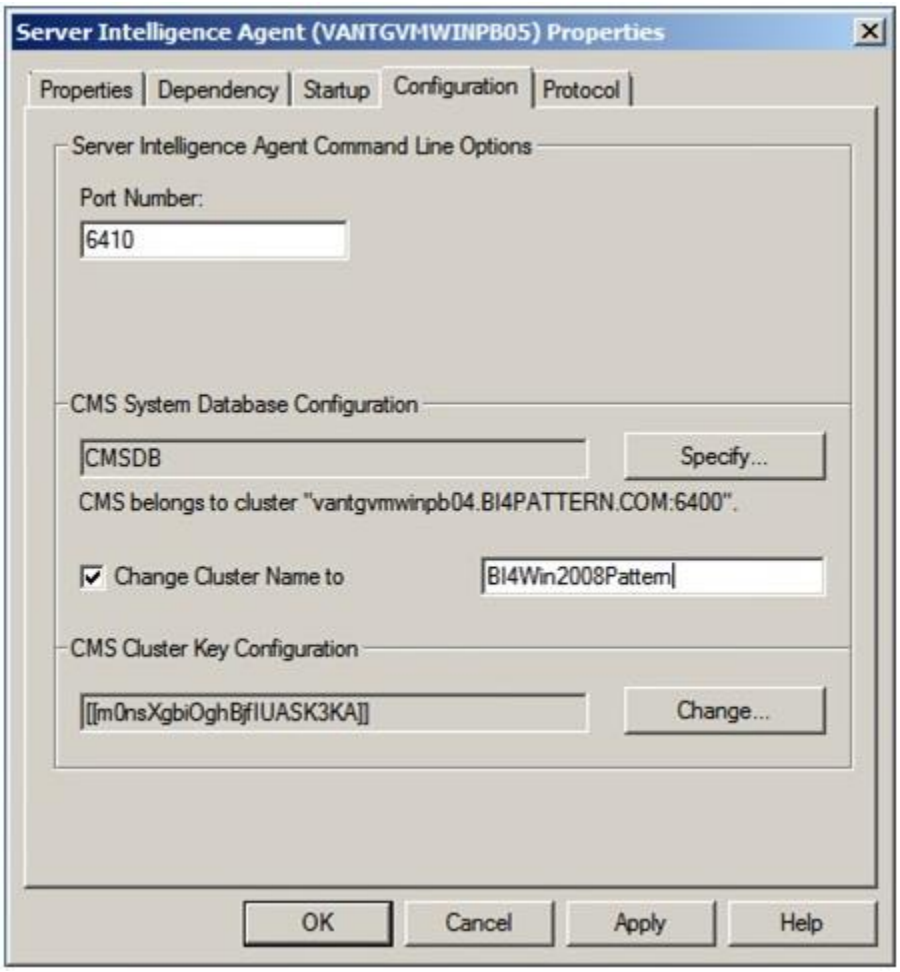
4. Right-click Server Intelligence Agent, and click Properties.



5. On the Configuration tab, select the Change Cluster Name to check box.



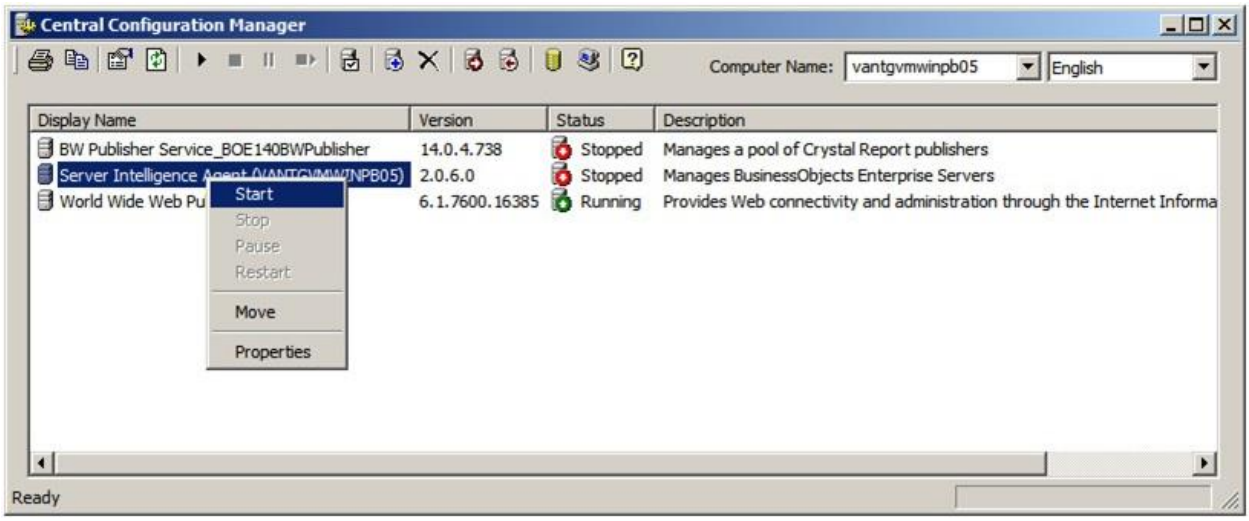
6. Type the new cluster name as follows: BI4Win2008Pattern.



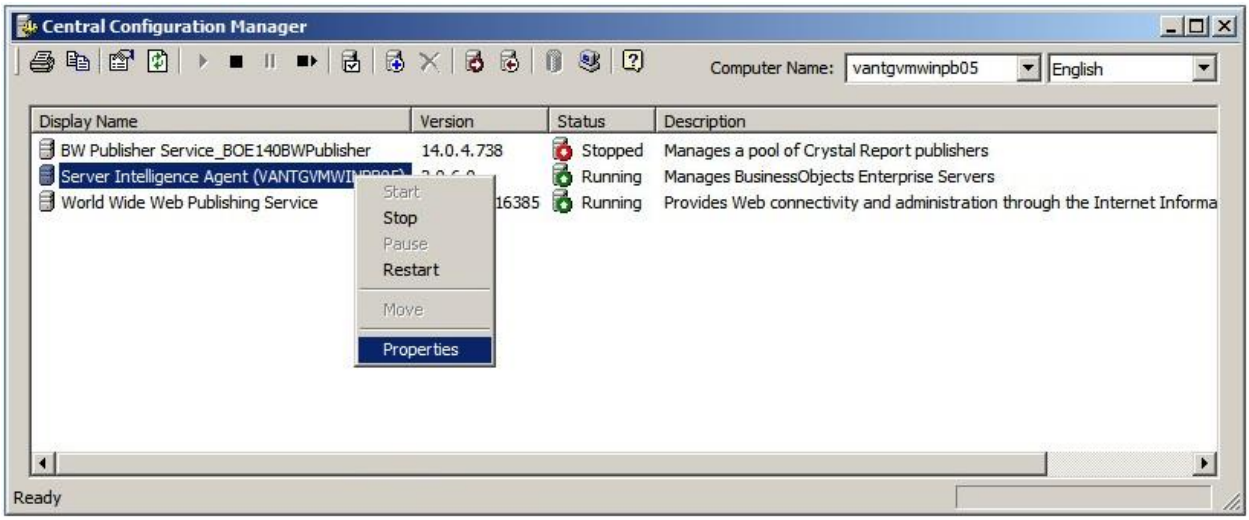
7. Click **Apply**, and then click **OK**.

To verify that the cluster name was changed

1. To start the SIA, in the "Central Configuration Manager" dialog box, right-click **Server Intelligence Agent,** and click **Start**.

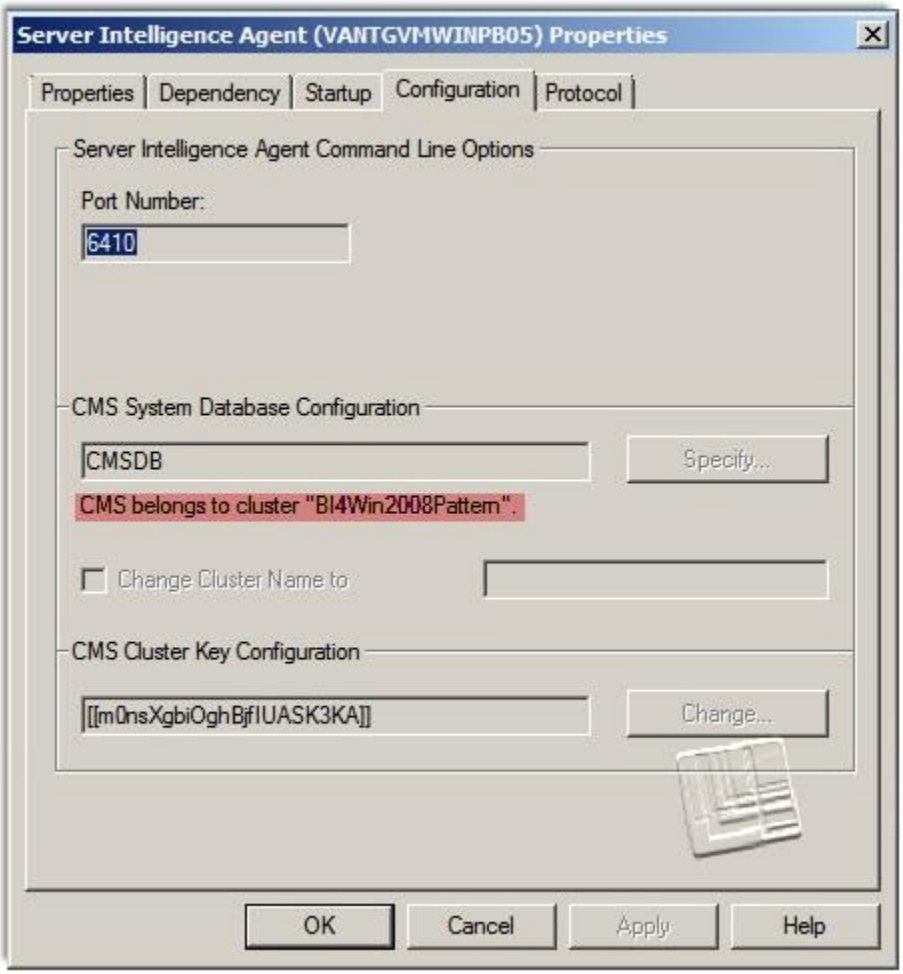


2. When the "Status" column displays "Running" for **Server Intelligence Agent**, right-click **Server Intelligence Agent**, and click **Properties**.



3. The "Server Intelligence Agent Properties" dialog box opens.

4. On the **Configuration** tab, verify that the "CMS System Database Configuration" area indicates the following: CMS belongs to cluster “BI4Win2008Pattern"



Splitting the Adaptive Processing Server (APS)

Best practices for splitting the APS

Many system-specific factors need to be considered when doing an APS split. For example:

- The number of CPUs and CPU cores used in the system.
- The amount of central memory.

As a result, this pattern does not provide instructions for doing an APS split because the configuration settings and combinations of those settings would vary from system to system.

For information to help you determine a split that is right for your system, and the goals you would like to accomplish with a split, refer to the following

guide: http://scn.sap.com/docs/DOC-31711. A strong background in BI platform 4.0 and understanding of your APS is recommended before performing a split.

Setting up the Application Server

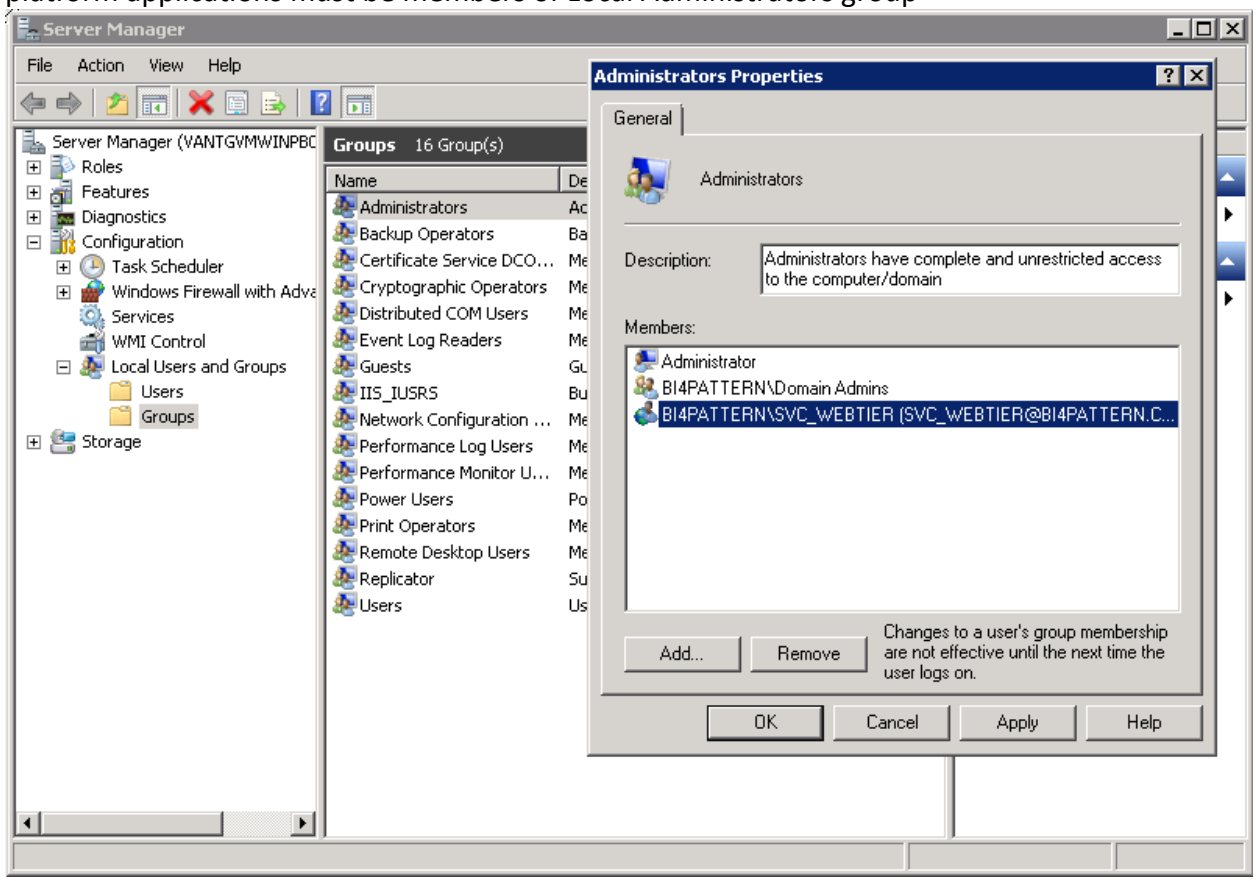
In this pattern, we set up two application server instances, running Tomcat 6.0.36 and will cluster them for session failover. The Tomcat server instances will use Java 1.7.0_09 as JDK.

We will be using 64bit versions of Tomcat and Java JDK.

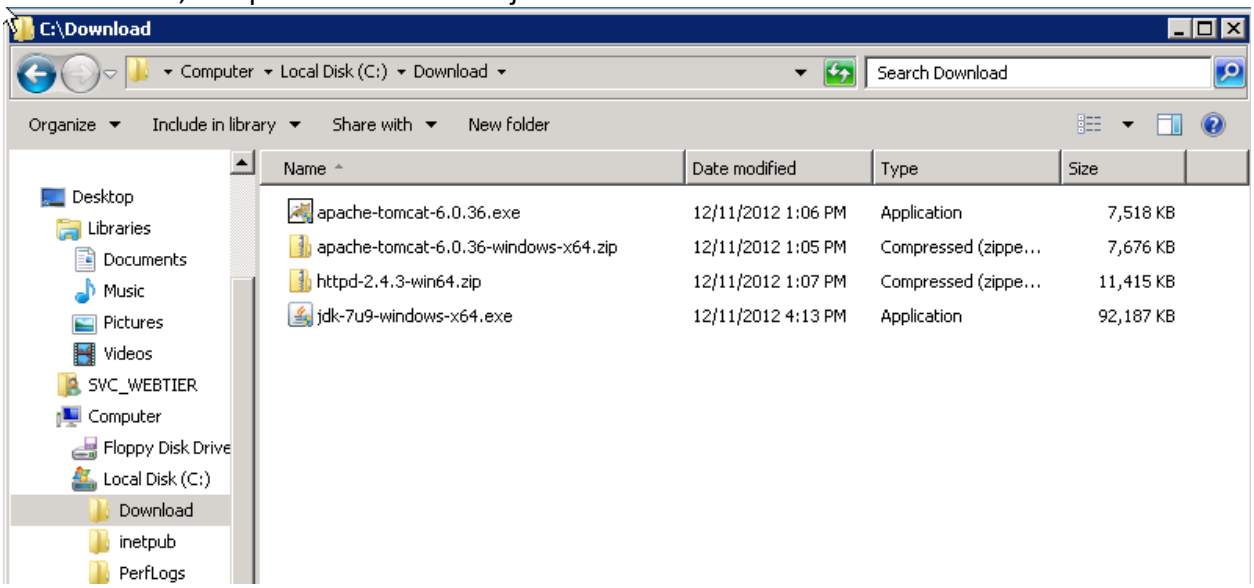
- Setting up Application Server 1
- Setting up Application Server 2
- Installing the BI platform web tier
- Configuring the Application Server Cluster

Setting up Application Server 1

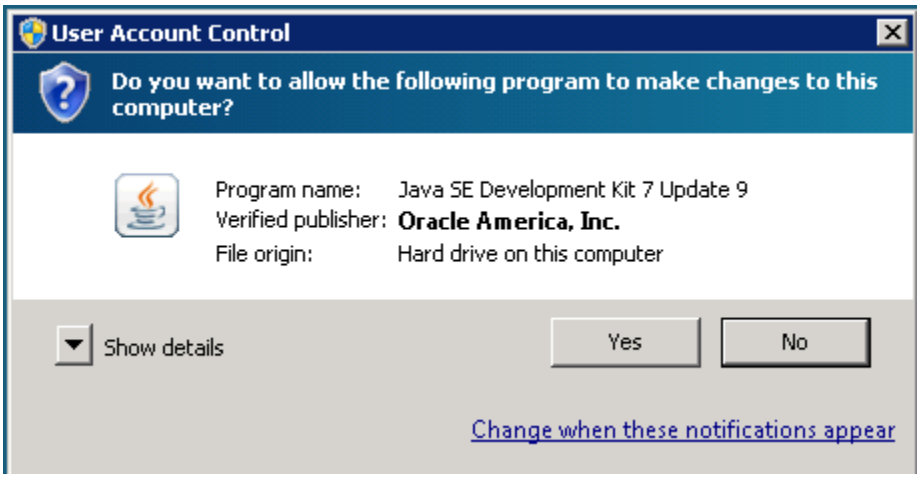
1. Log in to machine vantgvmwinpb02 using the account SVC_WEBTIER. SVC_WEBTIER is a domain user account and a member of local Administrators group. It is not enough to use Domain Administrator account because accounts used to install BI platform applications must be members of Local Administrators group

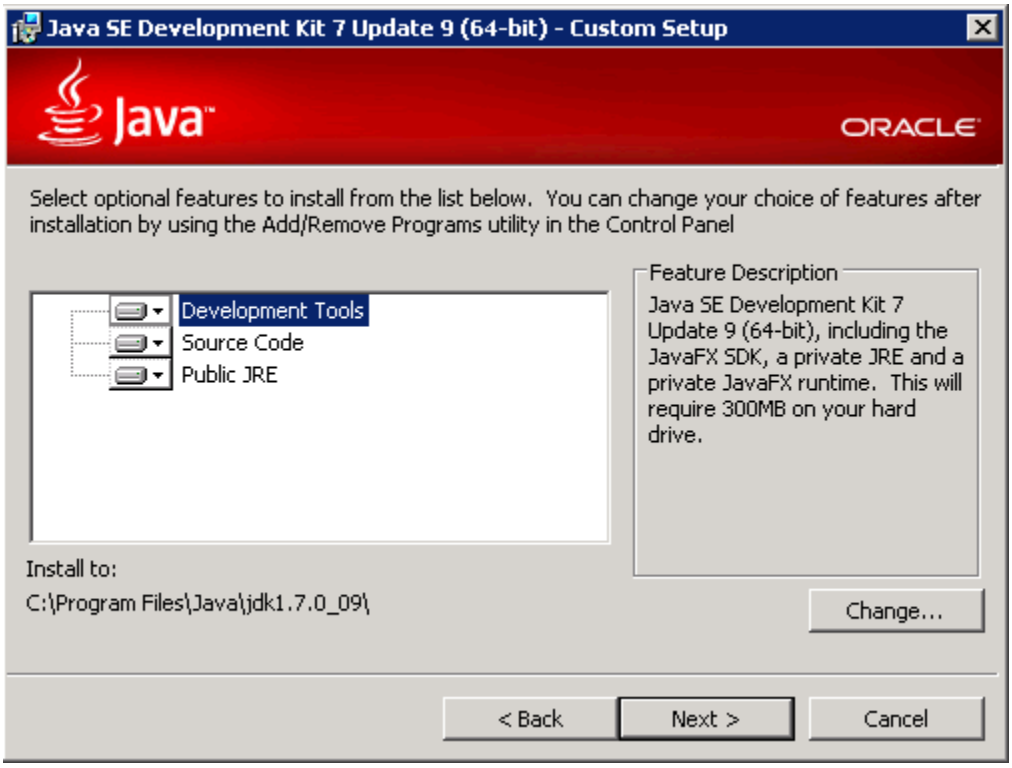


2. Download Installation packages for Tomcat and JDK from respective vendors.
   For the JDK, this patten uses version jdk-7u9-windows-x64.

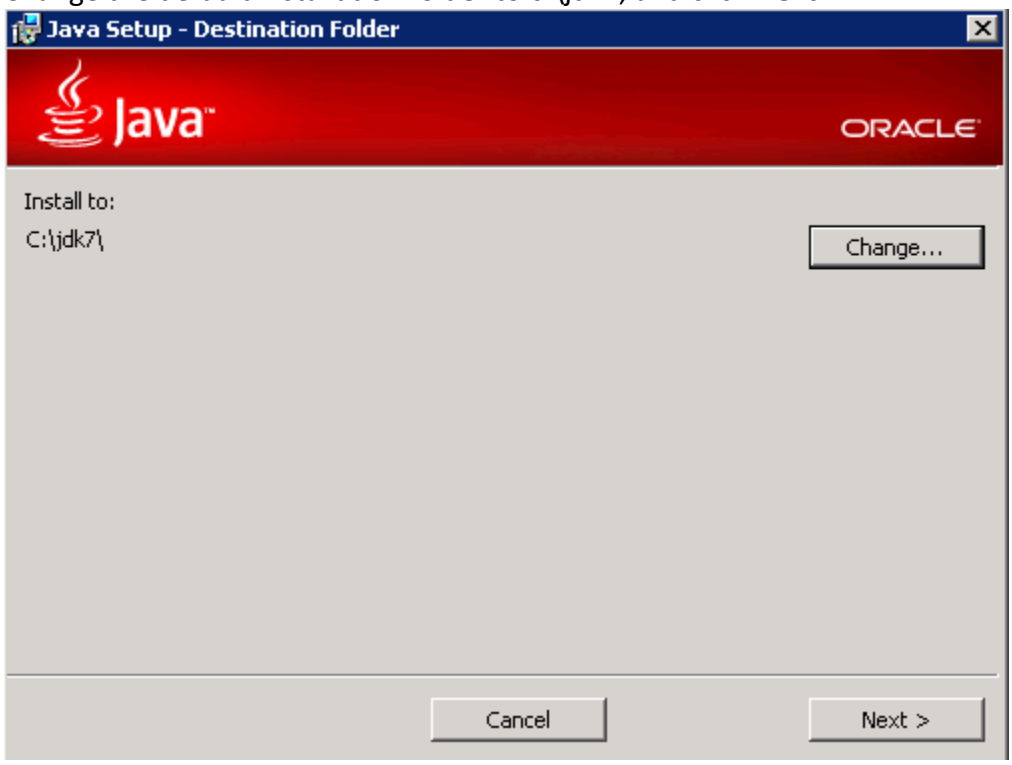


3. To install the JDK, double-click jdk-7u9-windows-x64.exe, and proceed through the installation wizard until you reach the "Destination Folder" page.



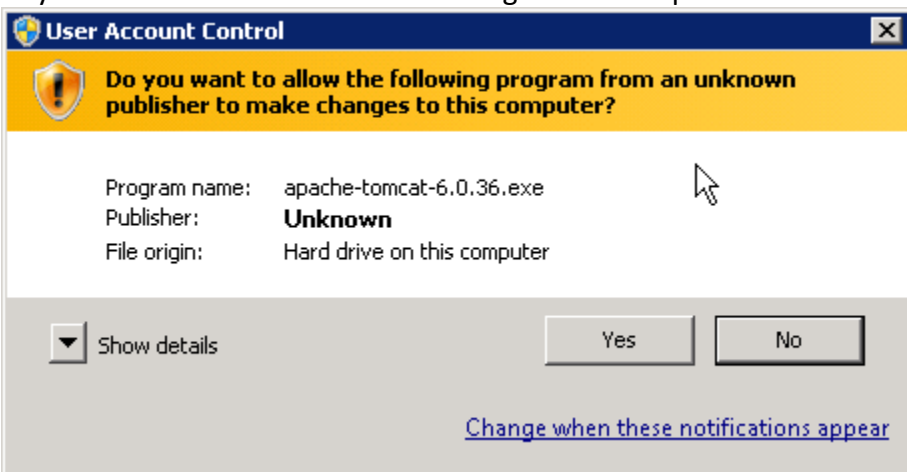


4. Change the default installation folder to c:\jdk7, and click **Next**.

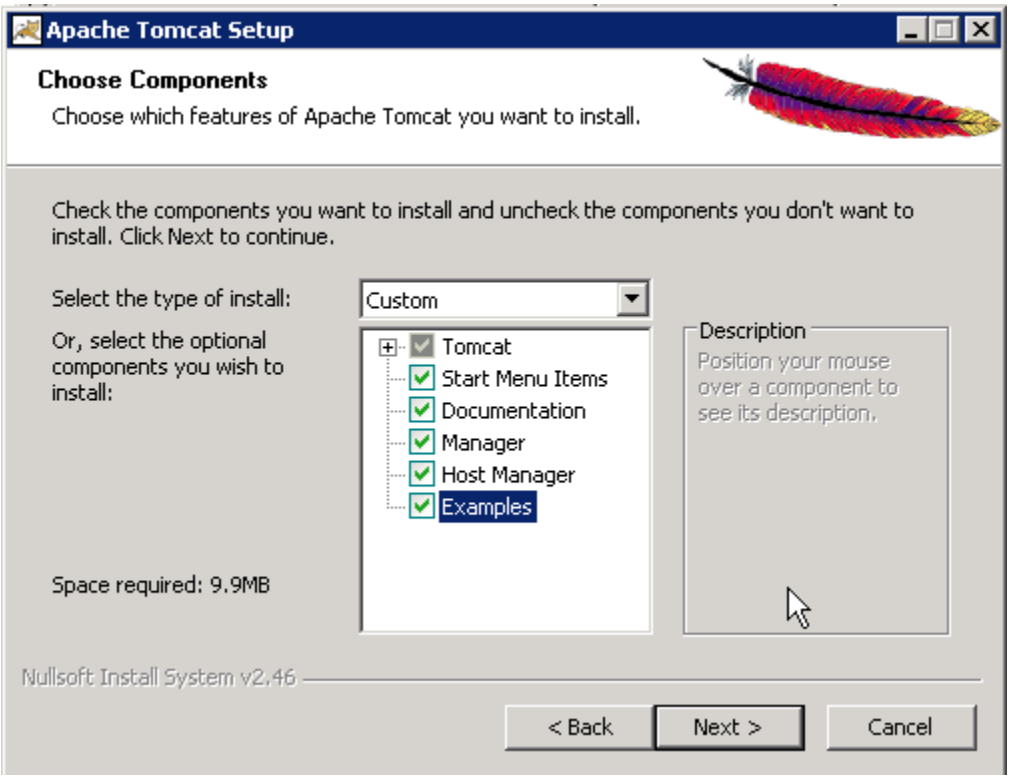


5. After the JDK installation is completed successfully, continue to install Apache Tomcat.

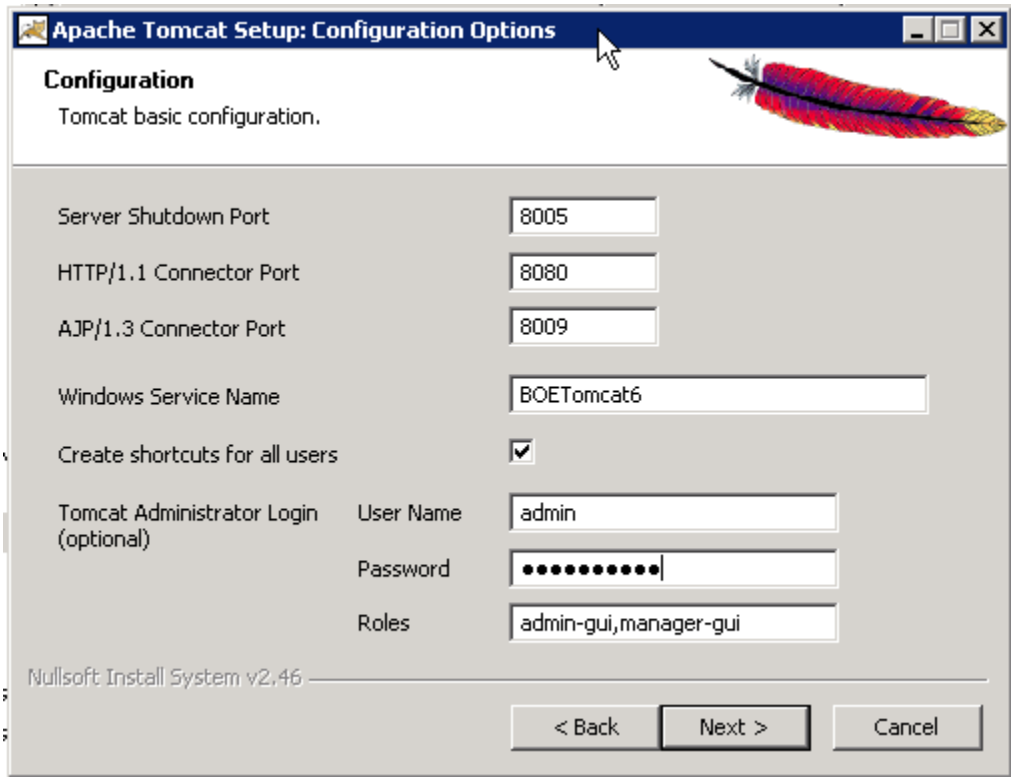
Since you are using non-default Administrator account, a security warnings will appear as you follow the installation and configurations steps:



6. Select the default Tomcat options, however, it is not required and all optional items below can be un-selected.



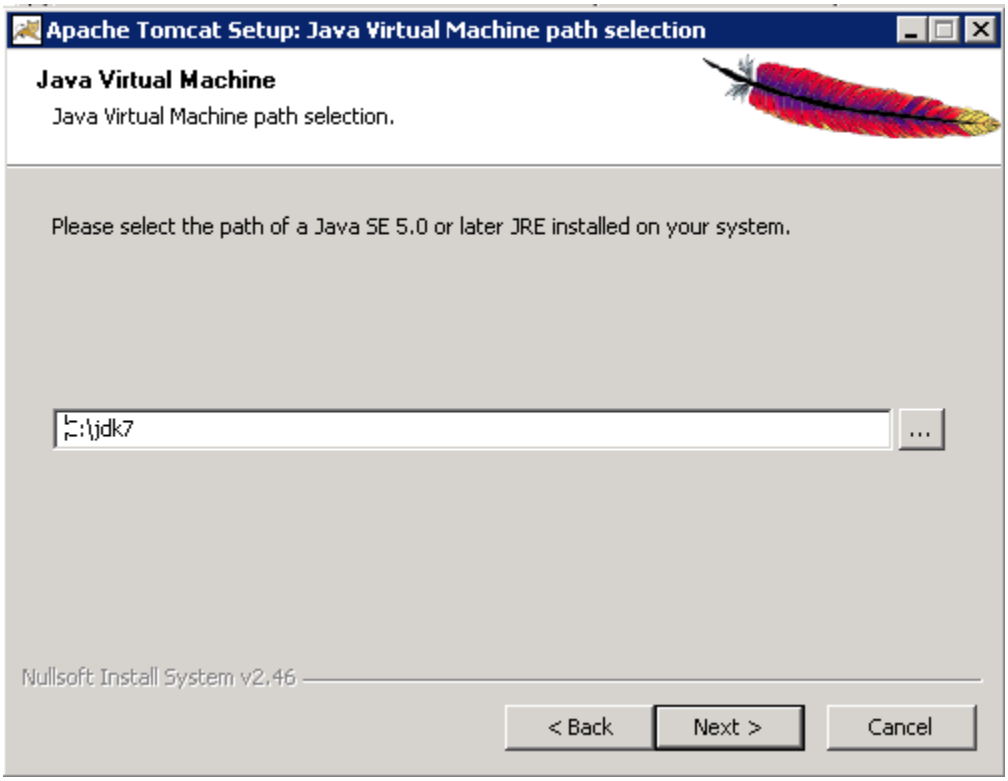
7. Select default Ports for Tomcat.
   Warning: Use what is the standard for your organization and make sure your selection is documented. It is easy to change this later, but proper documentation is paramount.



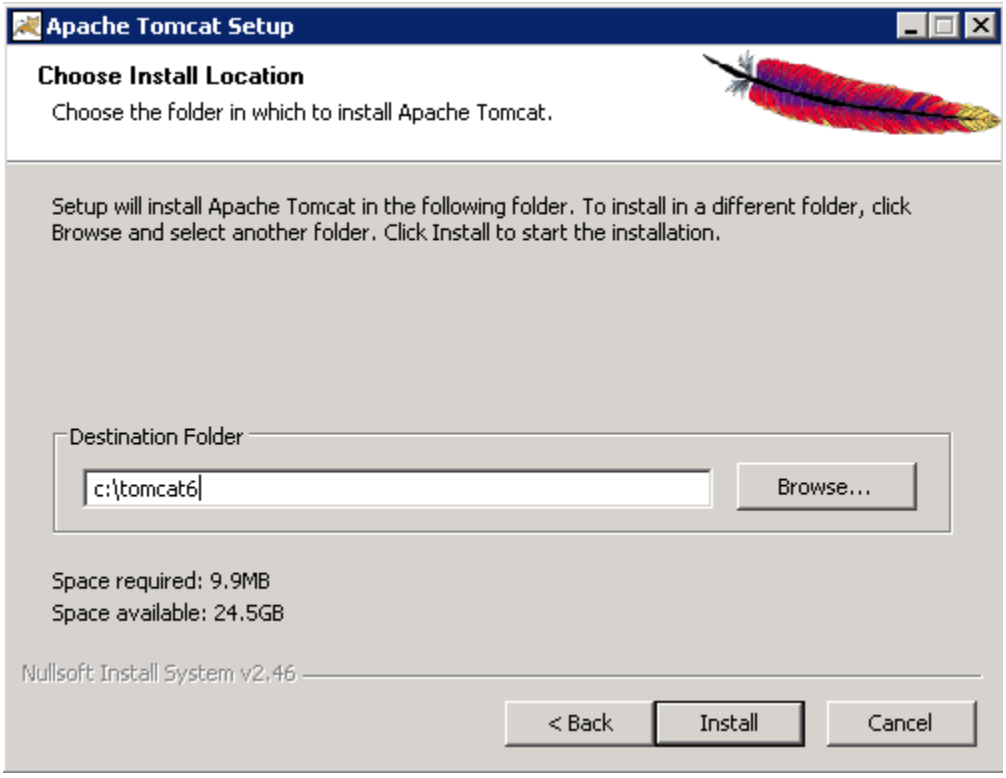
Create Tomcat administrator user should you need to later use tomcat management applications.

Tomcat Administrator: admin/Pattern123

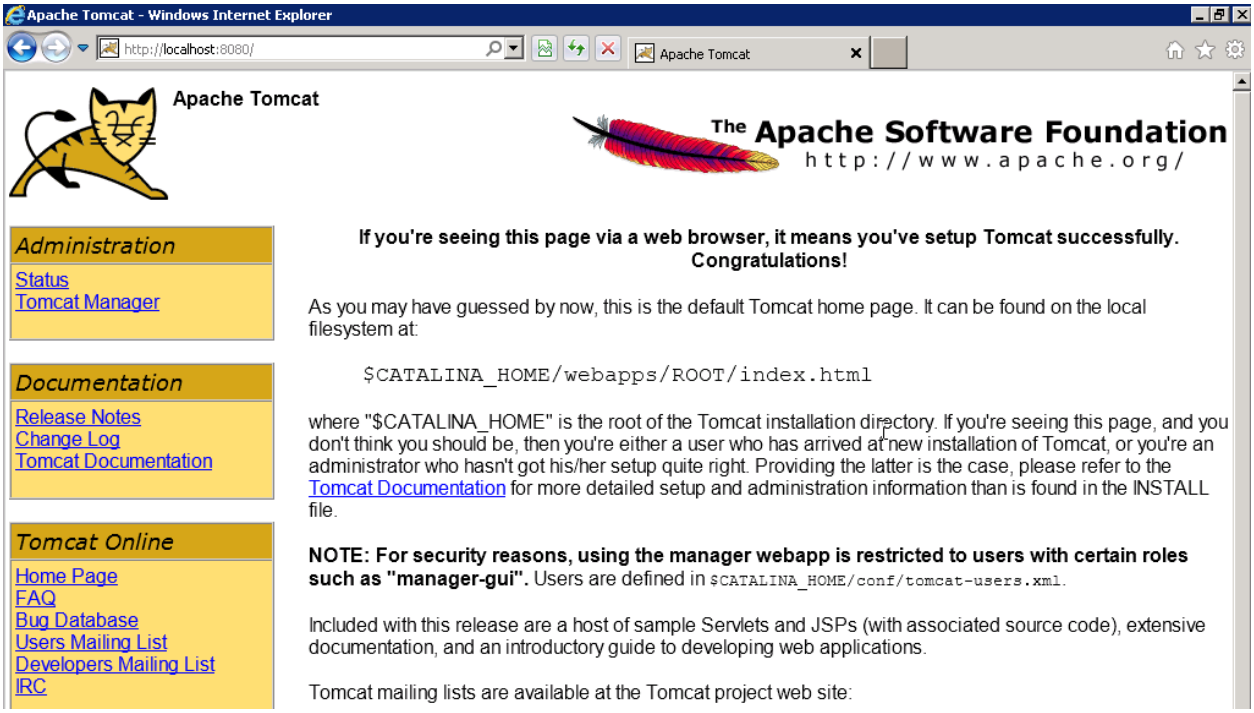
8. Provide directory of the JDK you installed.



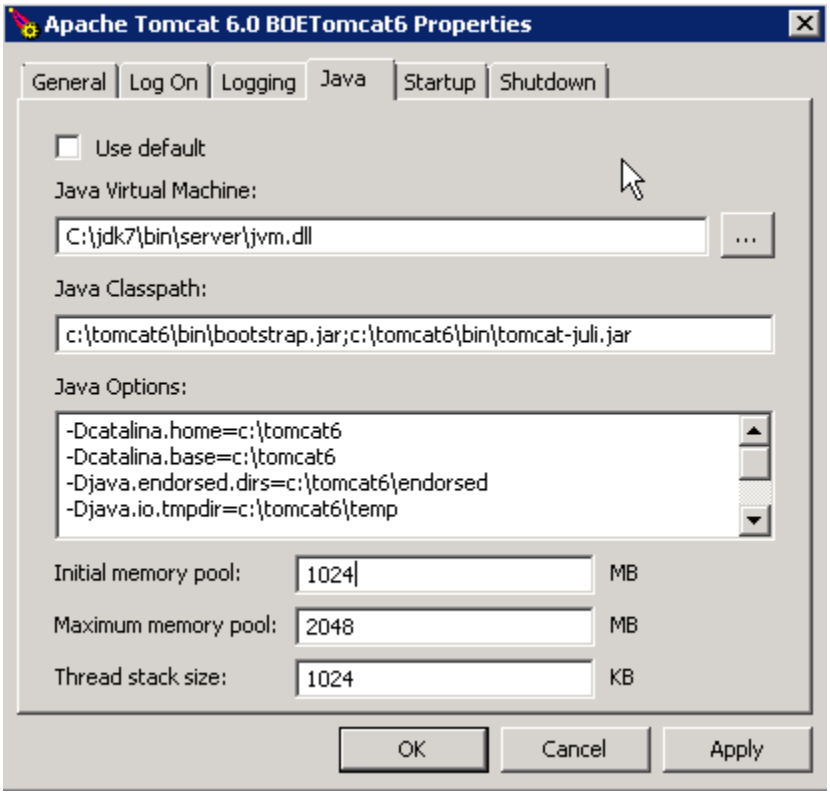
9. Install Tomcat in the c:\tomcat6 directory.



10. When installation completes successfully, let Tomcat start and verify that it installed properly by testing Tomcat home page at http:// vantgvmwinpb02:8080/



11. Launch the Tomcat Configuration program from the Start Menu.



Modify default values for Initial, Maximum memory pools and Stack size. Xms=1024, Xmx=2048 and Xss=1024 are the initial values that work in most default deployments.

Add -XX:MaxPermSize=512m under Java Options.
Further tuning of this and other Java parameters might be required later, based on performance and stability of your deployment.
Restart tomcat for settings to take effect.

Setting up Application Server 2

- To set up Application server 2, on the vantgvmwinpb03 machine, follow the steps in Setting up Application Server 1.
- To test the installation after it is complete, go to http://vantgvmwinpb03:8080.

Installing the BI platform web tier

Setting up BI platform web tier

By installing the web tier on each application server machine, the WDeploy tool is made available to build the SAP web applications on each server individually. In addition, this configuration lets you apply patches directly to each machine to ensure web applications are patched correctly.

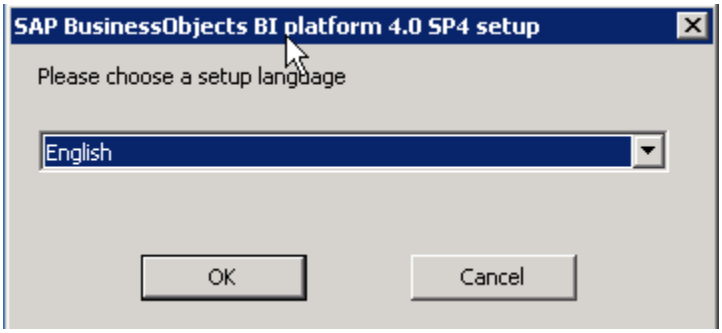
Prerequisites and additional information

- To do this task, you will need to have downloaded the BI platform 4.0 SP4 installation media to the machine. To download the installation media, go to the SAP Software Download Center. Store it in the Temp directory on the machine.
- You will need the name of your CMS and the port number it runs on.
- It is also possible to deploy the web applications without installing the web tier. For more information, see Web Application Deployment Guide for Windows (BI 4.0 SP4). That document can also be used as further reference throughout this task.

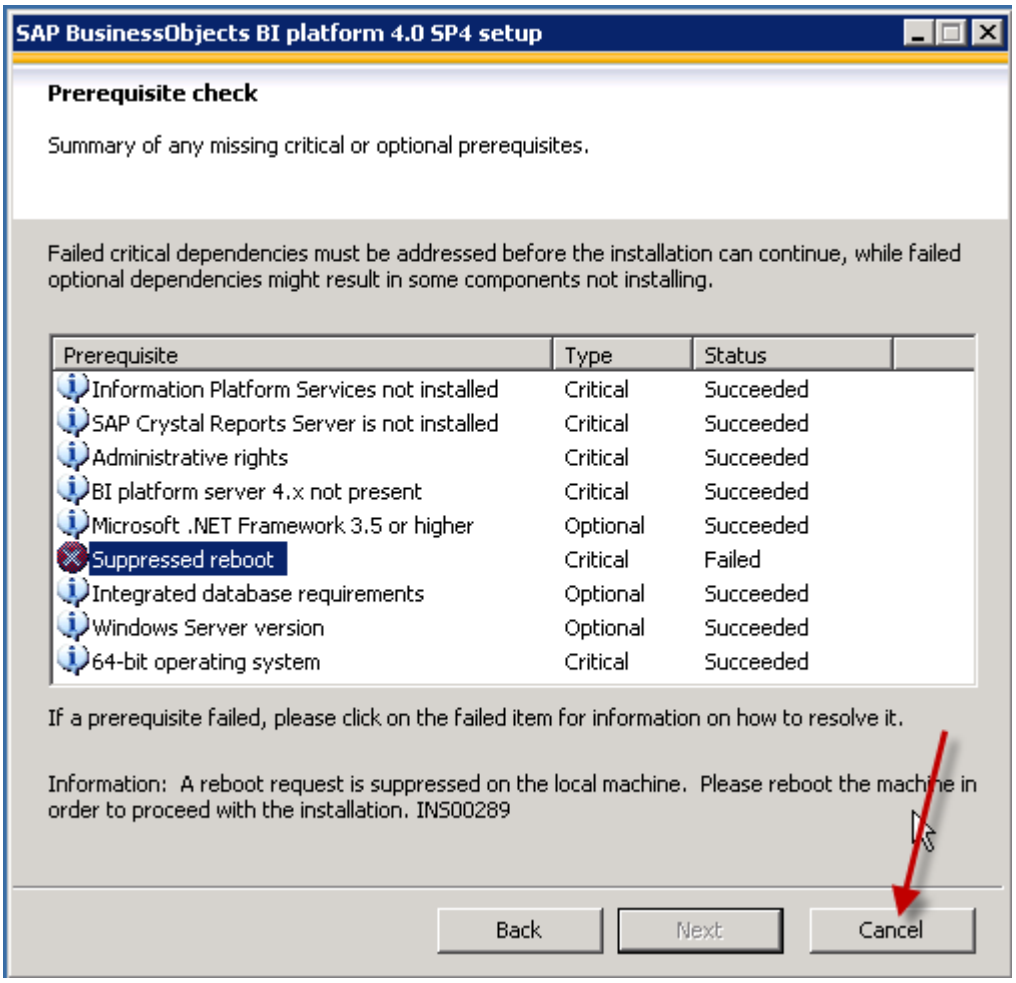
To install the BI platform web tier

1. Go to the folder where the BI platform 4.0 SP4 installation media was downloaded to, right-click the setup.exe file, and select Extract into.
   It is recommended to extract the archive into a folder that is closer to the root drive, away from the Temp folder.

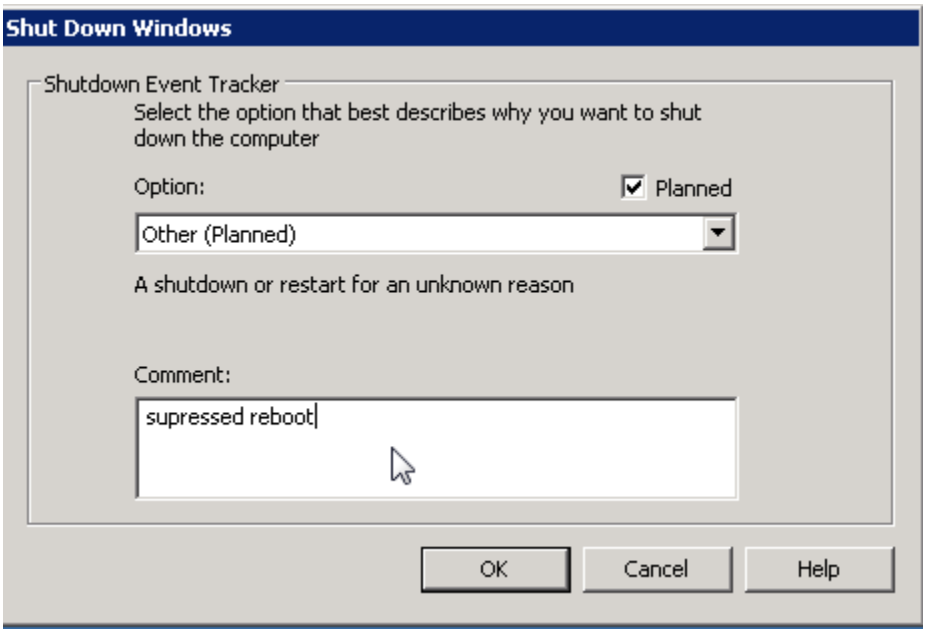
2. To start the installation program, go to the folder where the files were extracted to, and double-click **setup.exe**.
3. Select the interface language.



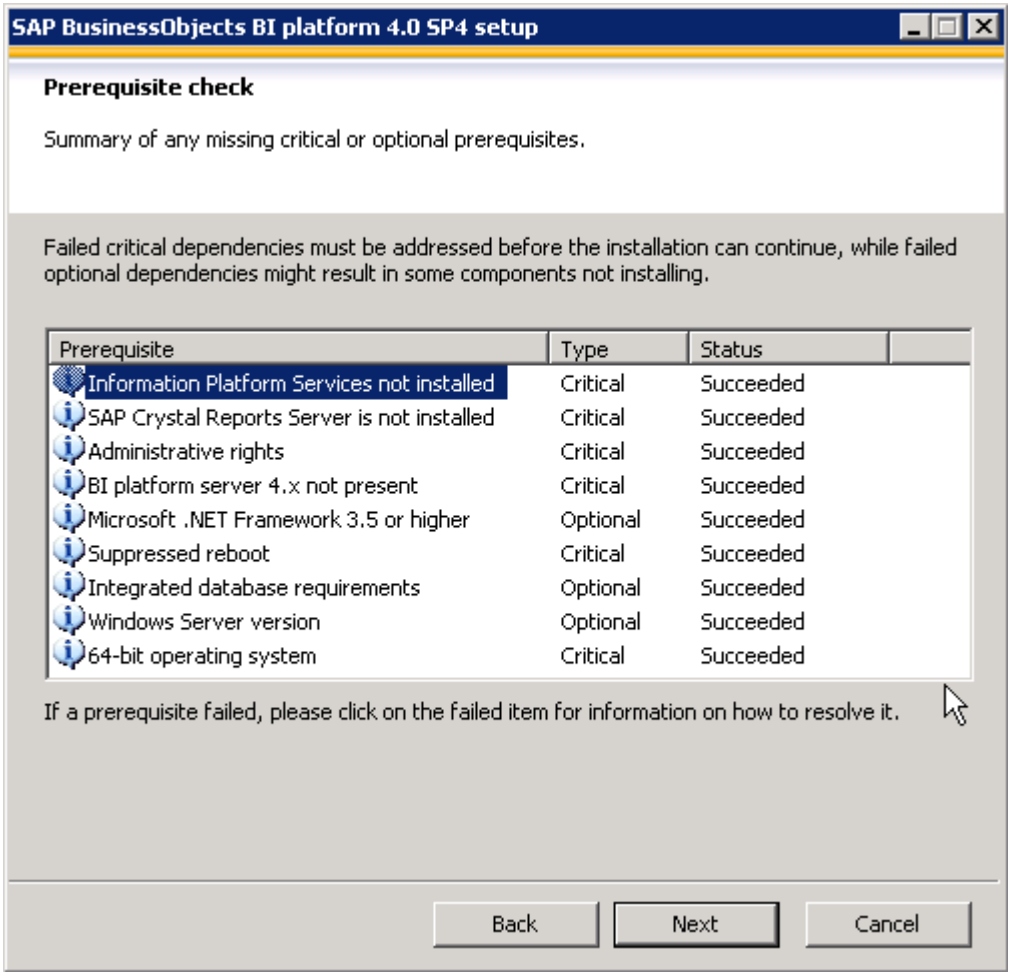
4. On the "Prerequisite check" page, due to a Suppressed reboot configuration, click **Cancel** to cancel the installation and manually reboot the machine.



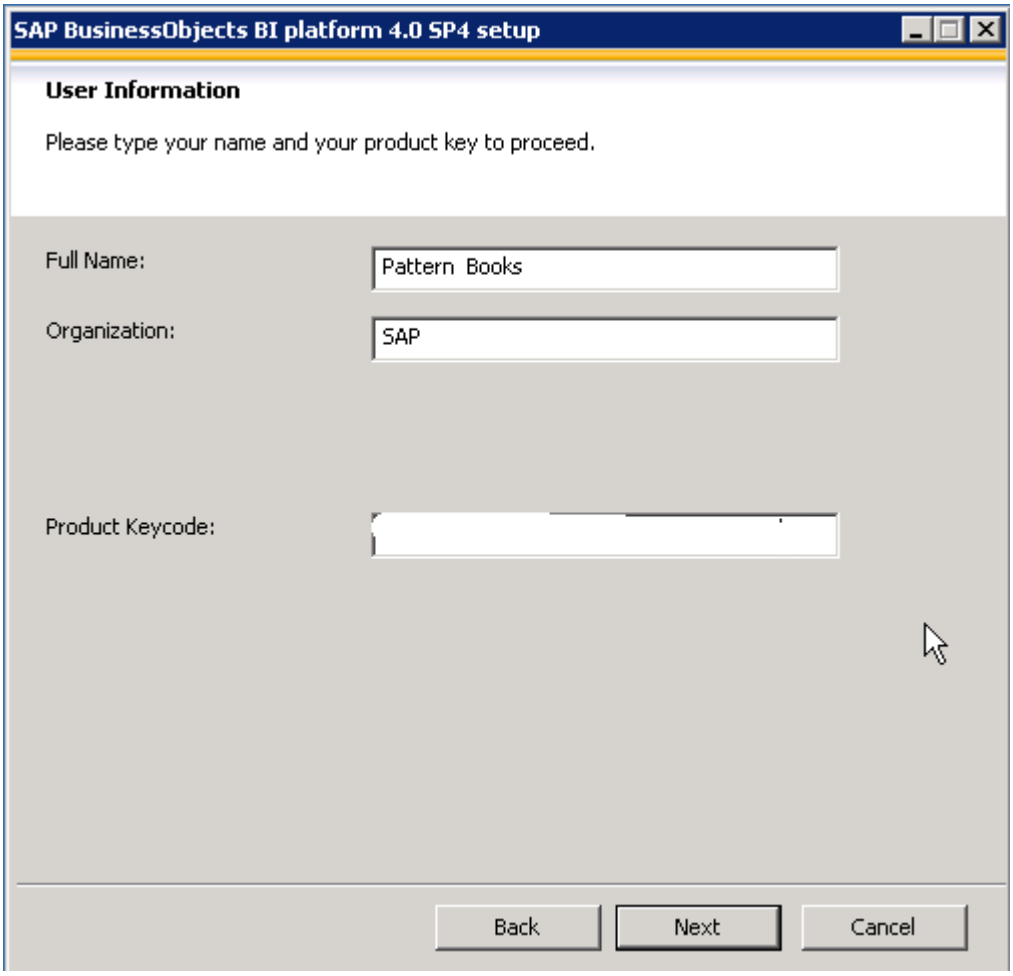
When rebooting, the standard Windows reboot dialog will appear. Enter your comments and continue.



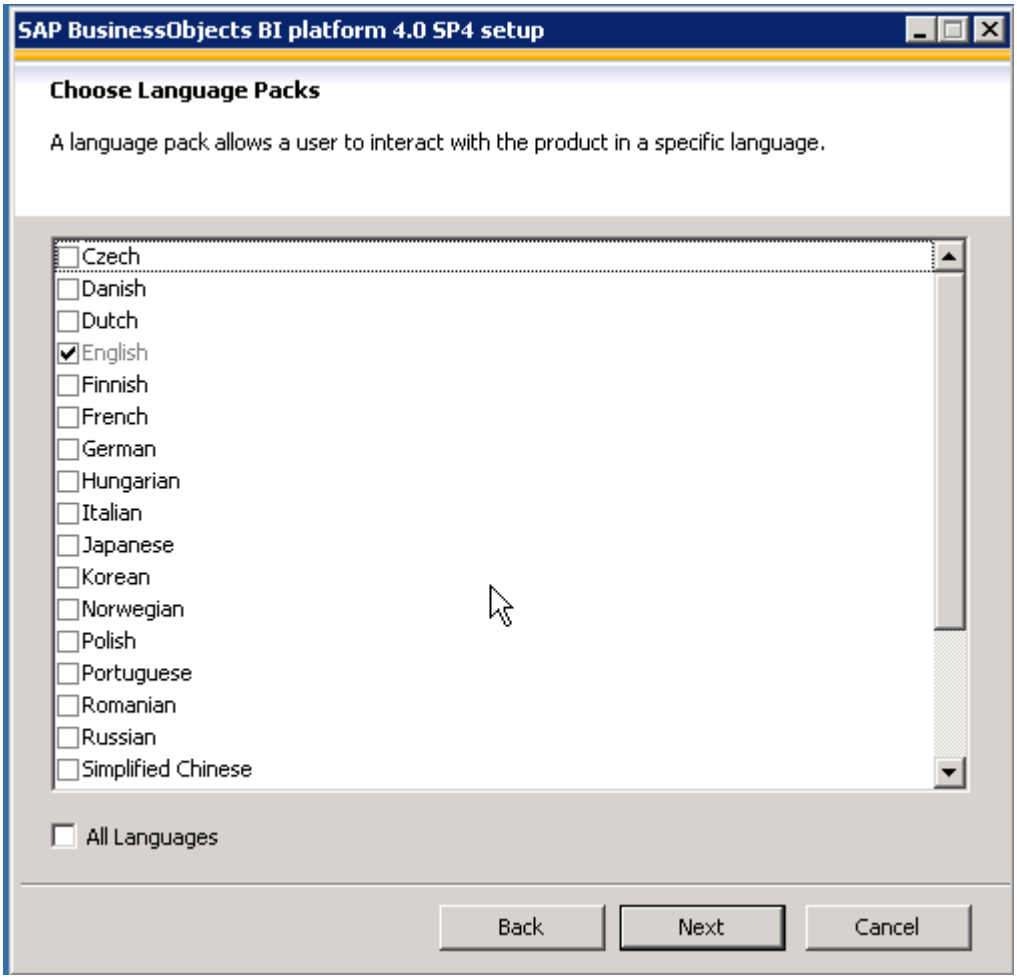
5. When the machine has finished restarting, double-click **setup.exe**.
   The "Prerequisite check" page shows all prerequisites in a “Succeeded” state.



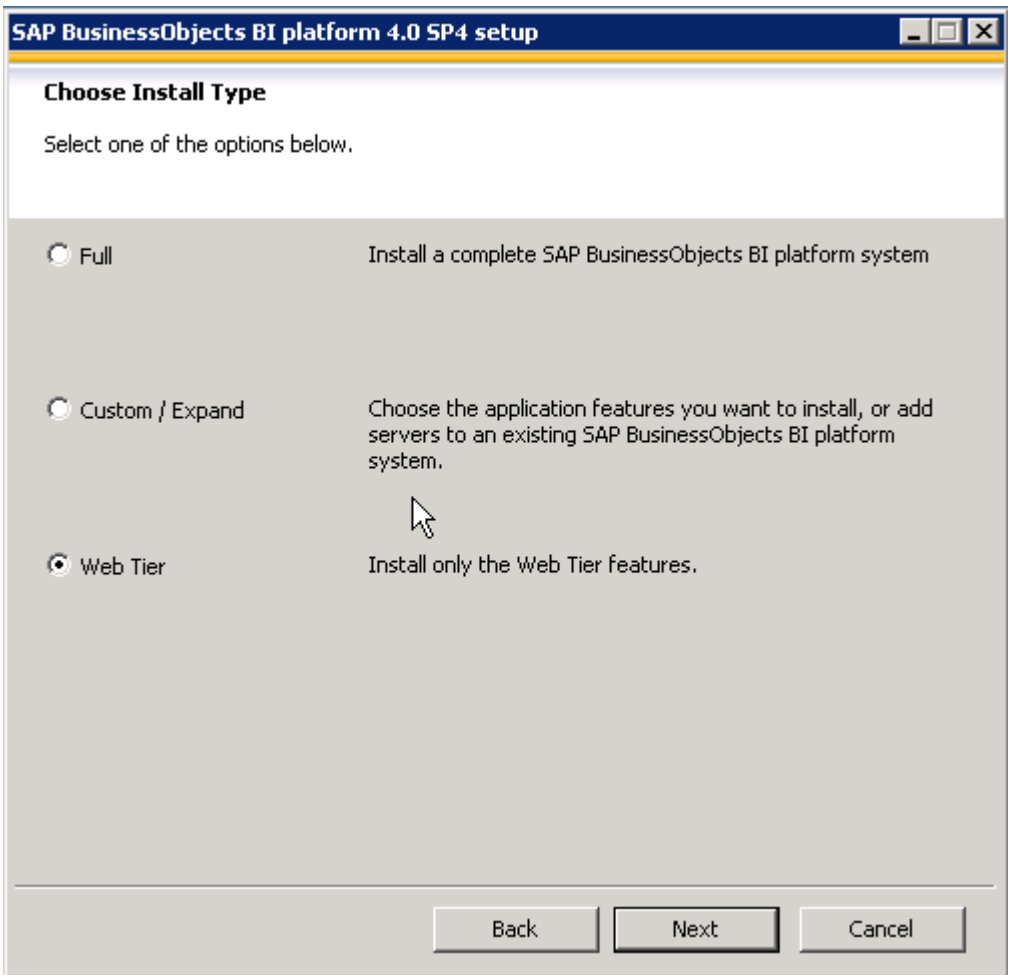
6. Accept the License agreement, and click Next.
7. Provide valid License Key, and click **Next**.



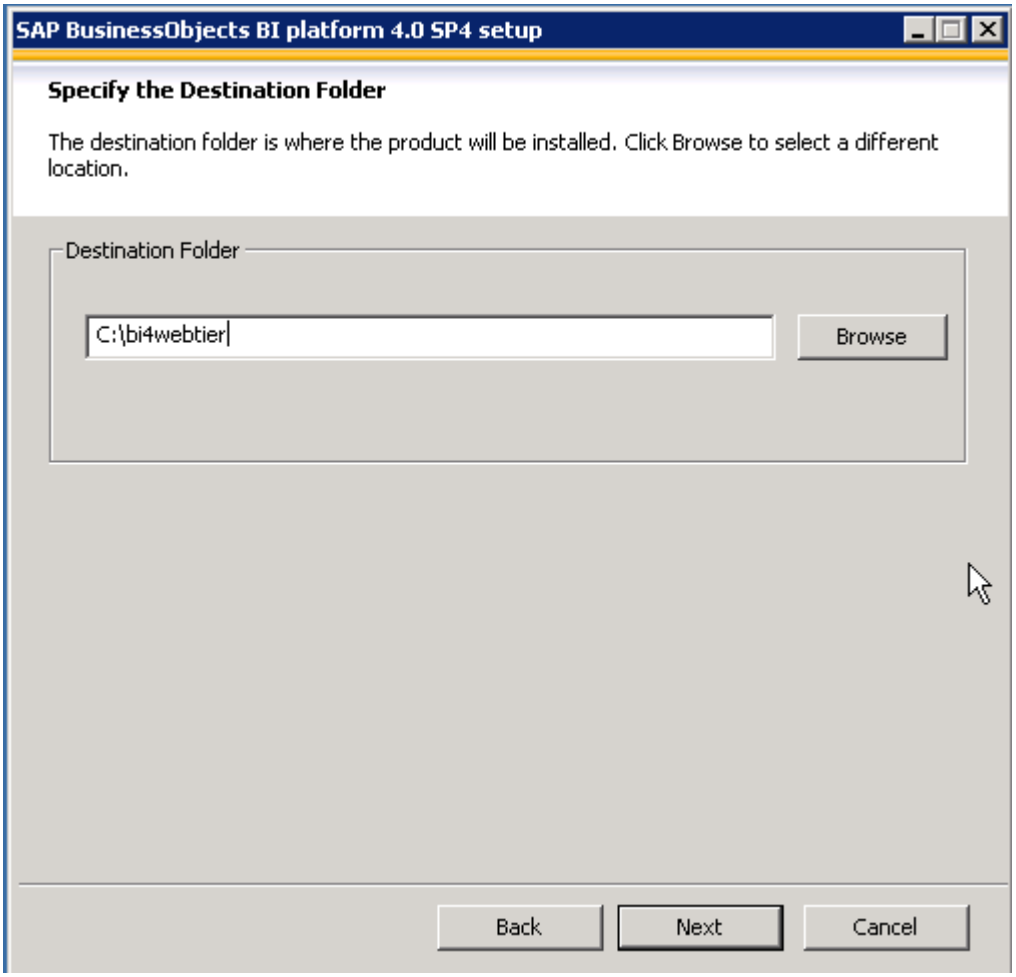
8. Select language pack you need.
   Warning: Language packs cannot be added after installation, they can only be removed.



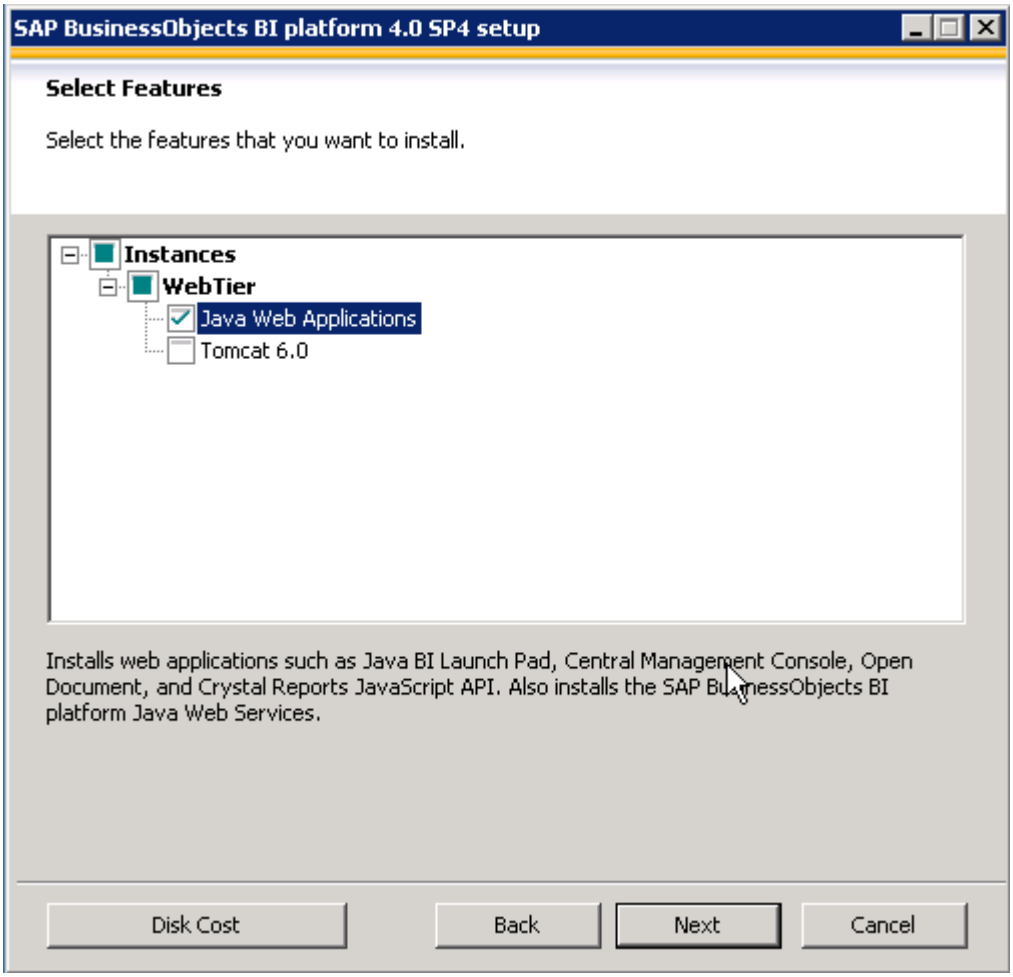
9. Click **Web Tier**, and click **Next**.



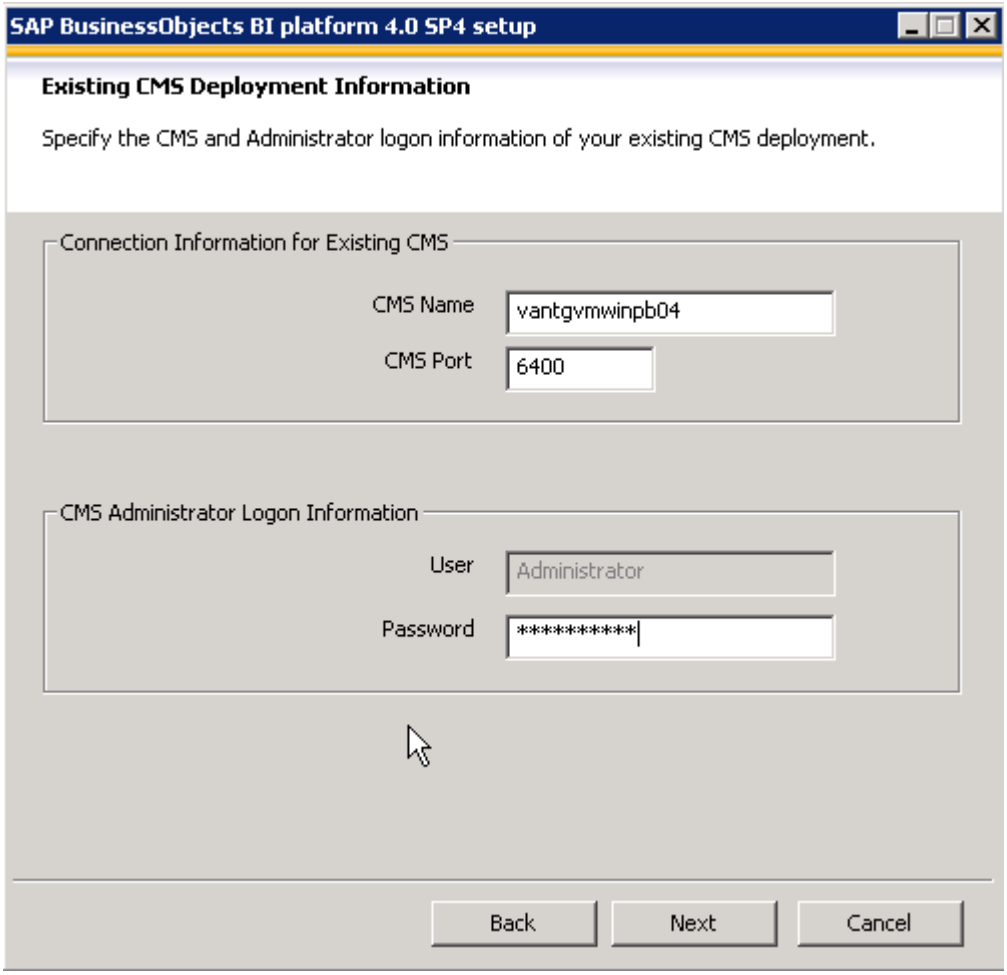
10. In the **Destination Folder** box, type c:\bi4webtier.



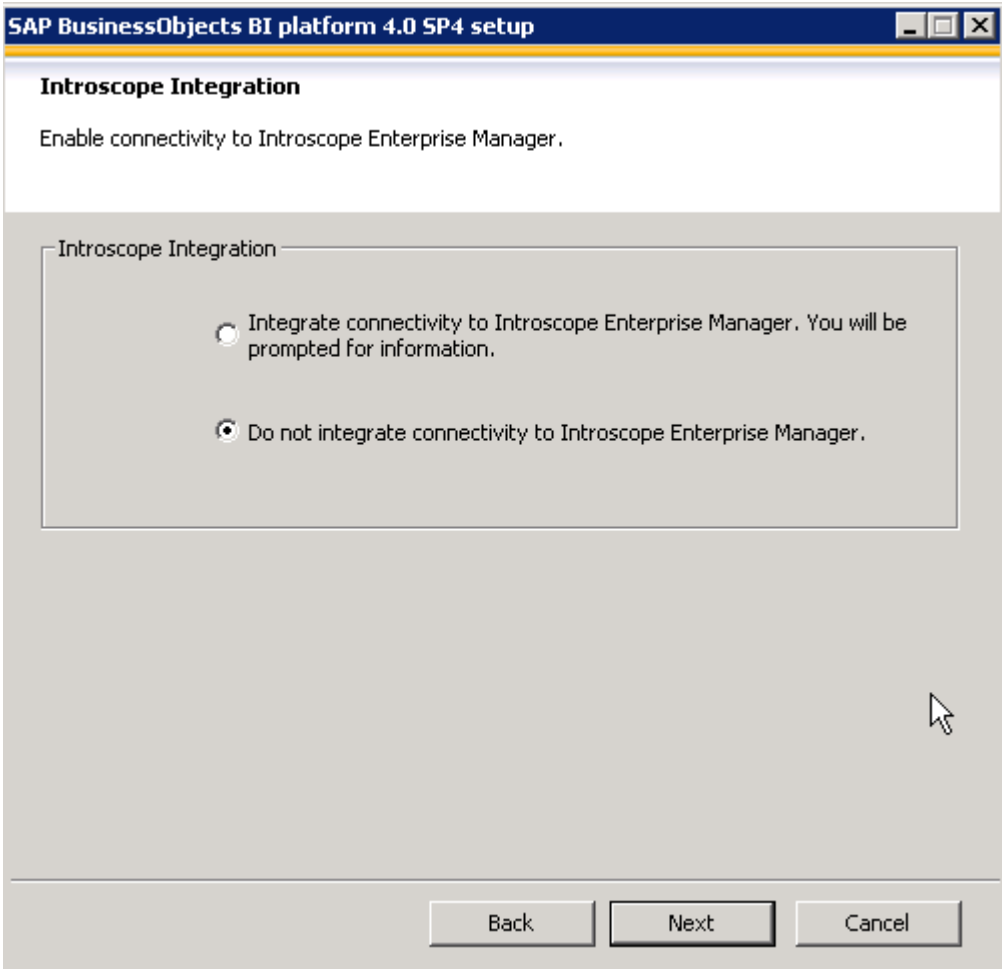
11. Clear the **Tomcat 6.0** check box (because this pattern uses an independent Tomcat installation).



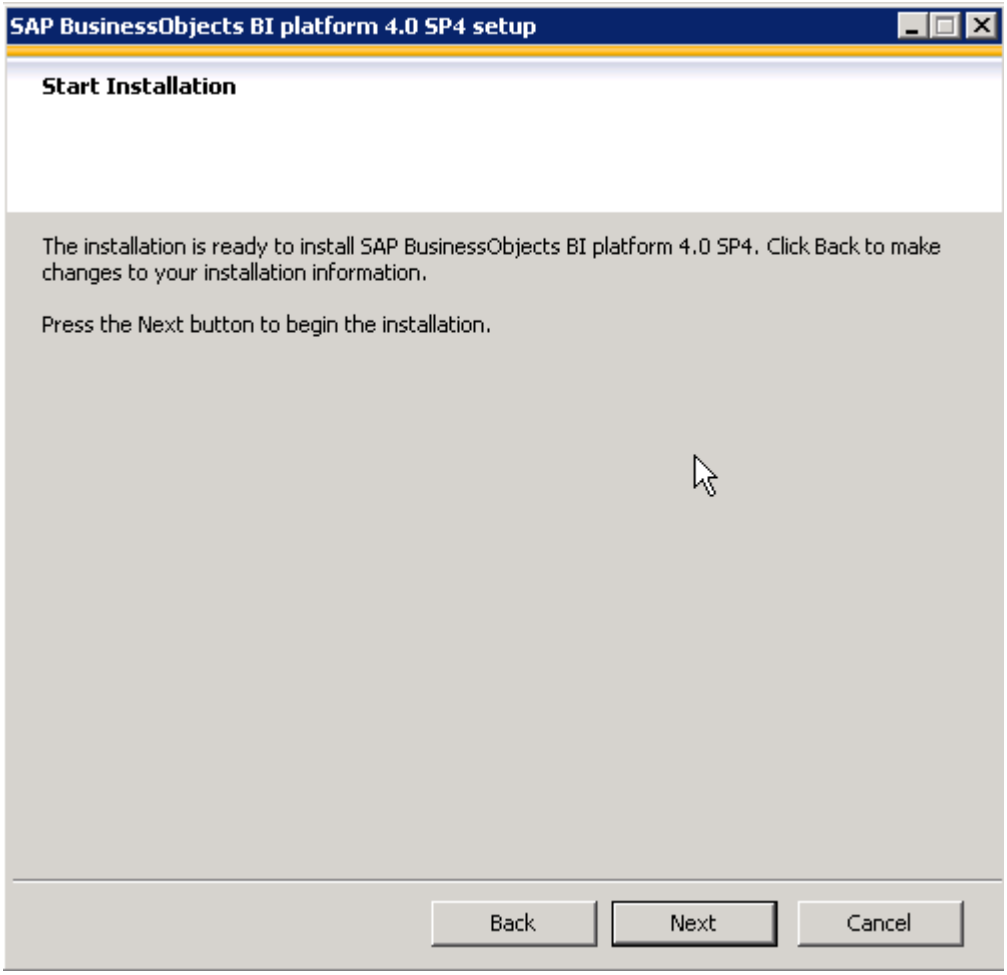
12. In the "Existing CMS Deployment Information" page, type the information required in the **CMS Name**, **CMS Port**, **User**, and **Password** boxes.



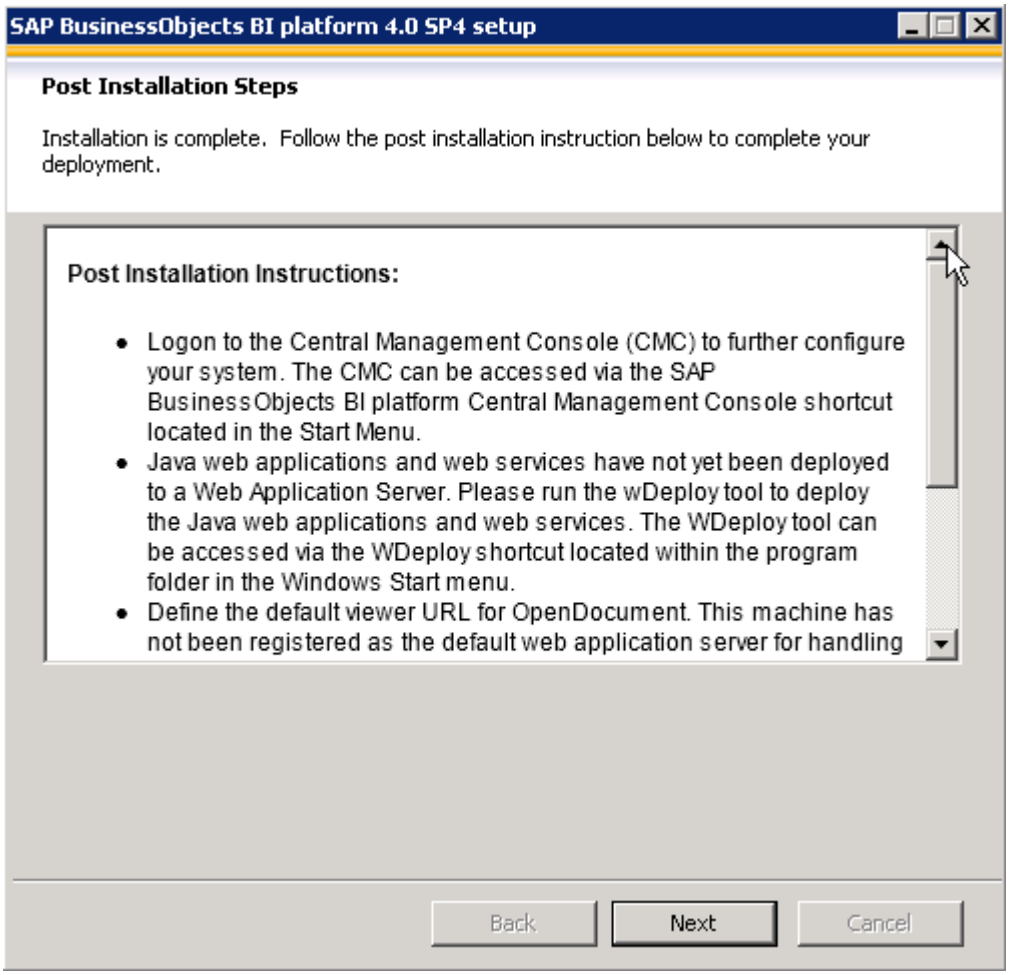
13. Because this pattern does not use Introscope management, click **Do not integrate connectivity to Introscope Enterprise Manager**, and click **Next**.



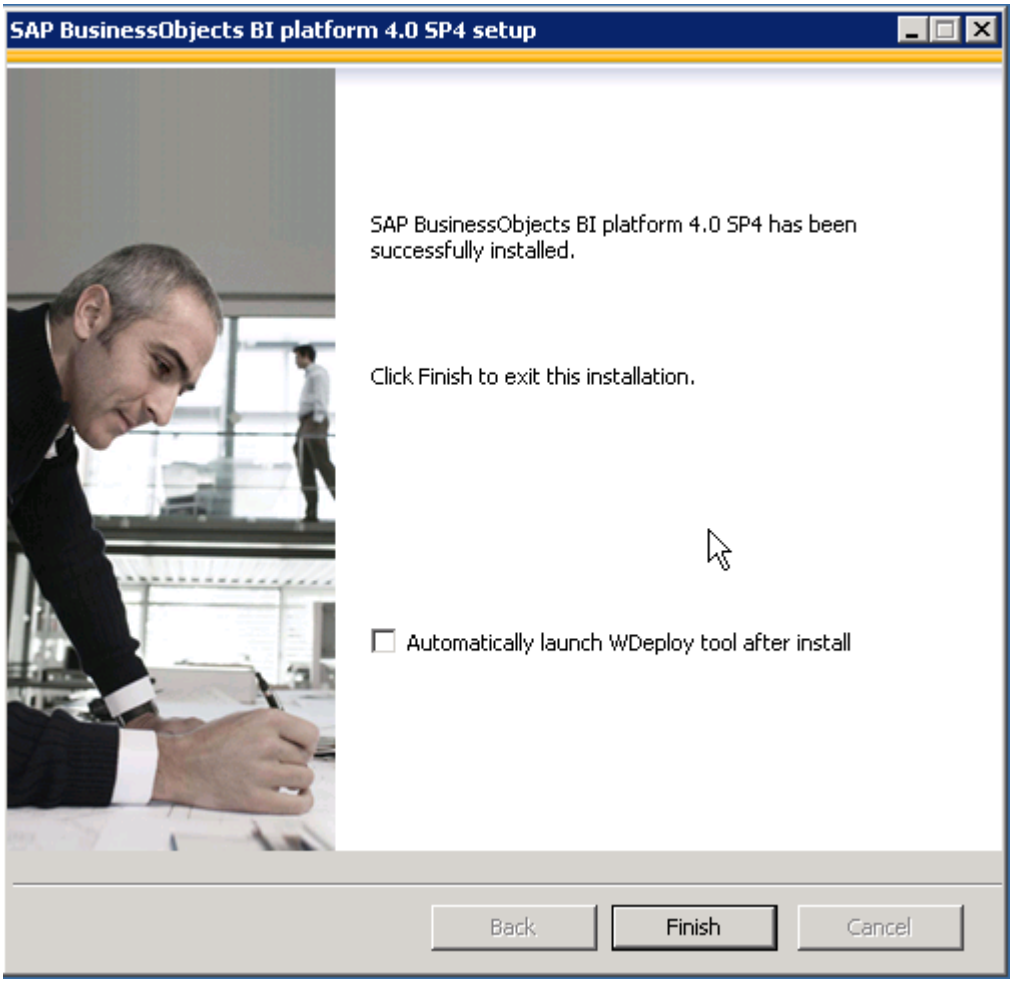
14. To start the installation, click **Next**.



15. To complete the installation, click **Next**.

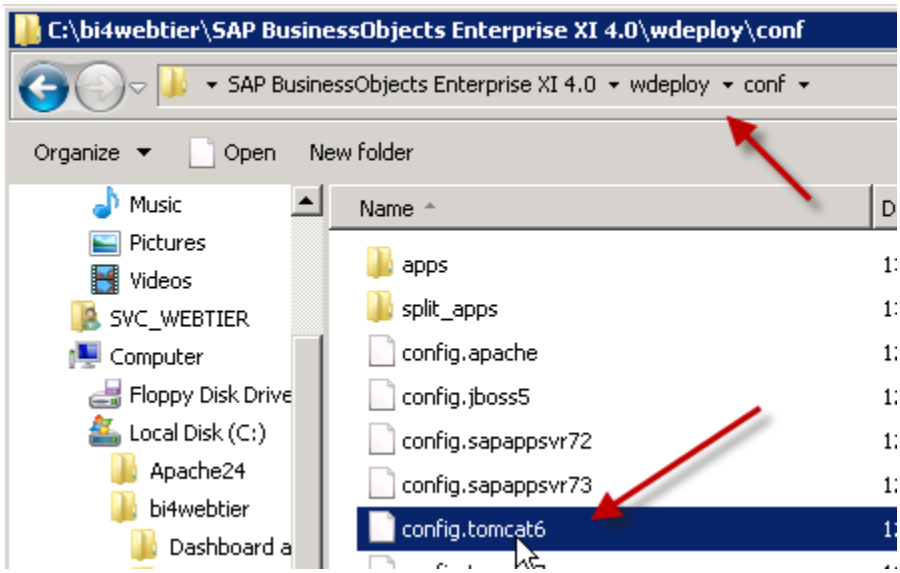


16. Ensure the **Automatically launch WDeploy tool after install** check box is clear, and click **Finish**.

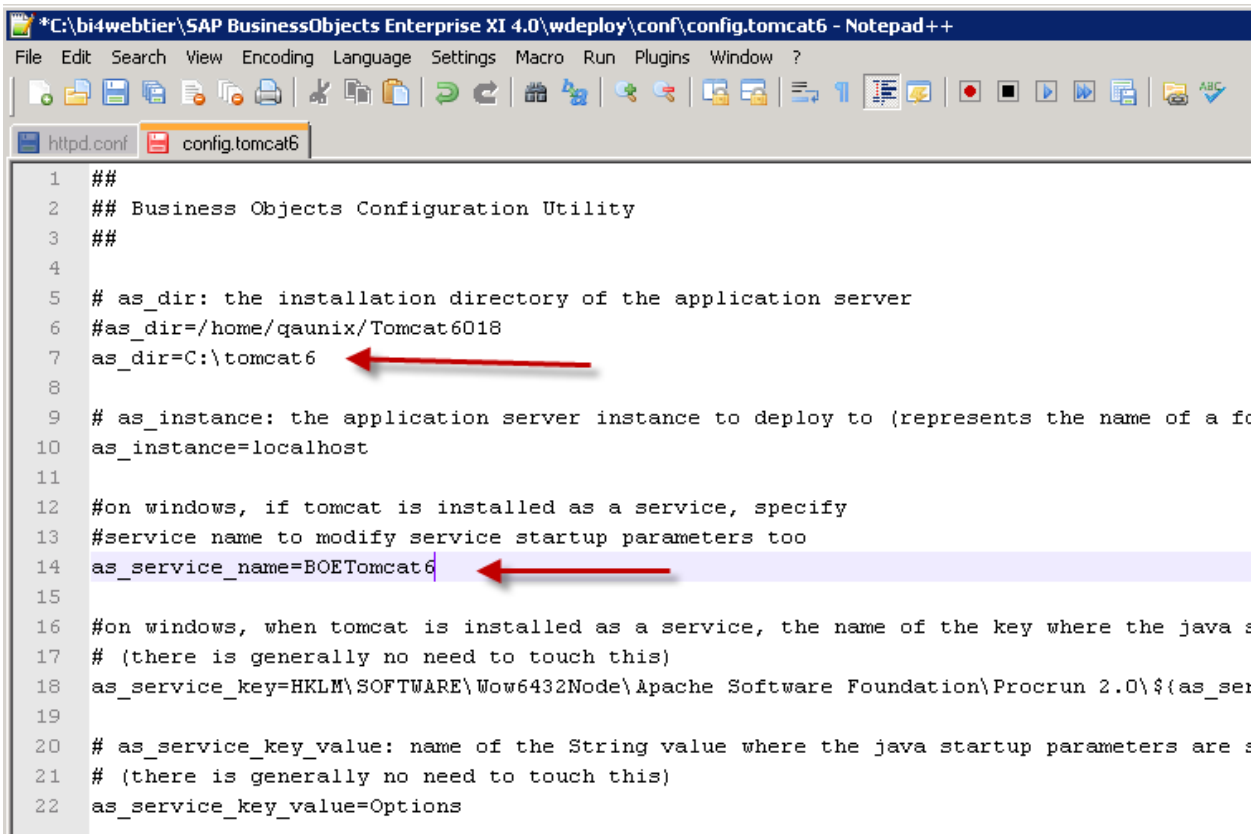


Before using WDeploy to deploy BI platform web applications to the Tomcat Application Server, you must ensure that the configuration files for the application server contain correct information, and modify them as needed (as shown here).

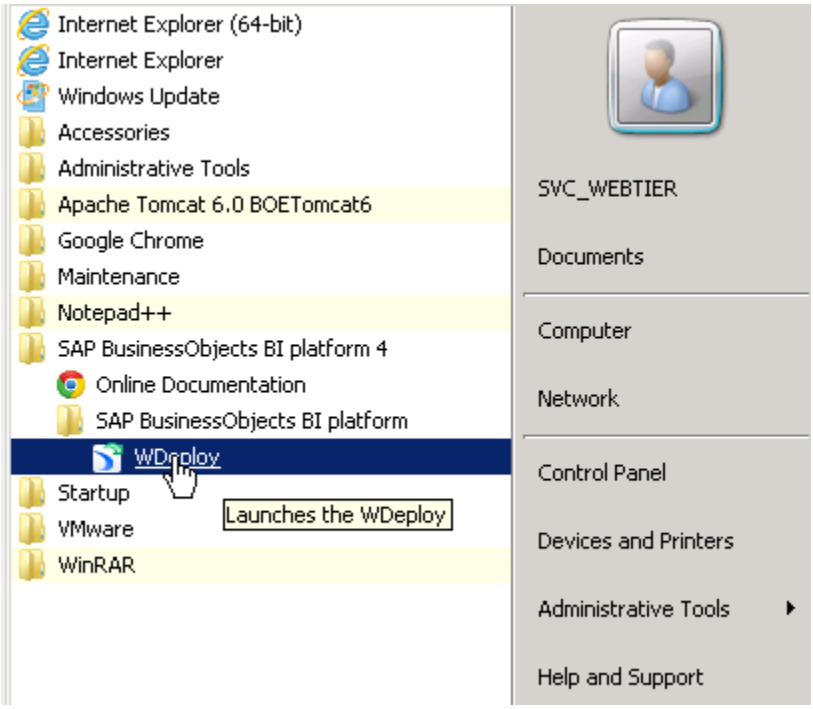
17. Go to the folder where the configuration files are stored: C:\bi4webtier\SAP BusinessObjects Enterprise XI 4.0\wdeploy\conf.

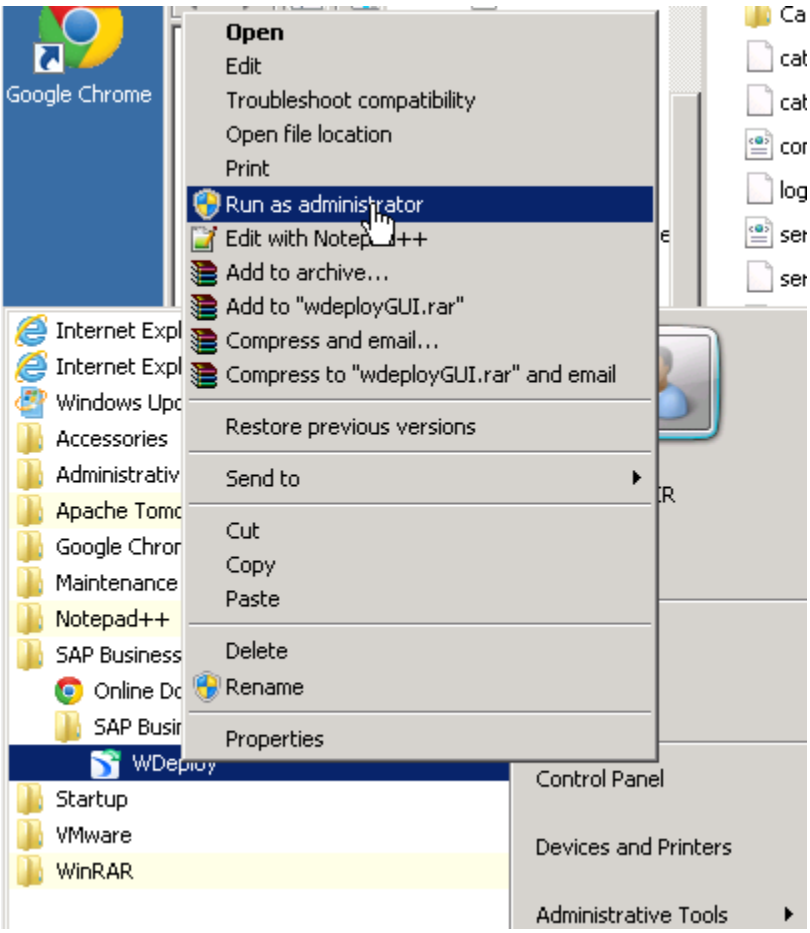


18. In a text editor, open the file config.tomcat6.
19. Verify that as_dir is set to the location of tomcat and that as_service_name is set to the correct service name for Tomcat.



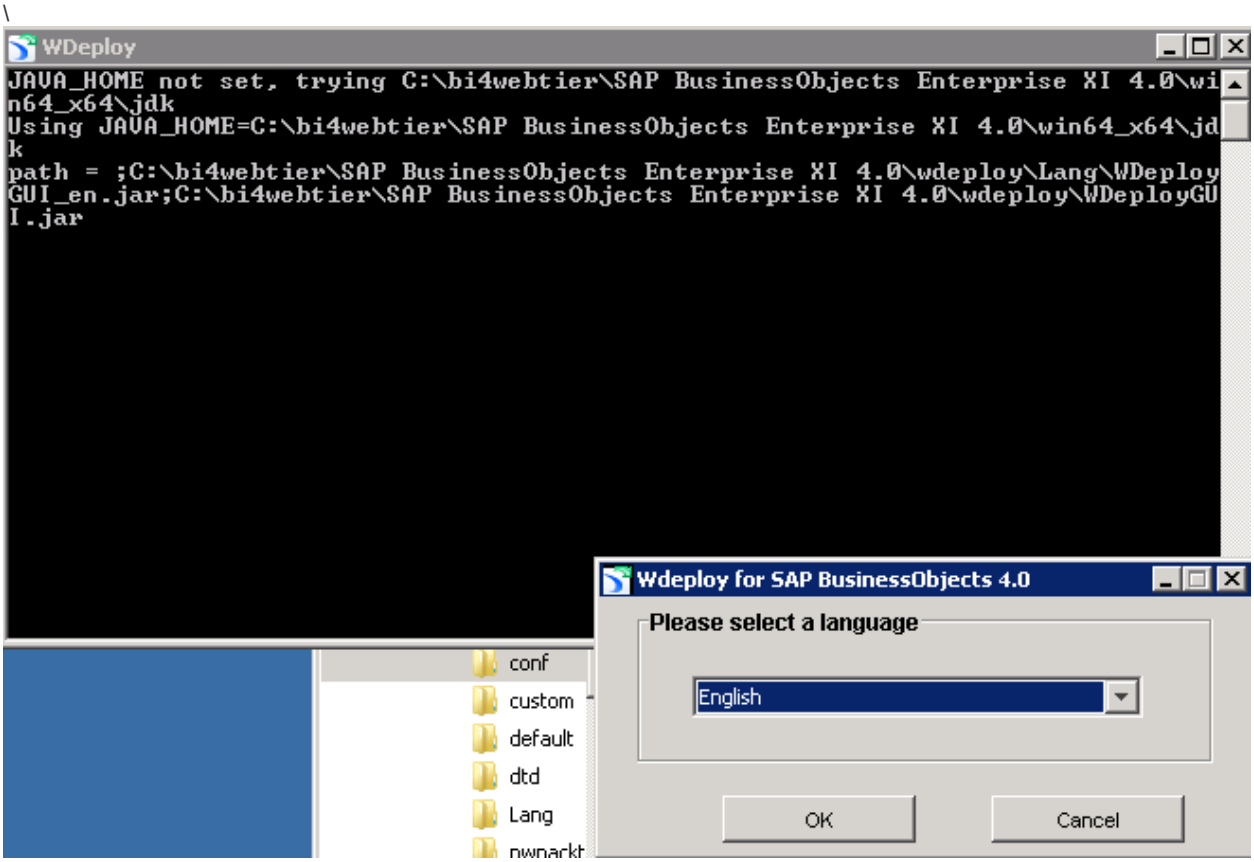
20. To start the WDeploy GUI tool, click **Start** > **All Programs** > **SAP BusinessObjects BI platform 4**, right-click **WDeploy**, and select **Run as administrator**.



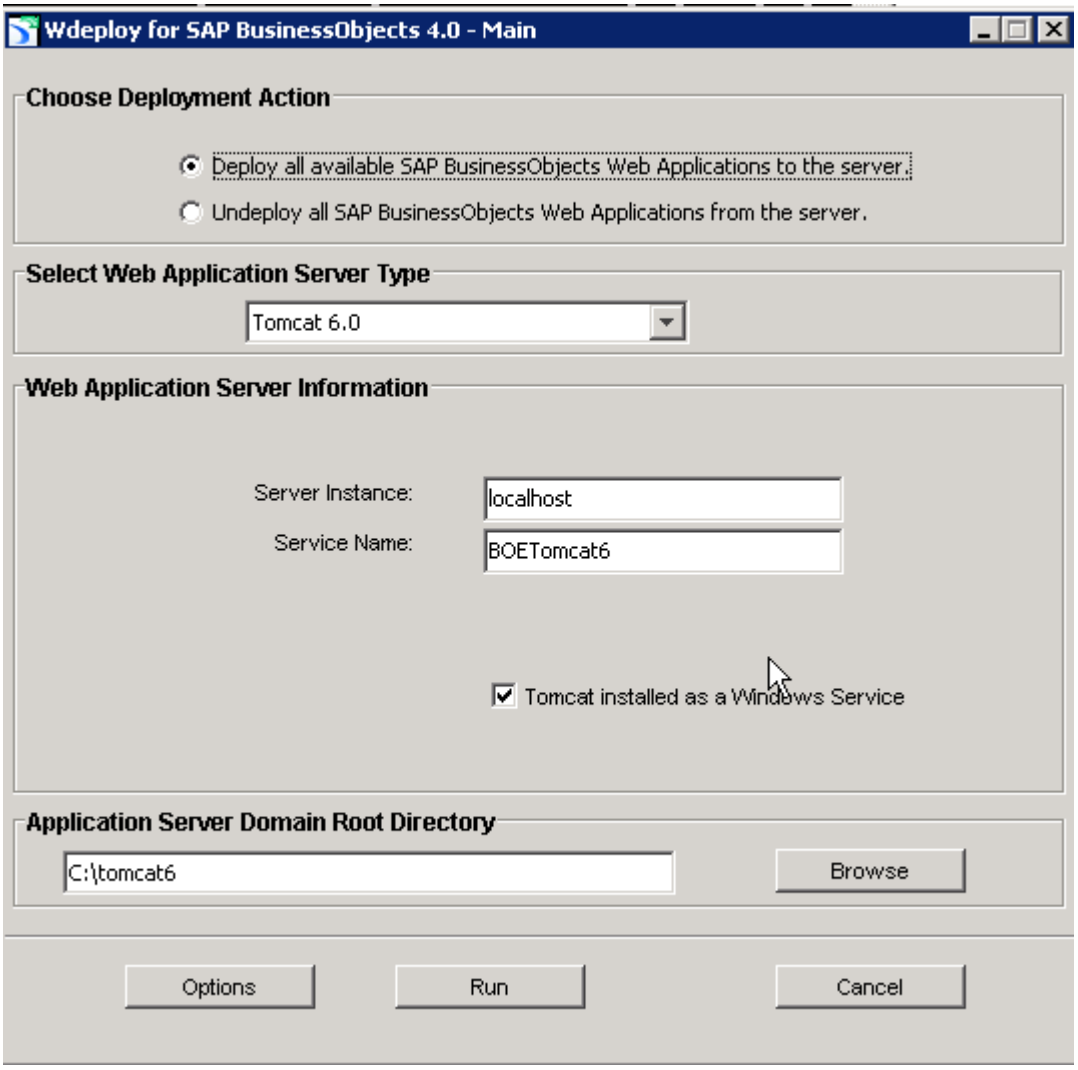


21. In the "Wdeploy for SAP BusinessObjects 4.0" dialog box, select **English**, and click **OK**.

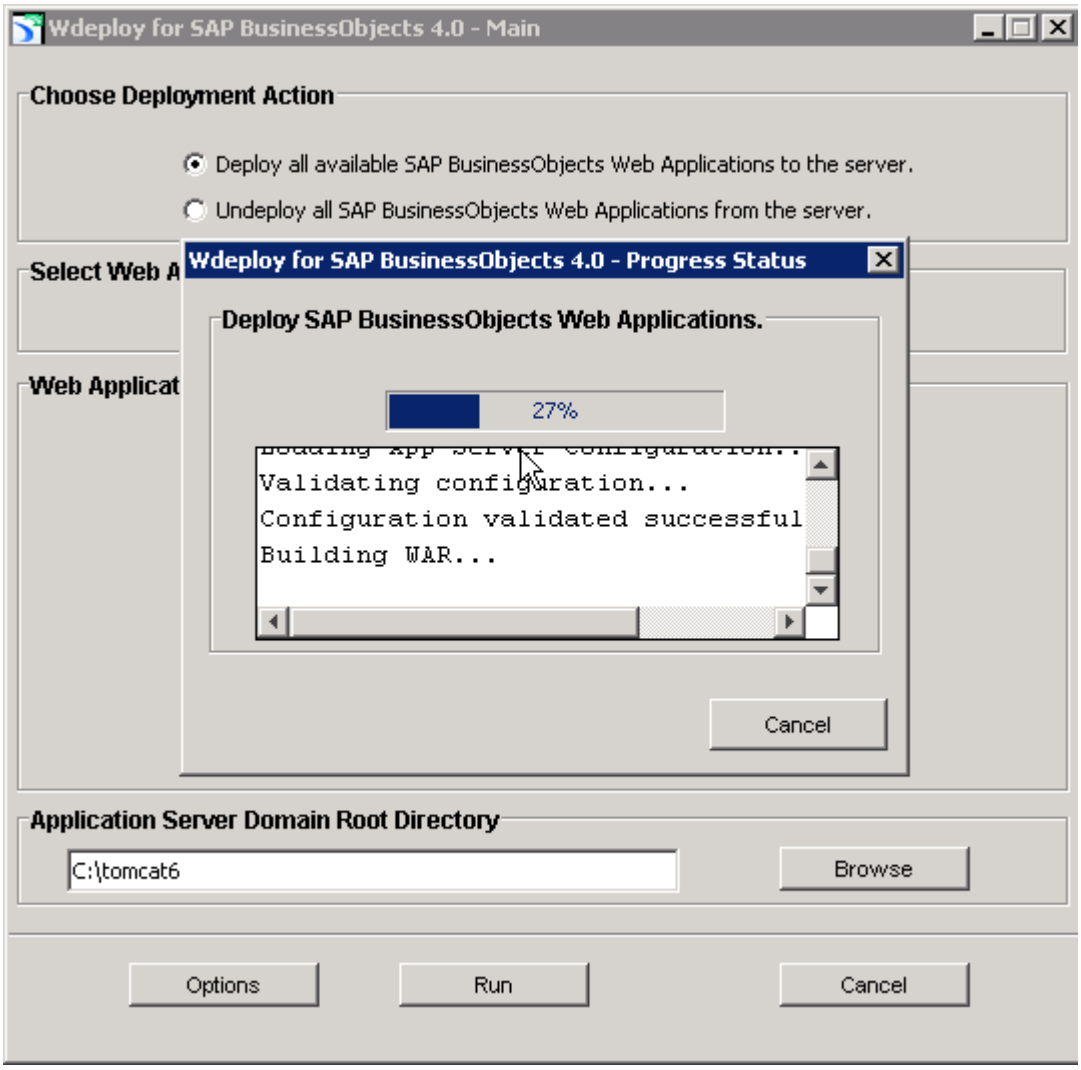
\



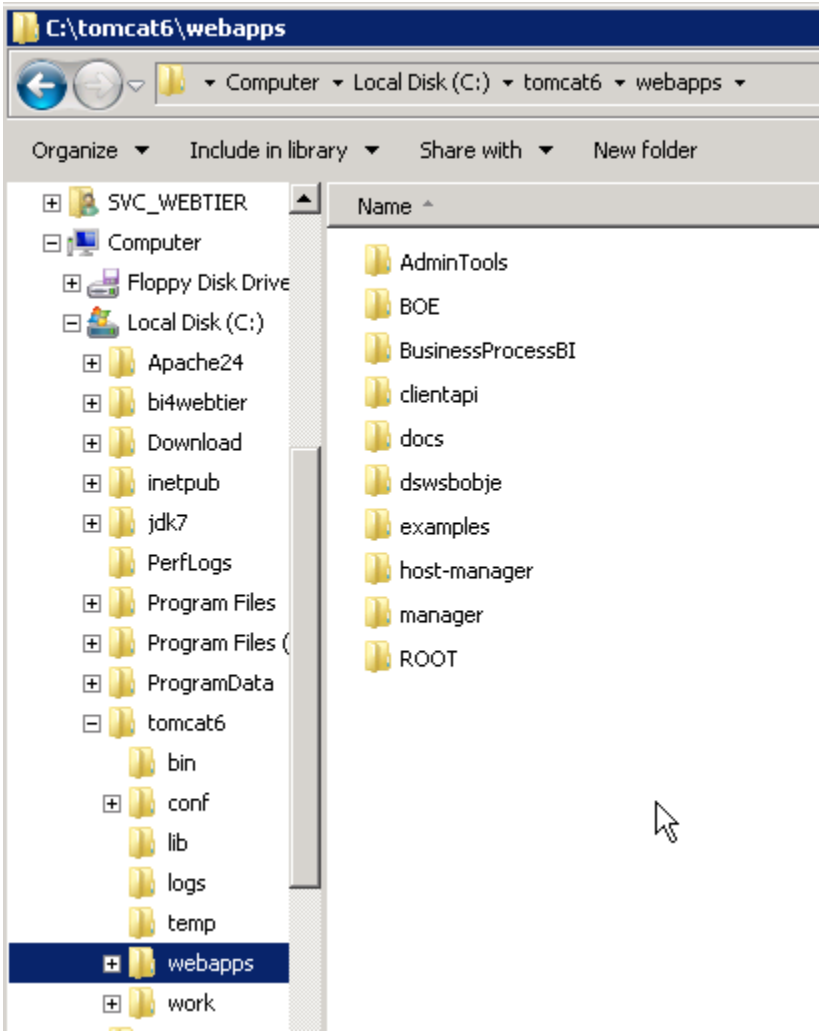
22. Click **Deploy All available SAP BusinessObjects Web Applications to the server**, and ensure the parameters are as shown here, and then click **Run**.



23. The following confirmation pop-up boxes appear:



24. After WDeploy has successfully deployed the web applications, go to the C:\tomcat6\webapps folder, and check that the list folders are as shown here:



25. To verify that the deployment is complete, go to these pages and see if you can log in to BI platform and to the CMC:
    - http://vantgvmwinpb02:8080/BOE/BI
    - http://vantgvmwinpb02:8080/BOE/CMC.
26. To complete installation of the Web tier on the second Application server machine, repeat all steps on vantgvmwinpb03

Configuring the Application Server Cluster

Clustering the Application Server

Tomcat 6 supports clustering of two or more application servers for session replication and failover. And because BI platform sessions are serialized, a user session can fail-over seamlessly to another instance of Tomcat, even when an application server fails. For example, if a user is connected to an application server that fails while the user is navigating a folder hierarchy. With

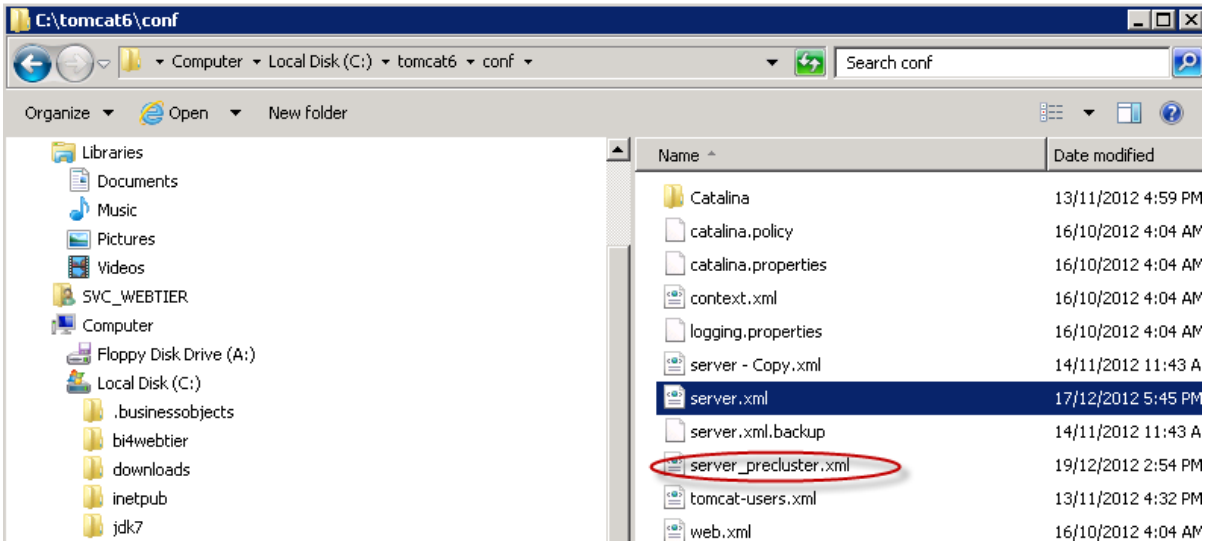
a correctly configured application server cluster, the user may continue navigating the folder hierarchy without being redirected to the login page or to the root folder.

Additional Information

For more information about configuring Tomcat 6 in a cluster, see the "How To" here http://tomcat.apache.org/tomcat-6.0-doc/cluster-howto.html.

To configure the Application Server cluster

1. Log in to machine vantgvmwinpb02 using the account SVN_WEBTIER.
2. Make a backup copy of the server.xml file located in c:\tomcat6\conf, renaming it (for example) server_precluster.xml.



3. In a text editor, open server.xml, go to the cluster section, and replace the following:
   <!--
   <Cluster className="org.apache.catalina.ha.tcp.SimpleTcpCluster"/>
   --> With the following:

```
<Cluster className="org.apache.catalina.ha.tcp.SimpleTcpCluster"
channelSendOptions="8">

<Manager className="org.apache.catalina.ha.session.DeltaManager"
expireSessionsOnShutdown="false" notifyListenersOnReplication="true"/>

<Channel className="org.apache.catalina.tribes.group.GroupChannel">

<Membership className="org.apache.catalina.tribes.membership.McastService"
address="228.0.0.4" port="45564" frequency="500" dropTime="3000"/>

<Receiver className="org.apache.catalina.tribes.transport.nio.NioReceiver"
address="auto" port="4000" autoBind="100" selectorTimeout="5000" maxThreads="6"/>

<Sender className="org.apache.catalina.tribes.transport.ReplicationTransmitter">

<Transport className="org.apache.catalina.tribes.transport.nio.PooledParallelSender"/>

</Sender>

<Interceptor
className="org.apache.catalina.tribes.group.interceptors.TcpFailureDetector"/>

<Interceptor
className="org.apache.catalina.tribes.group.interceptors.MessageDispatch15Interceptor"/

</Channel>

<Valve className="org.apache.catalina.ha.tcp.ReplicationValve" filter=""/>

<Valve className="org.apache.catalina.ha.session.JvmRouteBinderValve"/>

<ClusterListener
className="org.apache.catalina.ha.session.JvmRouteSessionIDBinderListener"/>

<ClusterListener className="org.apache.catalina.ha.session.ClusterSessionListener"/>

</Cluster>
```

```
server.xml
93    <Engine name="Catalina" defaultHost="localhost" jvmRoute="vantgvmwinpb03">
94
95      <!--For clustering, please take a look at documentation at:
96          /docs/cluster-howto.html  (simple how to)
97          /docs/config/cluster.html (reference documentation) -->
98
99      <Cluster className="org.apache.catalina.ha.tcp.SimpleTcpCluster" channelSendOptions="8">
100     <Manager className="org.apache.catalina.ha.session.DeltaManager"
101     expireSessionsOnShutdown="false" notifyListenersOnReplication="true"/>
102
103     <Channel className="org.apache.catalina.tribes.group.GroupChannel">
104
105     <Membership className="org.apache.catalina.tribes.membership.McastService"
106     address="228.0.0.4" port="45564" frequency="500" dropTime="3000"/>
107
108     <Receiver className="org.apache.catalina.tribes.transport.nio.NioReceiver"
109     address="auto" port="4000" autoBind="100" selectorTimeout="5000" maxThreads="6"/>
110
111     <Sender className="org.apache.catalina.tribes.transport.ReplicationTransmitter">
112     <Transport className="org.apache.catalina.tribes.transport.nio.PooledParallelSender"/>
113     </Sender>
114
115     <Interceptor className="org.apache.catalina.tribes.group.interceptors.TcpFailureDetector"/>
116     <Interceptor className="org.apache.catalina.tribes.group.interceptors.MessageDispatch15Interceptor"/>
117     </Channel>
118
119     <Valve className="org.apache.catalina.ha.tcp.ReplicationValve" filter=""/>
120     <Valve className="org.apache.catalina.ha.session.JvmRouteBinderValve"/>
121     <ClusterListener className="org.apache.catalina.ha.session.JvmRouteSessionIDBinderListener"/>
122     <ClusterListener className="org.apache.catalina.ha.session.ClusterSessionListener"/>
123     </Cluster>
124
```

The code for <cluster> represents the default cluster configuration, which functions properly for this pattern. Cluster membership is defined by the Multicast address 228.0.0.4. That value changes between independent clusters if you have several running on the same network. Session replication takes place over TCP/IP and uses port 4000 for communication.

4. Save and close the file.
5. Repeat Steps 1 - 4 on the machine named vantgvmwinpb03.
6. When you have completed setting up clustering on vantgvmwinpb03, restart Tomcat. The output from catalina.out will have an additional component when the second cluster member starts. At that point, the member will join the cluster. This is indicated in Tomcat as follows:

```
Mar 2, 2012 11:11:39 AM org.apache.catalina.ha.tcp.SimpleTcpCluster startInternalINFO:
Cluster is about to start
INFO: Setting cluster mcast soTimeout to 500
INFO: Sleeping for 1000 milliseconds to establish cluster membership, start level:4
>> Mar 2, 2012 11:11:40 AM org.apache.catalina.ha.tcp.SimpleTcpCluster memberAdded
INFO: Sleeping for 1000 milliseconds to establish cluster membership, start level:8
```

The Tomcat cluster is now functional.

Setting up Apache 2.4

This section shows how to set up the Apache 2.4 web server and reverse proxy for this pattern.

- Installing Apache 2.4 as a service
- Securing the Apache web server
- Configuring the reverse proxy
- Enabling the proxy cache

Installing Apache 2.4 as a service

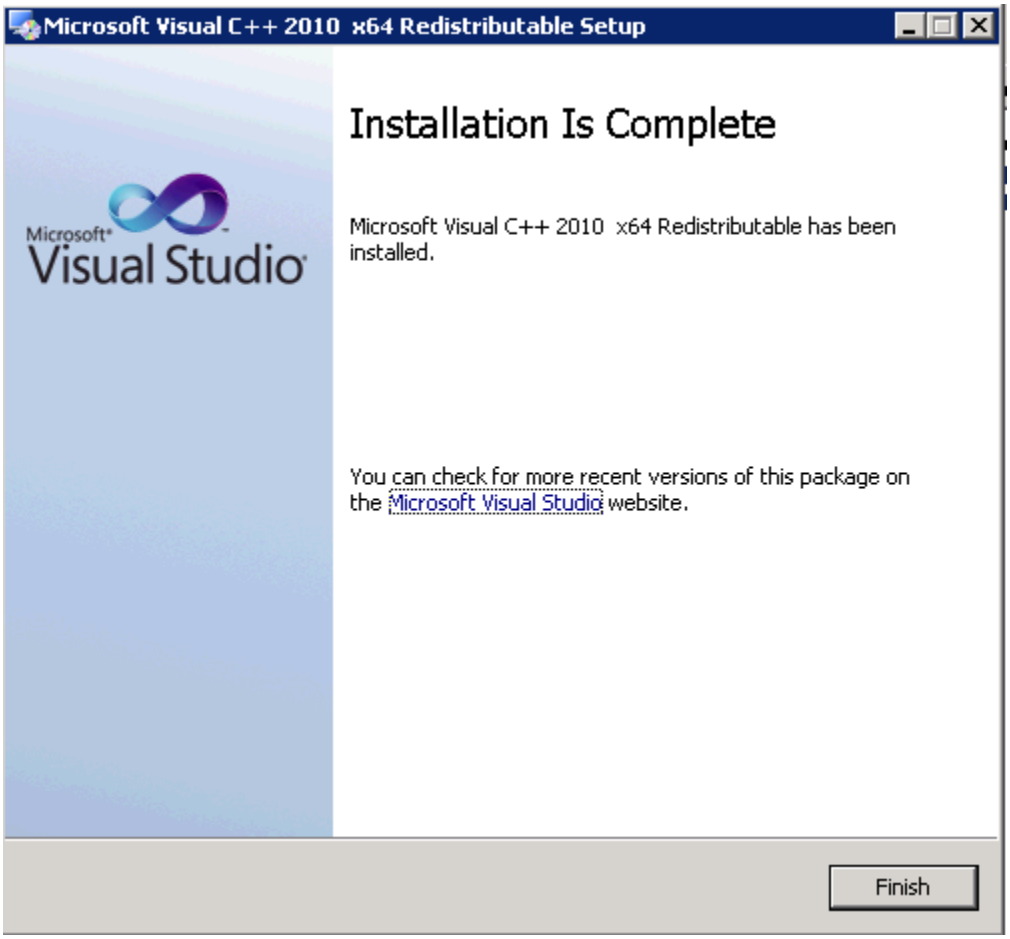
1. Log into **winpb01** as user **BI4PATTERN\Pattern01**

   Warning: **Account Permissions**

   Pattern01 is a local administrator account that is used to install and configure Apache. Apache will run as a service account named SVC_WEBTIER, which will have reduced permissions on the operating system (OS). Using this service account ensures that the Apache ID cannot be compromised and used for unauthorized access to the OS.

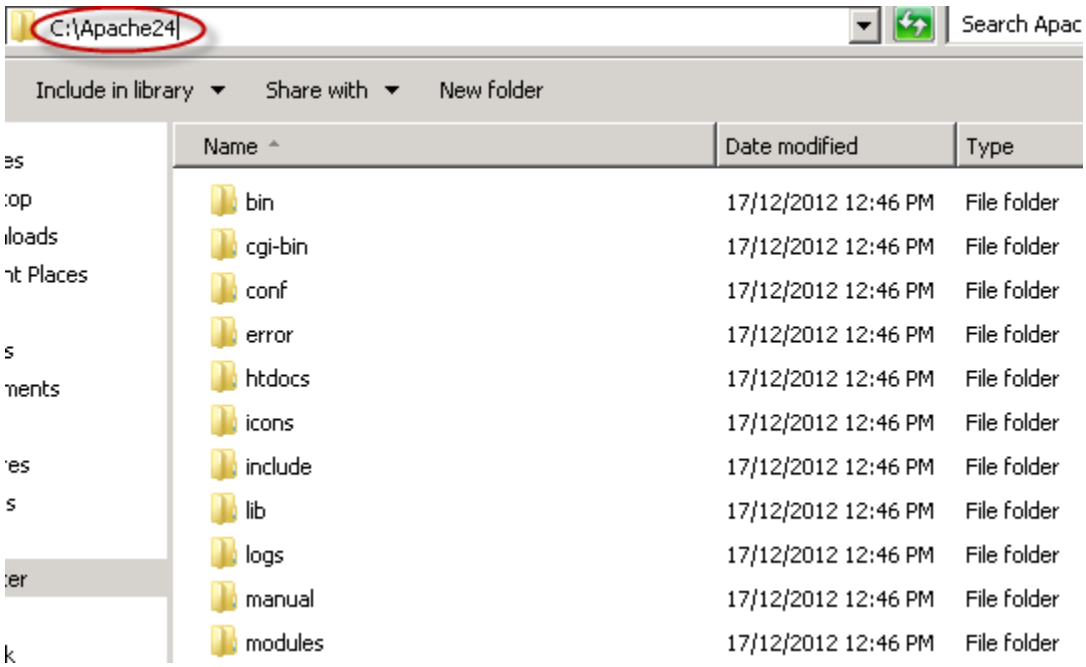
   For more information, see the Security Tips page and Apache HTTPD on Windows page on the Apache website.

2. Before you install Apache, download and install Microsoft Visual C++ 2010 SP1 Redistributable Package (x64): Microsoft Visual C++ 2010 SP1 Redistributable Package (x64)http://www.microsoft.com/download/en/details.aspx?id=13523.
   This package provides OS-specific functions that Apache 2.4 needs to run on Windows.



3. Go to the Apache Lounge website and download the latest, compiled 64-bit copy of Apache 2.4:http://www.apachelounge.com/download/win64/.
   At this time of writing, Apache 2.4.3 is the latest available release. Because the Apache project no longer provides compiled versions of Windows binaries, we use the compiled versions offered at Apache Lounge to avoid potential problems with manually compiling Apache on Windows.

4. Extract the Apache24 directory from the httpd-2.4.3-win64.zip file, and place it on the root of C: Default Windows Directories
   a. The root directory for Apache will be C:/Apache24. You can place the Apache root directory anywhere on the drive, but placing it at the root of the drive is necessary for these reasons:
   b. - It enables the pre-configured httpd.conf file to be used as a foundation.
   c. - It eliminates spaces in the directory name, which can cause problems.
   d. - It eliminates special characters in the directory name, such as the parentheses in (x86). Parentheses cause problems with the SSL configuration because Apache assumes they represent a cipher strength (for example, 512000).



5. To configure basic permissions on the web server, in a text editor open the file C:/Apache24/conf/httpd.conf, and do the following:
   - Uncomment the property **ServerName**, and set it to the Fully Qualified Domain Name (FQDN) and listening port of the server.
     In this pattern, ServerName is set to **vantgvmwinpb01.dhcp.pgdev.sap.corp:80**. For example:
     ServerName vantgvmwinpb01.dhcp.pgdev.sap.corp:80
   - To allow access only from machines in the **sap.corp** domain, update the **htdocs Directory** block as follows.
     a. Locate the following block in the httpd.conf file:

```
DocumentRoot "c:/Apache24/htdocs"
<Directory "c:/Apache24/htdocs">
    #
    # Possible values for the Options directive are "None", "All",
    # or any combination of:
    #   Indexes Includes FollowSymLinks SymLinksifOwnerMatch ExecCGI MultiViews
    #
    # Note that "MultiViews" must be named *explicitly* --- "Options All"
    # doesn't give it to you.
    #
    # The Options directive is both complicated and important.  Please see
    # http://httpd.apache.org/docs/2.4/mod/core.html#options
    # for more information.
    #
    Options Indexes FollowSymLinks

    #
    # AllowOverride controls what directives may be placed in .htaccess files.
    # It can be "All", "None", or any combination of the keywords:
    #   Options FileInfo AuthConfig Limit
    #
    AllowOverride None

    #
    # Controls who can get stuff from this server.
    #
    Require all granted
</Directory>
```

b. Modify the **Options** directive and **Require** directive as follows:

```
DocumentRoot "c:/Apache24/htdocs"
<Directory "c:/Apache24/htdocs">
    #
    # Possible values for the Options directive are "None", "All",
    # or any combination of:
    #   Indexes Includes FollowSymLinks SymLinksifOwnerMatch ExecCGI MultiViews
    #
    # Note that "MultiViews" must be named *explicitly* --- "Options All"
    # doesn't give it to you.
    #
    # The Options directive is both complicated and important.  Please see
    # http://httpd.apache.org/docs/2.4/mod/core.html#options
    # for more information.
    #
    Options +Indexes -ExecCGI

    #
    # AllowOverride controls what directives may be placed in .htaccess files.
    # It can be "All", "None", or any combination of the keywords:
    #   Options FileInfo AuthConfig Limit
    #
    AllowOverride None

    #
    # Controls who can get stuff from this server.
    #
    Require host sap.corp
</Directory>
```

- For extra security, disable access to the **cgi-bin** directory to prevent access to CGI scripts that could be run using the **-ExecCGI** option:
  a. Locate the following block in the httpd.conf file:

```
<Directory "c:/Apache24/cgi-bin">
    AllowOverride None
    Options None
    Require all granted
</Directory>
```

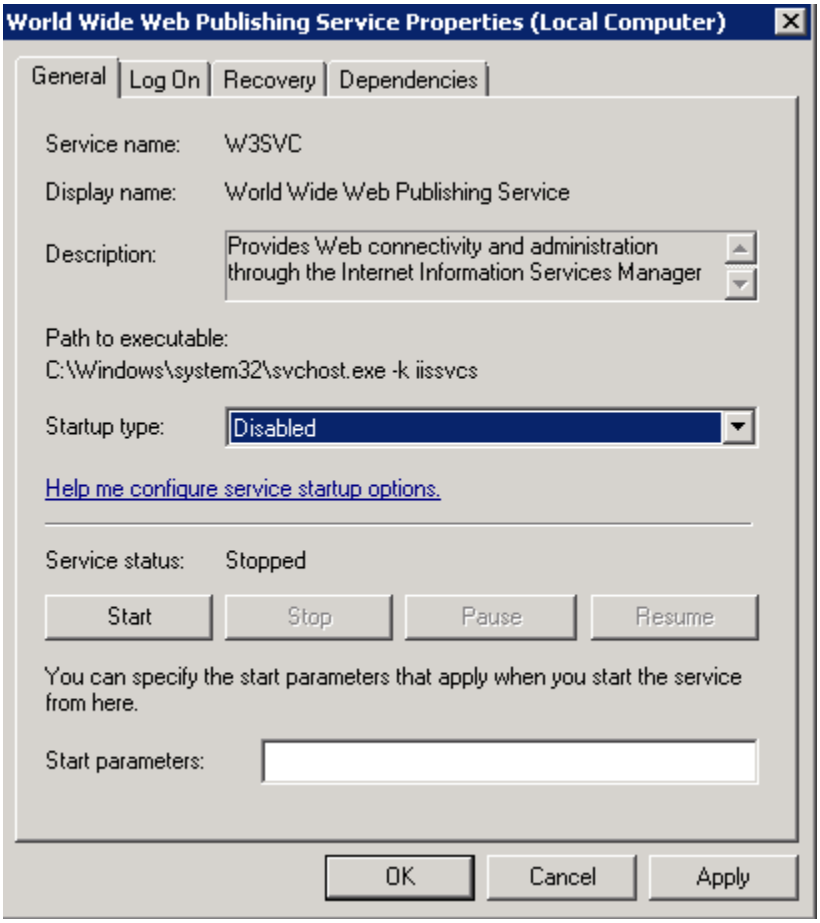
  b. Modify the **Require** directive as follows:

```
<Directory "c:/Apache24/cgi-bin">
    AllowOverride None
    Options None
    Require all denied
</Directory>
```

  c. Save the httpd.conf file.

6. Disable the IIS/World Wide Web Publishing Service so that Apache may listen on TCP ports 80 and 443.
   This is necessary because the server will host Apache as a web server.

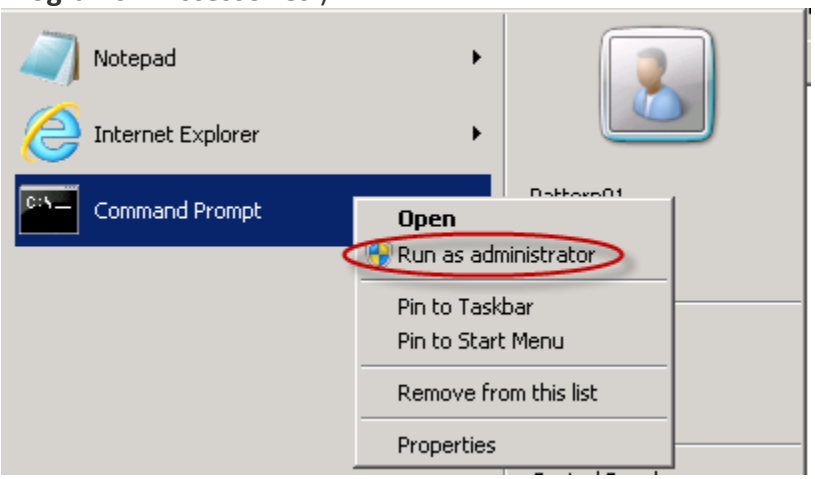
   - Click **Start** > **Run**, and in the **Open** box type services.msc.
     The "Services" dialog box opens.
   - Click **World Wide Web Publishing Service**, and click **Stop**.
   - Double-click **World Wide Web Publishing Service**.
     The "World Wide Web Publishing Service Properties (Local Computer)" dialog box opens.
   - In the **Startup type** box, select **Disabled**.



7. Install Apache 2.4 as a service that can be started automatically:

- To ensure Windows 2008 permissions properly allow the addition of a new Windows service, run the command prompt as Administrator:

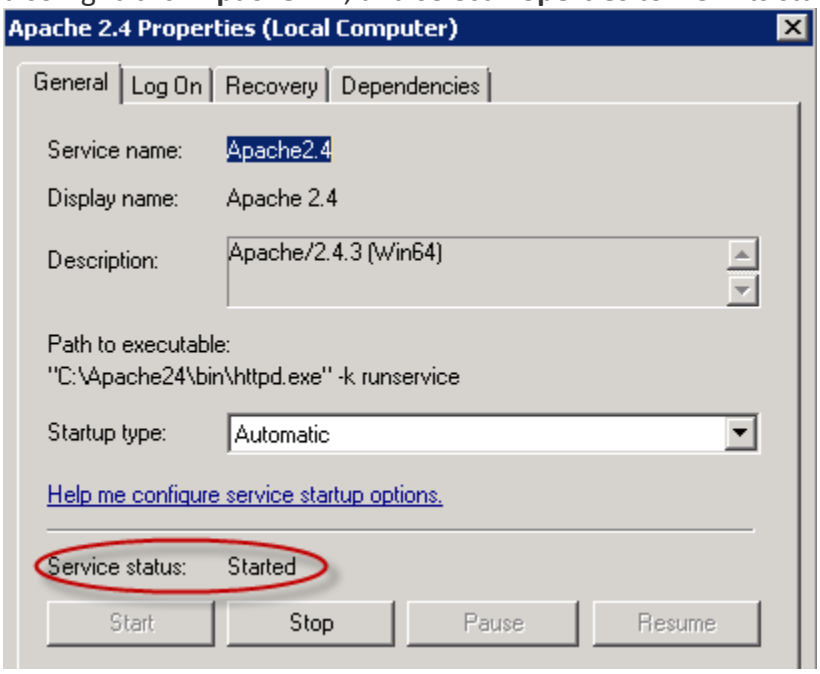
Click **Start**, right-click **Command Prompt**, and select **Run as Administrator**.
(If the **Command Prompt** option is not available on the Start menu, click **Start** > **All Programs** > **Accessories**.)



8. To allow users access on TCP port 80, add a Windows Firewall rule:
   a. Click **Start** > **Administrative Tools** > **Windows Firewall with Advanced Security**.
      The "Windows Firewall with Advanced Security on Local Computer" dialog box opens.
      The default Domain Profile in the pattern blocks inbound connections:

   b. In the "Windows Firewall with Advanced Security on Local Computer" pane (left side), right-click **Inbound Rules**, and select**New Rule**.
      The "New Inbound Rule" wizard opens.
   c. Select **Port**, and click **Next**.
   d. Ensure **TCP** is selected, and ensure **Specific local ports** is selected.
   e. In the **Specific local ports** box, type 80, and then click **Next**.
      Warning:To enable SSL traffic you would enter 443 instead, or allow access on both ports with the format 80, 443
   f. Ensure Allow **the connection** is selected, and click **Next**.
   g. Leave all options selected under the **Profile** section, and click **Next**.
   h. In the **Name** box, type HTTPD Inbound, and click **Finish**.
9. Test to ensure the core Apache service works and can be reached on port 80.
   a. Return to the **Services** snap in, or re-launch it by running the following command:
      Click **Start** > **Run**, and in the **Open** box type services.msc.
      The "Services" dialog box opens.

b. Refresh the "Services" dialog box by pressing **F5** on the keyboard, and then verify that the service **Apache 2.4** appears in the**Services (Local)** list.
c. Select **Apache 2.4**, and click **Start**.
The Status column indicates that Apache 2.4 has a status of **Started**. (You can also right-click **Apache 2.4**, and select**Properties** to view its status.)



d. In a web browser, go to http://vantgvmwinpb01.dhcp.pgdev.sap.corp.
e. On that web page, you will see the message "It works!"

Securing the Apache web server

Running the Apache Service as a Domain Account

After confirming that the web server is accessible when launched by the default **Local System** account, Apache must be configured to run as a service account with limited privileges on the web server, for the following reasons:* Apache must run as a domain account to access the network resources it needs.

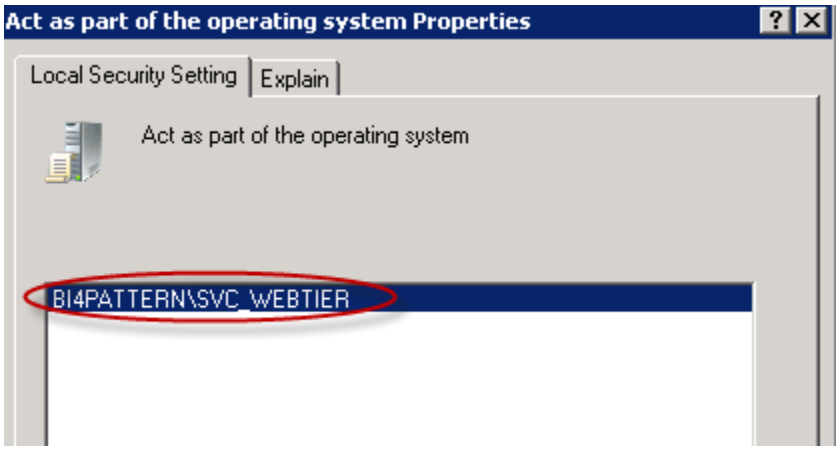
- To prevent unauthorized access to the entire system if Apache is compromised.

Workflow and additional information

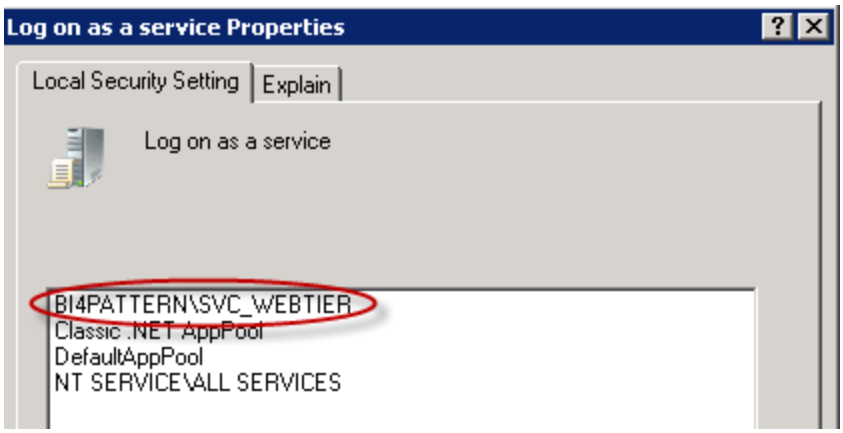
To secure the Apache Service account by setting it to run as a Domain account, you must do the following:* Modify the Local Security policy.

For more information about, see "Running Apache as a Serviceat http://httpd.apache.org/docs/2.4/en/platform/windows.html.

- Grant permissions to the Apache Service account.
- Modify the Apache Service account
    1. Log in to machine winpb01 using the account BI4PATTERN\BIPattern01.
    2. Click **Start** > **Administrative Tools** > **Local Security Policy**.
       The "Local Security Policy" dialog box opens.
    3. Expand Local Policies > User Rights Assignment.
    4. Double-click **Act as Part of the Operating System**.
       The "Act as part of the operating system Properties" dialog box opens.
    5. Click **Add Users or Group**.
       The "Select Users, Computers, Service Accounts, or Groups" dialog box opens.
    6. In the **Enter the object names to select** box, type BI4PATTERN\SVC_WEBTIER, and click **OK**.



    7. In the "Local Security Policy" dialog box, double-click **Log on as a service**, add the BI4PATTERN\SVC_WEBTIER account, and then click **OK**.



    8. Close the "Local Security Policy" dialog box.

To grant Permissions to the Apache service account

You need to grant the **SVC_WEBTIER** account the necessary privileges to run Apache. To add the **SVC_WEBTIER** account to the local**Users** group:

1. Go to Start > Administrative Tools > Active Directory Users and Computers>BI4PATTERN.COM > Builtin >
2. Double-click Users>Members >
3. Add > BI4PATTERN\SVC_WEBTIER
4. Click **OK** all the way out to complete the process.

Warning: Users Group Privileges

Members of the **Users** group inherit Read access to resources on the local machine. Apache requires Read access to most resources within its directory structure, but permissions must be added manually (as shown in the next task) to ensure only the minimum required rights are applied.

To modify the Apache Service account

1. To open Apache, click **Start** > **Run**, and in the **Open** box type C:\Apache24.
2. Right-click the logs directory, and select **Properties**.
   The "logs Properties" dialog box opens.
3. On the **Security** tab, click **Edit**.
   The "Permissions for logs" dialog box opens.
4. Click **Add**.
   The "Select Users, Computers, Service Accounts, or Groups" dialog box opens.
5. In the **Enter the object names to select** box, type BI4PATTERN\SVC_WEBTIER, and click **OK**.
6. In the "Permissions for logs" dialog box, grant to the SVC_WEBTIER account the **Modify**, **Read & execute**, **Read**, and **Write**permissions to the logs directory, and then click **OK**.
7. Stop the Apache Service:
   a. Click **Start** > **Run**, and in the **Open** box type services.msc.
      The "Services" dialog box opens.
   b. Select **Apache 2.4**, and click **Stop**.
8. Return to the C:\Apache2.4 directory, and double-click **logs**.
9. To clear the directory for the new service account, delete all files in the logs directory.
10. Return to the "Services" dialog box, and double-click the **Apache 2.4** service.
11. On the **Log On** tab, click **This account**.

12. For the account, type BI4PATTERN\SVC_WEBTIER.
13. For the password, type WebTier*123, and then click **OK**.
14. Restart the Apache 2.4 service.

Note: If the service fails to start, to troubleshoot the problem, follow the steps shown here: http://httpd.apache.org/docs/2.4/en/platform/windows.html.

Configuring the reverse proxy

A reverse proxy is useful when making a BI platform 4.0 environment available to the web while ensuring the application server is not directly accessible to external users. In that case, a reverse proxy is configured to make calls through the firewall, and deliver content to external clients.

In Apache 2.4, the module mod_proxy is used to deploy this functionality.
The mod_proxy module is extended by additional modules:*mod_proxy_http, which provides proxy functionality over HTTP or HTTPS.

- mod_proxy_ajp, which uses AJP13 protocol.
- mod_proxy_balancer, which delivers load balancing as part of the proxy solution.

This pattern uses mod_proxy_http as an extension to mod_proxy, for the following reasons:

- The use of mod_proxy_http has been tested and proven to be robust, secure, and scalable. For more information, see **BIP on Linux with Tomcat and Sybase ASE Pattern Book**.
- Most architectures require all communication originating from the web to be secured over SSL. The AJP protocol does not natively support this, and therefore a reverse proxy is needed.

Workflow

To configure the reverse proxy for this pattern, you do the following:

- Configure mod_proxy_http.
- Configure Tomcat to communicate with the reverse proxy.
- Test the reverse proxy.

To configure mod_proxy_http

1. Log in to machine winpb01 using the account BI4PATTERN\BIPattern02.
2. In a text editor, open this file C:\Apache24\conf\httpd.conf.
3. Uncomment the following 5 lines to enable proxy and dependent functionality:

- LoadModule proxy_module modules/mod_proxy.so
- LoadModule proxy_http_module modules/mod_proxy_http.so
- LoadModule proxy_balancer_module modules/mod_proxy_balancer.so
- LoadModule lbmethod_bybusyness_module modules/mod_lbmethod_bybusyness.so
- LoadModule lbmethod_byrequests_module modules/mod_lbmethod_byrequests.so

Warning: Apache 2.4 has separated the modules needed to implement individual load balancing algorithms. The byrequests method is the default algorithm and is required for all configurations. This pattern uses by busyness, a method suitable for "bursty" applications such as BI platform.

For more information about load balancing algorithms, see http://httpd.apache.org/docs/current/mod/mod_proxy_balancer.html.

4. To define the proxy-enabled load balancer, add the following block of text to the bottom of the httpd.conffile:

```
#Define Reverse Proxy Load Balancer

<Proxy balancer://BI4Pattern>

BalancerMember http://vantgvmwinpb02.dhcp.pgdev.sap.corp:8080/ max=64
connectiontimeout=1200 keepalive=on route=vantgvmwinpb02
BalancerMember http://vantgvmwinpb03.dhcp.pgdev.sap.corp:8080/ max=64
connectiontimeout=1200 keepalive=on route=vantgvmwinpb03

ProxySet lbmethod=bybusyness
ProxySet stickysession=JSESSIONID
</Proxy>
```

5. To enable reverse proxy for each of the BI platform web applications, add the following block of text below the load balancer section:

```
#Define ProxyPass Rules for Reverse Proxy

#AdminTools for Query Builder
<Location /AdminTools>
ProxyPass balancer://BI4Pattern/AdminTools stickysession=JSESSIONID
ProxyPassReverse balancer://BI4Pattern/AdminTools
ProxyPassReverseCookiePath balancer://BI4Pattern/AdminTools /AdminTools
</Location>

#BOE access to BI Launch Pad and CMC
<Location /BOE>
ProxyPass balancer://BI4Pattern/BOE stickysession=JSESSIONID
ProxyPassReverse balancer://BI4Pattern/BOE
ProxyPassReverseCookiePath balancer://BI4Pattern/BOE /BOE
</Location>

<Location /BusinessProcessBI>
ProxyPass balancer://BI4Pattern/BusinessProcessBI stickysession=JSESSIONID
ProxyPassReverse balancer://BI4Pattern/BusinessProcessBI
ProxyPassReverseCookiePath balancer://BI4Pattern/BusinessProcessBI
/BusinessProcessBI
</Location>

<Location /clientapi>
ProxyPass balancer://BI4Pattern/clientapi stickysession=JSESSIONID
ProxyPassReverse balancer://BI4Pattern/clientapi
ProxyPassReverseCookiePath balancer://BI4Pattern/clientapi /clientapi
</Location>

#Web Service access
<Location /dswsbobje>
ProxyPass balancer://BI4Pattern/dswsbobje stickysession=JSESSIONID
ProxyPassReverse balancer://BI4Pattern/dswsbobje
ProxyPassReverseCookiePath balancer://BI4Pattern/dswsbobje /dswsbobje
</Location>

#MobileBIService access
<Location /MobileBIService>
ProxyPass balancer://BI4Pattern/MobileBIService stickysession=JSESSIONID
ProxyPassReverse balancer://BI4Pattern/MobileBIService
ProxyPassReverseCookiePath balancer://BI4Pattern/MobileBIService /MobileBIService
</Location>

#MOBIServer access
<Location /MOBIServer>
ProxyPass balancer://BI4Pattern/MOBIServer stickysession=JSESSIONID
ProxyPassReverse balancer://BI4Pattern/MOBIServer
ProxyPassReverseCookiePath balancer://BI4Pattern/MOBIServer /MOBIServer
</Location>
```

6. To enable the load balancer management interface, add the following block of text bellow the reverse proxy section:

```
<Location /balancer-manager>
    SetHandler balancer-manager
    Require host vantgvmwinpb01.dhcp.pgdev.sap.corp
</Location>
```

Warning: This interface lets an administrator enable or disable load balancer members, and therefore must be secured to prevent unauthorized access. The directive here ensures it can only be accessed by a user connected to the physical machine where the proxy resides.

7. Save and close the file.
8. To apply the settings, restart the **Apache 2.4** service.

To configure Tomcat to communicate with the reverse proxy

1. Log in to machine winpb02 using the account BI4PATTERN\BIPattern02.
2. In a text editor, open this file C:\tomcat6\conf\server.xml.
3. Add the proxyName and proxyPort properties to the HTTP connector.
   a. Locate the following line:
   ```
   <Connector port="8080" protocol="HTTP/1.1"
   connectionTimeout="20000" redirectPort="8443"
   compression="on" URIEncoding="UTF-8"
   compressionMinSize="2048"
   noCompressionUserAgents="gozilla, traviata"
   compressableMimeType="text/html,text/xml,text/plain,te
   xt/css,text/javascript,text/json,application/json"/>
   ```
   b. Modify it as follows:
   ```
   <Connector port="8080" protocol="HTTP/1.1"
   connectionTimeout="20000" redirectPort="8443"
   compression="on" URIEncoding="UTF-8"
   compressionMinSize="2048"
   noCompressionUserAgents="gozilla, traviata"
   compressableMimeType="text/html,text/xml,text/plain,te
   xt/css,text/javascript,text/json,application/json"
   proxyName="vantgvmwinpb01.dhcp.pgdev.sap.corp"
   proxyPort="80"/>
   ```
4. Configure the jvmRoute property to match the Apache load balancer worker.
   a. Locate the following line:
   ```
   <Engine name="Catalina" defaultHost="localhost">
   ```
   b. Modify it as follows:
   ```
   <Engine name="Catalina" defaultHost="localhost"
   jvmRoute="vantgvmwinpb02">
   ```
5. Save and exit the file.
6. To apply the changes, restart the Tomcat 6 service.

7. Log in machine winpb03 using the account BI4PATTERN\BIPattern03.
8. In a text editor, open this file C:\tomcat6\conf\server.xml.
9. Add the properties proxyName and proxyPort to the HTTP connector.
   Locate the following line:

```
<Connector port="8080" protocol="HTTP/1.1"
connectionTimeout="20000" redirectPort="8443"
compression="on" URIEncoding="UTF-8"
compressionMinSize="2048" noCompressionUserAgents="gozilla,
traviata"
compressableMimeType="text/html,text/xml,text/plain,text/cs
s,text/javascript,text/json,application/json"/>
```

   Modify it as follows:

```
<Connector port="8080" protocol="HTTP/1.1"
connectionTimeout="20000" redirectPort="8443"
compression="on" URIEncoding="UTF-8"
compressionMinSize="2048" noCompressionUserAgents="gozilla,
traviata"
compressableMimeType="text/html,text/xml,text/plain,text/cs
s,text/javascript,text/json,application/json"
proxyName="vantgvmwinpb01.dhcp.pgdev.sap.corp"
proxyPort="80"/>
```

10. Configure the property jvmRoute to match the Apache load balancer worker.
    Locate the following line : `<Engine name="Catalina" defaultHost="localhost">`
    Modify it as follows: `<Engine name="Catalina" defaultHost="localhost" jvmRoute="vantgvmwinpb03">`
11. Save and exit the file.
12. To apply the changes, restart the **Tomcat 6** service.

To test the reverse proxy

1. Log in to machine winpb01 using the account BI4PATTERN\BIPattern01.
2. Open a web browser, and go to http://vantgvmwinpb01.dhcp.pgdev.sap.corp/balancer-manager.
   The following page is displayed:

Load Balancer Manager for vantgvmwinpb01.dhcp.pgdev.sap.corp

Server Version: Apache/2.4.3 (Win64)
Server Built: Aug 18 2012 14:13:48

LoadBalancer Status for balancer://bi4pattern

MaxMembers	StickySession	DisableFailover	Timeout	FailoverAttempts	Method	Path	Active
2 [2 Used]	JSESSIONID	Off	0	1	bybusyness	/cluster	Yes

Worker URL	Route	RouteRedir	Factor	Set	Status	Elected	Busy	Load	To	From
http://vantgvmwinpb02.dhcp.pgdev.sap.corp:8080/	vantgvmwinpb02		1	0	Init Ok	199	0	-26	275K	503K
http://vantgvmwinpb03.dhcp.pgdev.sap.corp:8080/	vantgvmwinpb03		1	0	Init Ok	161	0	26	302K	592K

3. Open a new web browser window, and go to http://vantgvmwinpb01.dhcp.pgdev.sap.corp/BOE/BI.
   The BI Launch Pad Log On page is displayed.

4. Return to the balancer-manager page, and refresh it.
   Note the change in number in the **Elected** column on one of the nodes.
   The **Busy** column will quickly increment as well.

Enabling the proxy cache

The Apache web server works efficiently with BI platform because Apache caches static resources, such as JavaScript and HTML files, instead of storing them on the server. BI platform uses those files frequently, and Apache can serve them quickly from the cache.

In this pattern, mod_cache_disk is used to store cache on the local drive. This pattern does not use mod_cache_mem (for in-memory caching) because mod_cache_mem is bound to an individual process and does not persist when the service is restarted.

In this pattern, the static content is initially stored on Tomcat, but subsequent storage of static resources is cached for faster response.
For more information about creating a static content split, and manipulating headers, see Improving the User Experience in SAP BI Platform 4.0 with Apache and WDeploy.

Workflow and additional information

- **Prepare the file system.**
  To use mod_cache, you must create a directory on the local machine where Apache has permissions to write files. It is recommended that the directory be separate from the Apache installation directory to avoid conflicts with existing permissions.

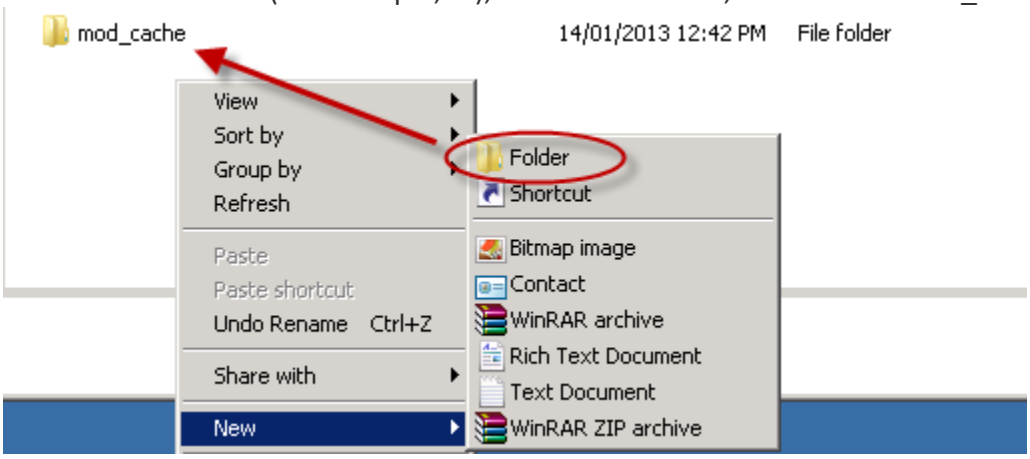
- **Configure mod_cache.**
  The next step is to configure Apache to load and enable the mod_cache module.
- **Schedule the htcacheclean process for cache management.**
  To manage disk space used by mod_cache, set up the Apache automated clean-up process named htcacheclean.
  htcacheclean can also be used from the command line to list the URL currently available in cache or to remove individual entities. For more information, go to http://httpd.apache.org/docs/current/en/programs/htcacheclean.html.
- **Test the cache.**
  Test and confirm that the module is functioning as expected.
  Steps provided here are based on the "Cache Status and Logging" section of the "Apache Module mod_cache" page athttp://httpd.apache.org/docs/current/en/mod/mod_cache.html.

  It is recommended to take steps to avoid a multitude of requests being sent to the server when a page is not in the cache. For more information, see the section "Avoiding the thundering heard" at http://httpd.apache.org/docs/current/en/mod/mod_cache.html.

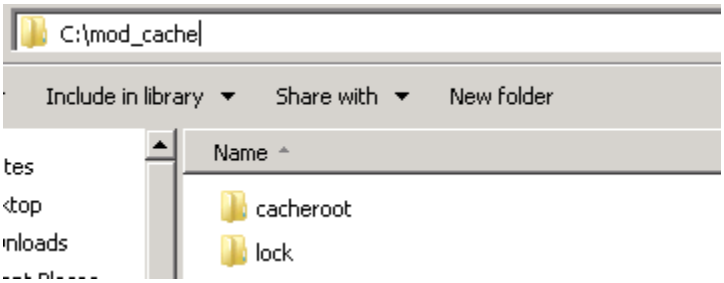
  For more information about using a cache system with Apache, see http://httpd.apache.org/docs/current/en/caching.html.

To prepare the file system

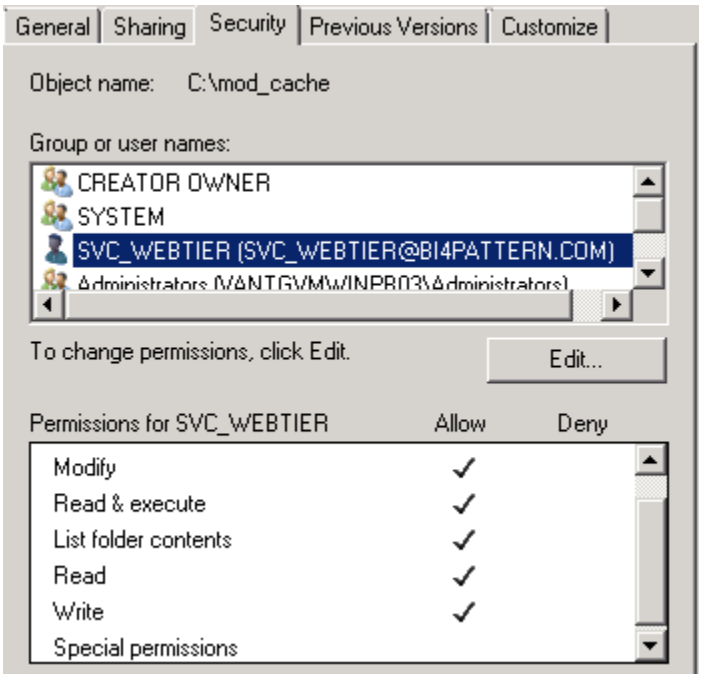
1. Log in to machine winpb01 using the account BI4PATTERN\BIPattern01.
2. Go to the root drive (for example, C:), add a new Folder, and name it mod_cache.



3. Double-click the **mod_cache** folder and create a subfolder named cacheroot.
4. At the same folder level as cacheroot, create another folder, and name it lock.



5. To set security on the mod_cache folder, return to the root of C, right-click **mod_cache**, and select **Properties**.
   The "mod_cache Properties" dialog box opens.
6. On the Security tab, set the permissions on the mod_cache folder:
   a. Click **Edit** > **Add**.
      The "Select Users, Computers, Service Accounts, or Groups" dialog box opens.
   b. In the **Enter the object names to select** box, type BI4PATTERN\SVC_WEBTIER.
   c. Grant **Modify** permissions to the mod_cache folder by selecting the check box in the **Allow** column.



   d. Click **Apply**, and click **OK**.

To configure mod_cache

1. In a text editor, open this file C:\Apache24\conf\httpd.conf.
2. To enable mod_cache and mod_cache_disk, uncomment the following lines:

```
LoadModule cache_module modules/mod_cache.so
LoadModule cache_disk_module modules/mod_cache_disk.so
```

3. To configure mod_cache, scroll to the bottom of the file, and add the following lines:

```
#Remove hostname from ETag so that identical files from winpb02
#and winpb03 Tomcat are not cached separately
FileETag MTime Size

#====================Configure mod_cache==============
<IfModule mod_cache.c>
#Address the Thundering Herd identified in Apache's Caching Guide CacheLock on
CacheLockPath C:/mod_cache/lock
CacheLockMaxAge 5


#This parameter tells Apache to ignore unique session identifiers #when caching
static content.
#SAP BI Platform 4.0 uses the strings jsessionid and bttoken to
#identify user sessions.

CacheIgnoreURLSessionIdentifiers jsessionid bttoken

#Don't cache cookies as they are unique per user

CacheIgnoreHeaders Set-Cookie

#Enable mod_disk_cache instead of mod_mem_cache
<IfModule mod_cache_disk.c>
CacheRoot c:/mod_cache/cacheroot
CacheEnable disk /
CacheDirLevels 2
CacheDirLength 1
</IfModule>
</IfModule>
```

Warning: Apache 2.4 Name Change
In Apache 2.2, mod_cache_disk was named mod_disk_cache. This name change results in a slightly different configuration to the IfModule section in the httpd.config file. The renaming of mod_disk_cache to mod_cache_disk is important to make note of when upgrading from Apache 2.2 to Apache 2.4.

4. To enable mod_cache, restart the Apache service:
   a. Click **Start** > **Run**, and in the **Open** box type services.msc.
      The "Services" dialog box opens.

b. Select Apache 2.4, and click **Restart**.

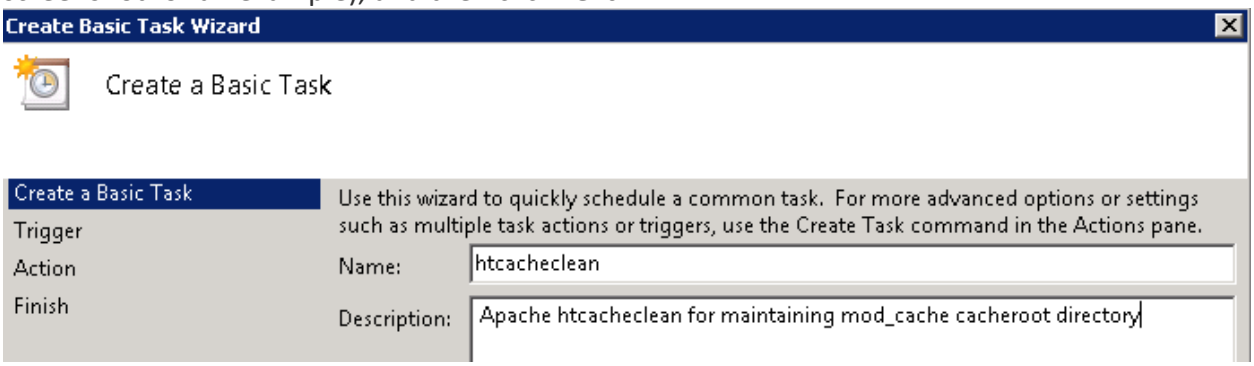
To schedule the htcacheclean process for cache management

On Windows, the htcacheclean process can be configured to run as a scheduled task to maintain the cache at a manageable size. On Linux, this process runs as a daemon, regularly maintaining the cache directory to ensure it doesn't grow too large.

Warning: Log On as a Batch Job

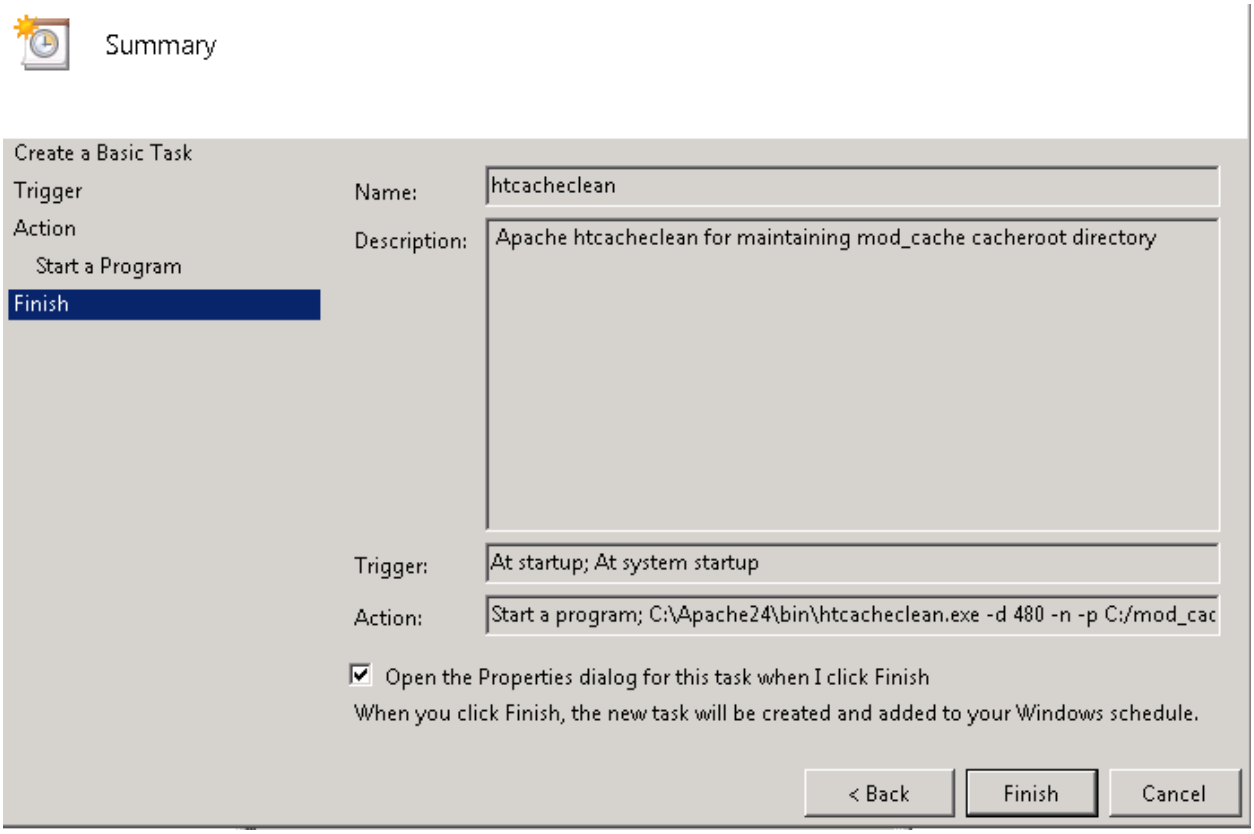
To schedule this process, the Log On as a Batch Job permission must be granted to the service account. This permission is often linked to a domain policy and may require a domain administrator to grant it.

1. Open the Windows task scheduler:
   Click **Start** > **Run**, and in the **Open** box type control.exe schedtasks.
   The "Task Scheduler" dialog box opens.
2. Right-click **Task Scheduler Library** and select **Create Basic Task**.
   The "Create Basic Task" wizard opens.
3. In the **Name** box, type htcacheclean.
4. In the **Description** box, type a description of what htcacheclean will be used for (see screenshot for an example), and then click**Next**.

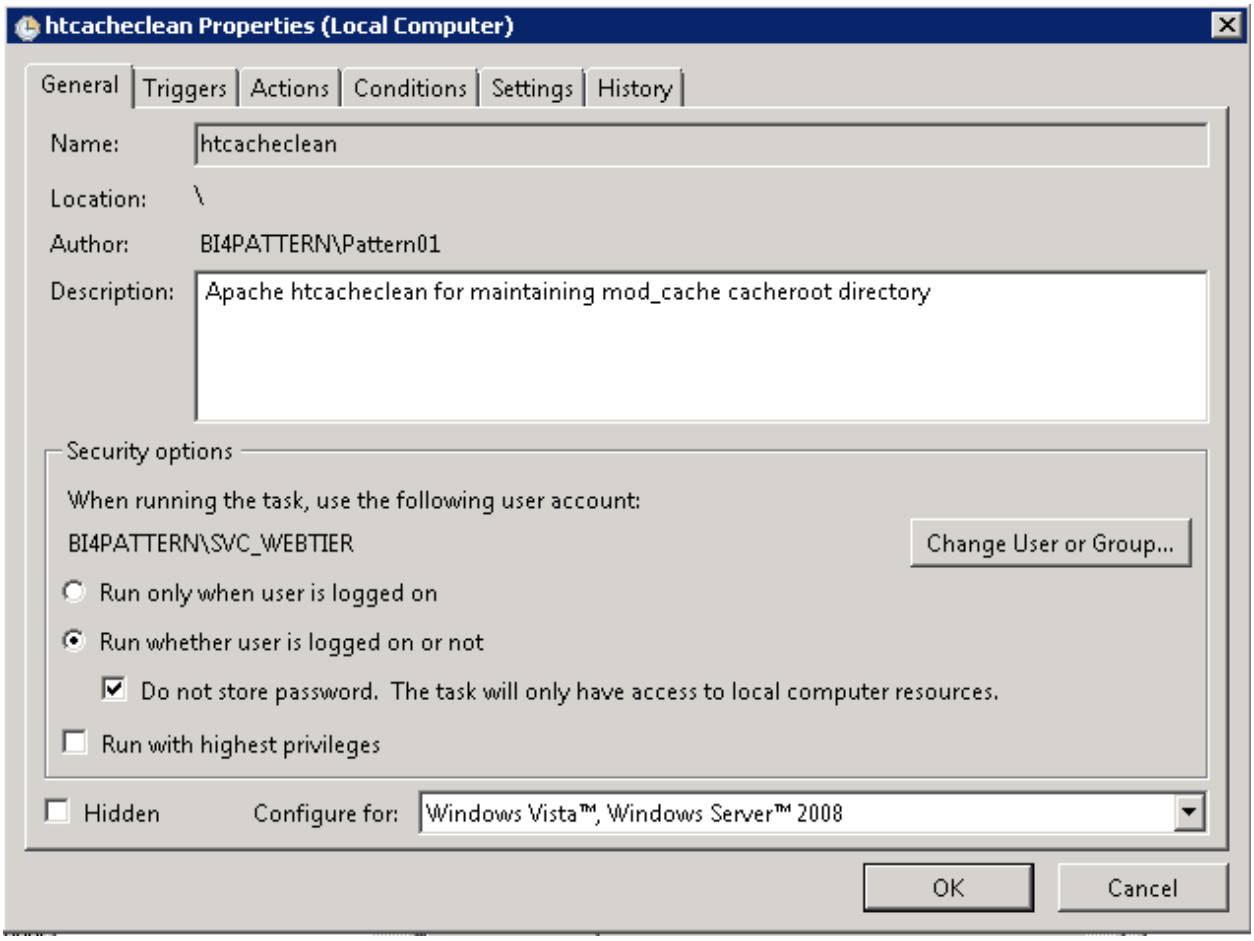


5. On the "Task Trigger" page, select When the computer starts, and click Next.
6. On the "Action" page, select Start a program, and click Next.
7. On the "Start a Program" page, in the Program/script box, type the following:

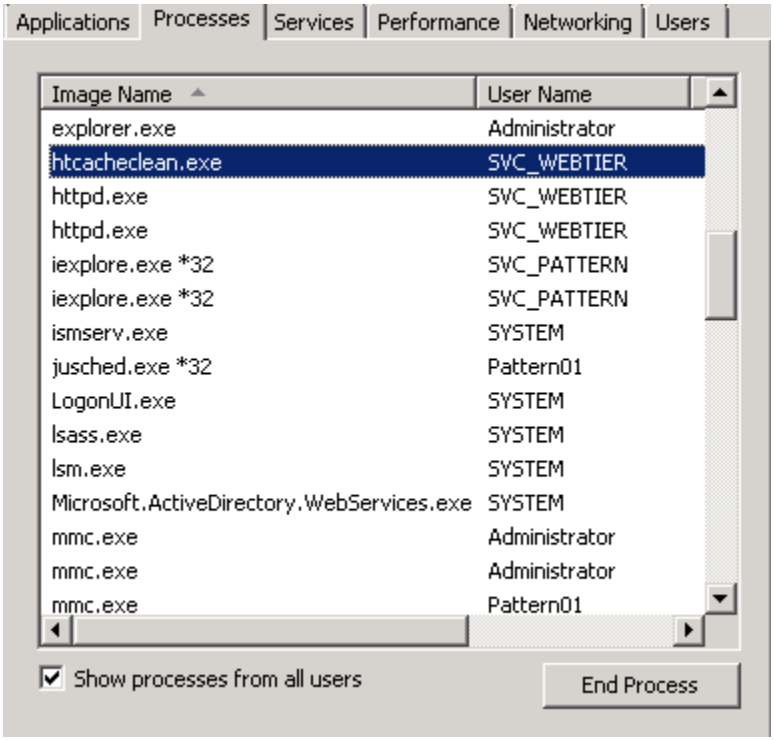
   C:\Apache24\bin\htcacheclean.exe
8. In the Add arguments (optional) box, add the following arguments, and then click Next:
   -d 480 -n -p C:/mod_cache/cacheroot -l 500M --i
   Warning: Type the optional commands but do not copy them. The characters are not preserved correctly when using clipboard and it can cause the htcacheclean process to fail
9. Select the **Open the properties dialog for this task when I click Finish** check box, and click **Finish**.



10. Click the Change User or Group button, type BI4PATTERN\SVC_WEBTIER*, and then click OK.
11. Click Run whether user is logged on or not, select the Do not store password check box, and then click OK.
12. This scheduled task does not require access to non-local resources.



13. For the password, type WebTier*123.
14. Right-click the htcacheclean task, and click Run.
15. Right-click the Windows task bar, and select Start Task Manager.
    The "Windows Task Manager" dialog box opens.
16. On the Processes tab, click Show Processes from all Users.
    The htcacheclean.exe process appears in the list.



This scheduled task will cause **htcacheclean** to run every 480 minutes (8 hours), with a goal of keeping the overall cache at 500 MB. The process will consume minimal system resources and take action only when it detects a modification to the cache.

To test the cache

Testing is especially important with a dynamic application such as BI platform to ensure that private data is not shared between clients.

1. In a text editor, open C:\Apache24\conf\httpd.conf.
2. To have the cache record a log file, scroll to the bottom of the httpd.conf file, and add the following lines:

   ```
   LogFormat "%h %l %u %t \"%r\" %{cache-status}e %>s %b" cache
   CustomLog logs/mod_cache.log cache
   ```

   Note: This block of code configures a custom logging format that contains the Apache variable %{cache-status}, and prints each request to a log file named mod_cache.log. The output records the content that is served from cache, and when content is not served from the cache, the log will record the reasons why.
3. Save and close the file.
4. Run the following commands to stop Apache and clear the **logs** directory for easier reading:
   a. Click **Start** > **Run**, and in the **Open** box type services.msc.
      The "Services" dialog box opens.
   b. Select the **Apache 2.4** service, and click **Stop**.

c. Click **Start** > **Run**, and in the **Open** box type C:\Apache24\logs.
   The "logs" dialog box opens.
d. Select all files (**access** and **error** logs are displayed), and delete them.
e. Return to the "Services" dialog box, select the **Apache 2.4** service, and click **Start.**
f. Return to the "logs" dialog box, and ensure that a new file named mod_cache has been created.

access	15/01/2013 12:25 PM	Text Document	0 KB
error	15/01/2013 12:25 PM	Text Document	1 KB
httpd.pid	15/01/2013 12:25 PM	PID File	1 KB
mod_cache	15/01/2013 12:25 PM	Text Document	0 KB

5. Open Internet Explorer, go to the BI Launch Pad: http://vantgvmwinpb01.dhcp.pgdev.sap.corp/BOE/BI.
6. In the **User Name** box, type Administrator, and for the password type Pattern123.
7. Return to the "logs" dialog box, and double-click the **mod_cache** file.
   Note the following lines that contain details about a cache "miss":

   "GET /BOE/portal/1212190046/shared/js/accessibility/accessibility_util.js HTTP/1.1"
   cache miss: attempting entity save
8. Close the file, and return to Internet Explorer.
9. To ensure requests are sent to Apache, clear the browser cache:
   a. Click Tools > Internet Options > Browsing History > Delete > Delete > Ok.
   b. Click Log Off at the top of the BI Launch Pad.
   c. Log in again to BI Launch Pad, with the user name Administrator and password Pattern123.
   d. Press F5 on your keyboard to ensure the page is actively refreshed.
10. Return to the "logs" dialog box, and open the mod_cache file.
11. Note that the most recent request for accessibility_util.js now displays "cache hit":
    "GET /BOE/portal/1212190046/shared/js/accessibility/accessibility_util.js HTTP/1.1"
    cache hit
    This indicates that mod_cache is now configured correctly.

Setting up the Authentication Server

This pattern uses Windows Active Directory (AD) and SAP authentication. The following sections provide step-by-step instructions and details for the set up.

- Setting up the SAP plug-in
  - Setting up SAP SSO using the Security Token Service (STS)

- Setting up the Windows Active Directory (AD) server
- Setting up the Windows AD plug-in
    - Kerberos
    - Setting up Manual Java Authentication
    - Setting up Single Sign On using Vintela

Setting up the SAP plug-in

This page is the overview of the SAP plugin within the CMC. Select Setting up SAP SSO using the Security Token Service (STS) to find setup instructions for the SAP SSO service.

Prerequisites

When installing BI platform, the SAP authentication plug-in needs to have been selected during the installation.

To use SAP authentication, you must have a Business Warehouse (BW) or Enterprise Core Component (ECC) system to connect to.

About the SAP security plug-in

The SAP security plug-in lets you map user accounts and roles from BW and ECC systems to the BI platform. The plug-in enables the system to verify all login requests that specify SAP authentication. Users are authenticated against the BW or ECC system and have their membership in a mapped SAP role verified, before they are granted an active BI platform session by the CMS. User lists and role memberships are dynamically maintained by the system.

Configuring the BW system for access from BI platform

Before configuring the plug-in in the CMC you will first create a user account and role on the BW system. The user account will be used for searching directory information, and the role will be used to contain the authorization for that account within BW.

Workflow

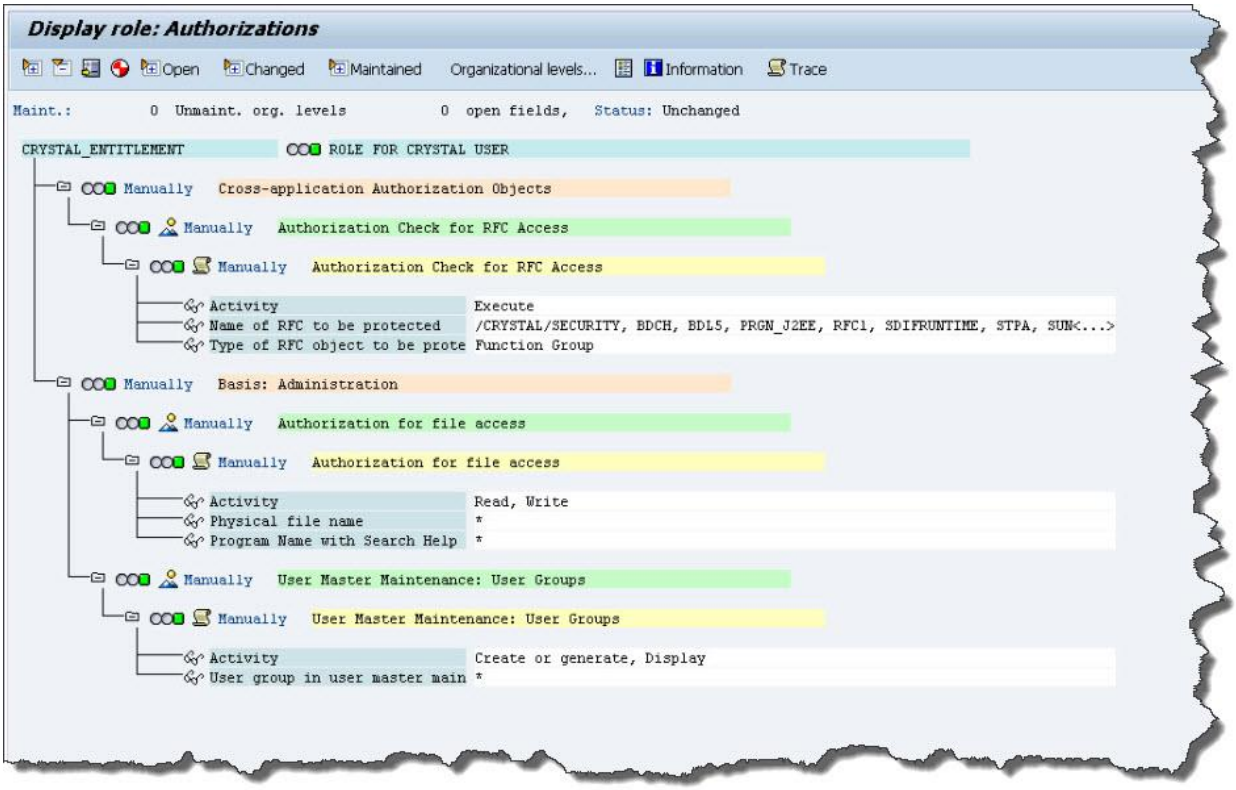
- Create a role in BW.
- Create a user account in BW.
- Configure authentication from the CMC.

To create a role in BW

1. Open a SAPGUI connection to the BW server you will be connecting to, and log in with an account that belongs to the SAP_ALL profile.
2. Run the transaction /npfcg.
3. For the role name, type CRYSTAL_ENTITLEMENT, and click Single Role .
4. To save the role, click **Role > Save**.
5. On the **Authorizations** tab, click **Change Authorization Data**.
6. Set the authorizations as shown in this table:

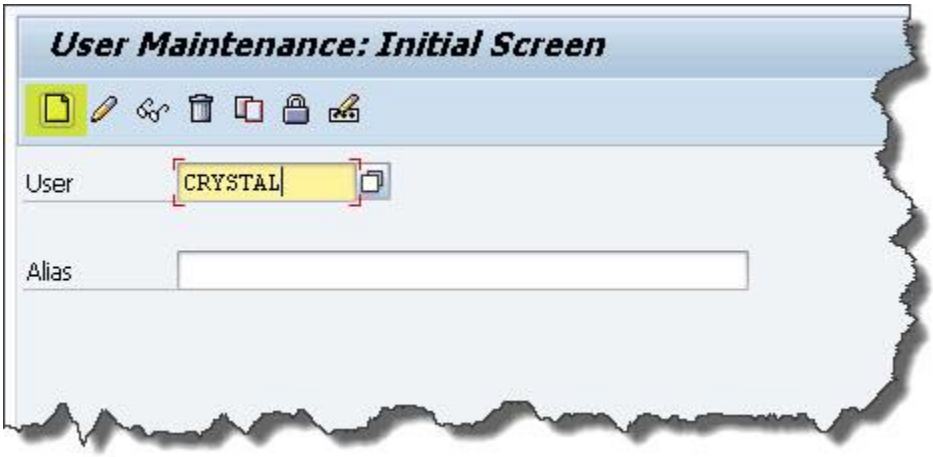
Authorization object	Field	Value
Authorization for file access (S_DATASET)	Activity (ACTVT)	Read, Write (33, 34)
	Physical file name (FILENAME)	* (denotes All)
	ABAP program name (PROGRAM)	*
Authorization Check for RFC Access (S_RFC)	Activity (ACTVT)	16
	Name of RFC to be protected (RFC_NAME)	BDCH, STPA, SUSO, BDL5, SUUS, SU_USER, SYST, SUNI, RFC1, SDIFRUNTIME, PRGN_J2EE, /CRYSTAL/SECURITY
	Type of RFC object to be protected (RFC_TYPE)	Function group (FUGR)
User Master Maintenance: User Groups (S_USER_GRP)	Activity (ACTVT)	Create or Generate, and Display (03)
	User group in user master maintenance (CLASS)	* **Note:** For greater security, you may prefer to explicitly list the user groups whose members require access to BI platform.

7. When complete, verify that the authorizations for the role are as shown here, and then save the settings:



To create a user account in BW

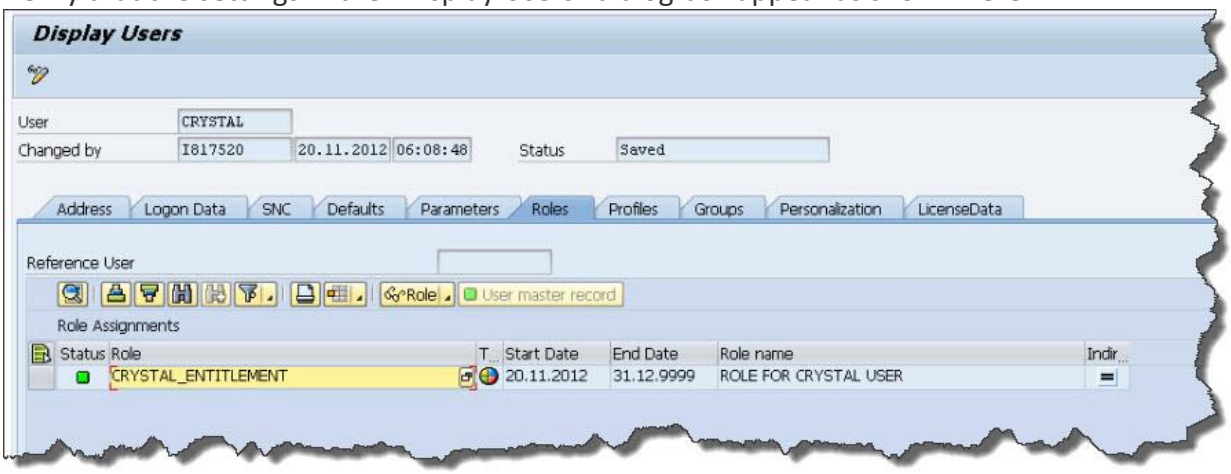
1. Open a SAPGUI connection to the BW server you will be connecting to, and log in with an account that belongs to the SAP_ALL profile.
2. Run the transaction /nsu01.
3. Type the user name CRYSTAL, and click the Create icon.



4. On the **Logon Data** tab, set **User Type** to Dialog.
5. Set an initial password.
   Note: On the Logon Data tab, set User Type to Dialog.

Set an initial password.

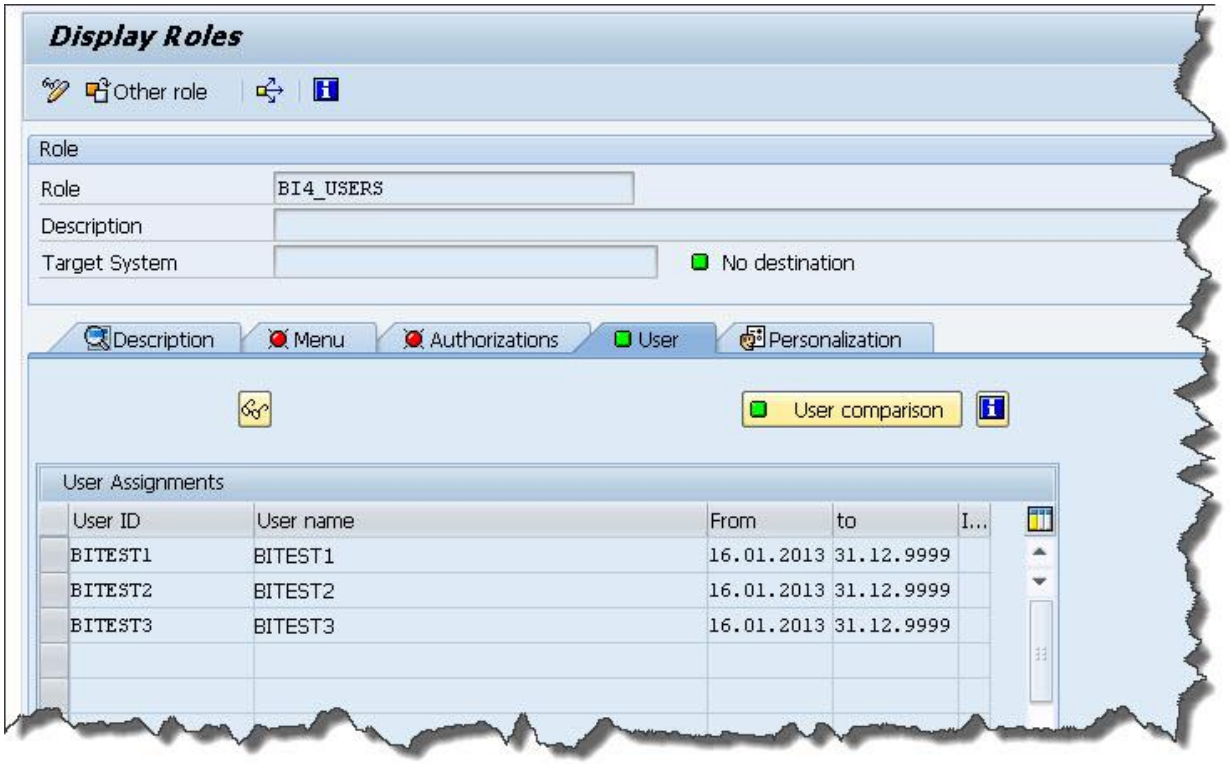
6. On the **Roles** tab, select the first line, and click the **Search** icon (on right side).
7. In the **Single Role** box, type the name of the role you created ({{CRYSTAL_ENTITLEMENT),}}and select the green check box (execute).
8. Select the check box next to the role name, and select the green check again (execute) Verify that the settings in the "Display Users" dialog box appear as shown here:



9. Save the user role.

Reminder: Setting an initial password will mean the first time you log in as this user the password will need to be changed. The next time you log in to the SAPGUI utility, be sure to log in with the CRYSTAL user account so that you can reset the password and clear the initial password status

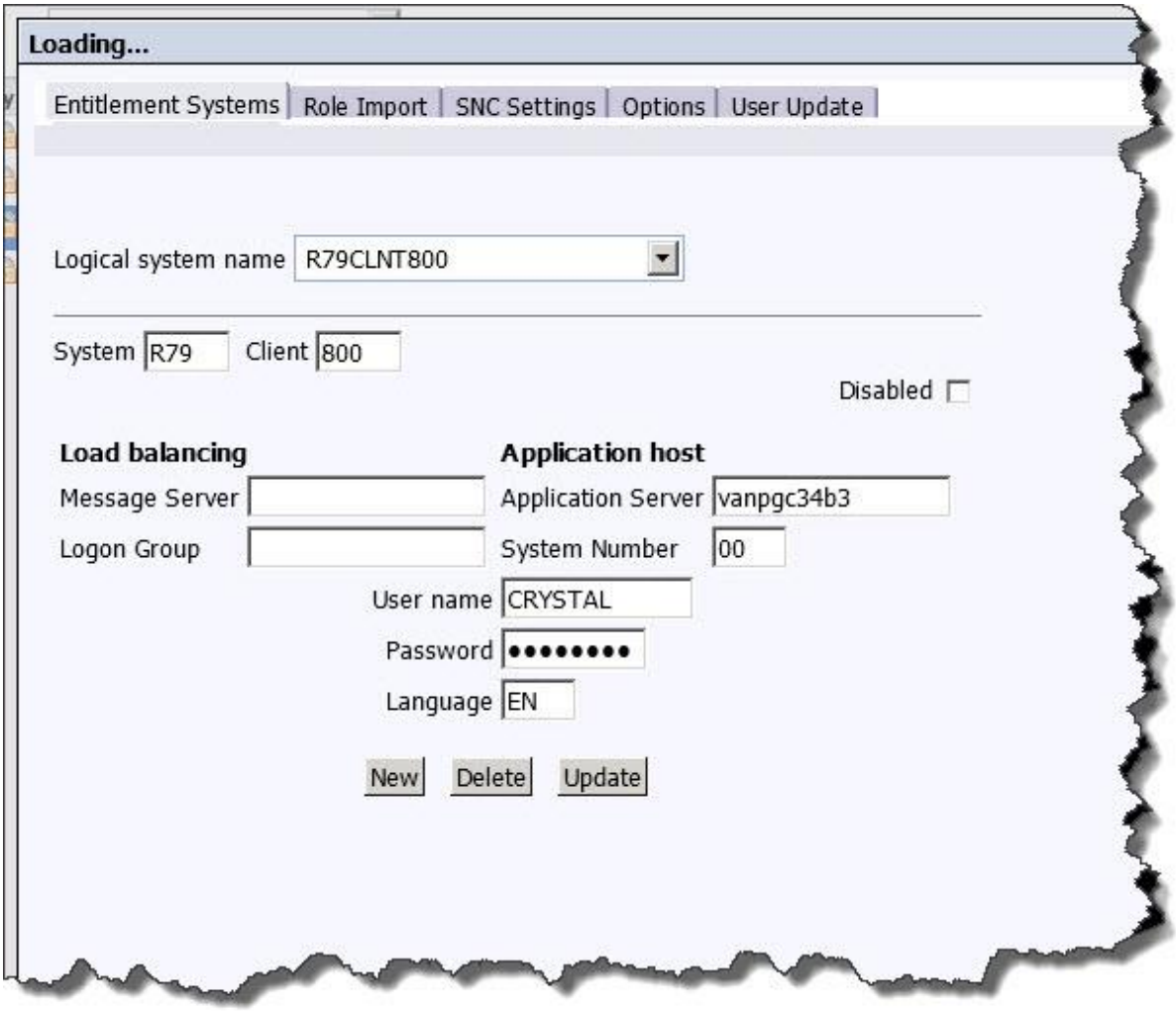
Warning: For the use of this pattern, other user accounts and roles were created.



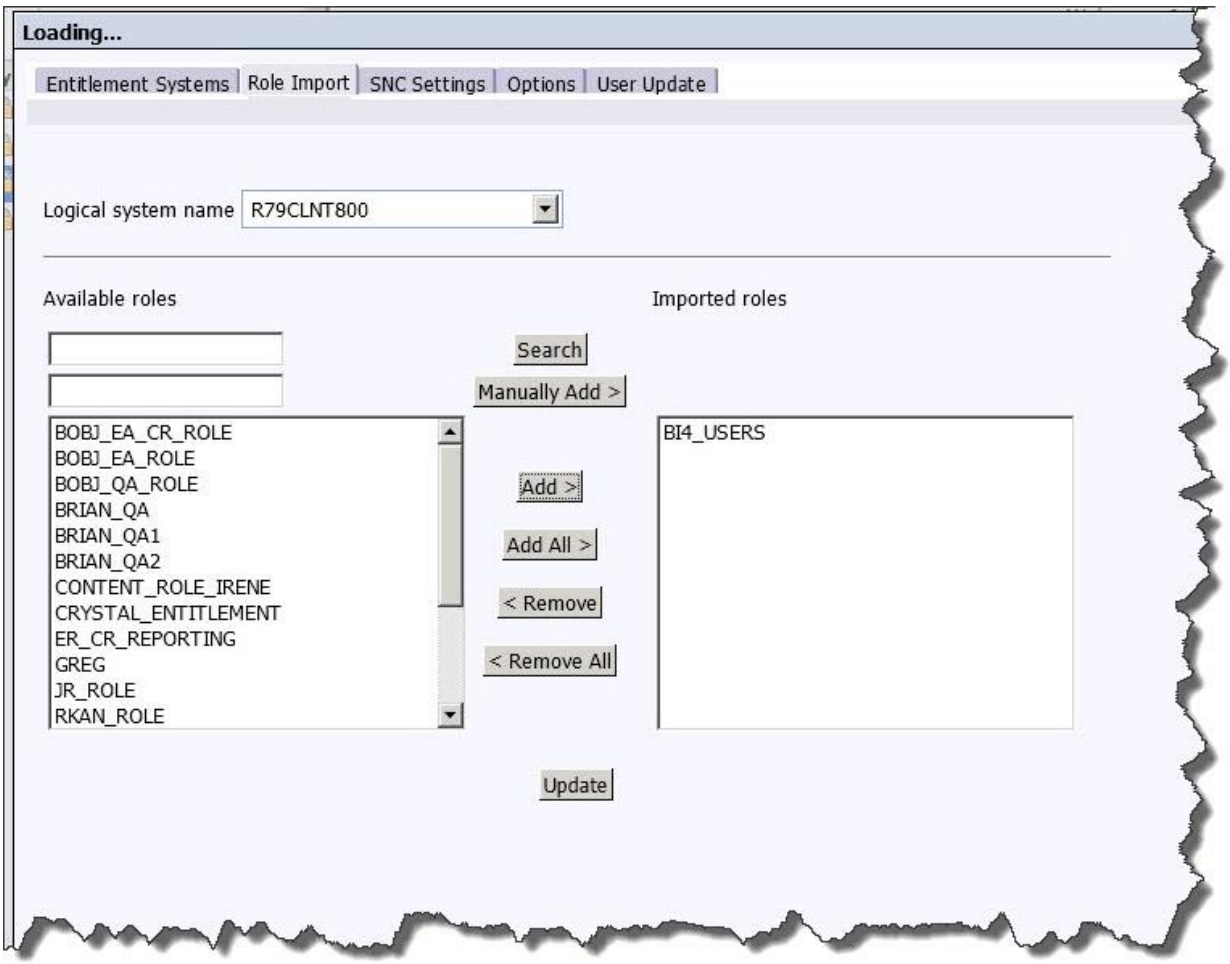
To configure SAP authentication from the CMC

To simplify administration, the BI platform supports SAP authentication for user and group accounts. Before users can use their SAP user name and password to log into the system, their SAP accounts must be mapped to the Business Intelligence platform. Then you can create a new account or link to an existing BI platform account.

1. Open the CMC, and in the "Authentication management" area, and double-click **SAP**.
2. To begin configuring the SAP plug-in, type the credentials in the **System, Client, Application Server, System Number, User name, Password** , and **Language** boxes*.*
3. Press **Update** to commit, the **Logical system name** will appear.



4. Click the **Role Import** tab.
   A list of roles to be populated for the selected entitlement system is displayed.
5. Select the roles that contain user accounts you want to have mapped to Business Intelligence Platform.
   This pattern maps the BI4_USERS role.



6. Click **Update** to commit the change.
7. On the **User Update** tab, in the "Update Roles Only" area click **Update Now**, and in the "Update Roles and Aliases" area click **Update Now**.

The user roles are mapped into the system, with permissions to manually log in using the SAP credentials.

Setting up SAP SSO using the Security Token Service (STS)

Setting up SAP SSO using the Security Token Service (STS)

By using SAP Single Sign-On (SSO) through the Security Token Service (STS), you can schedule reports that use SSO connections to an SAP data source.

Workflow

- Create the certificate and keystore files.
- Add the certificate to the Business Warehouse system.
- Configure the CMC to use the SAP SSO Service.

To create the certificate and keystore files

1. Log in to the machine with administrative permissions, and use a command prompt window to go to C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\win64_x64\sapjvm\bin.

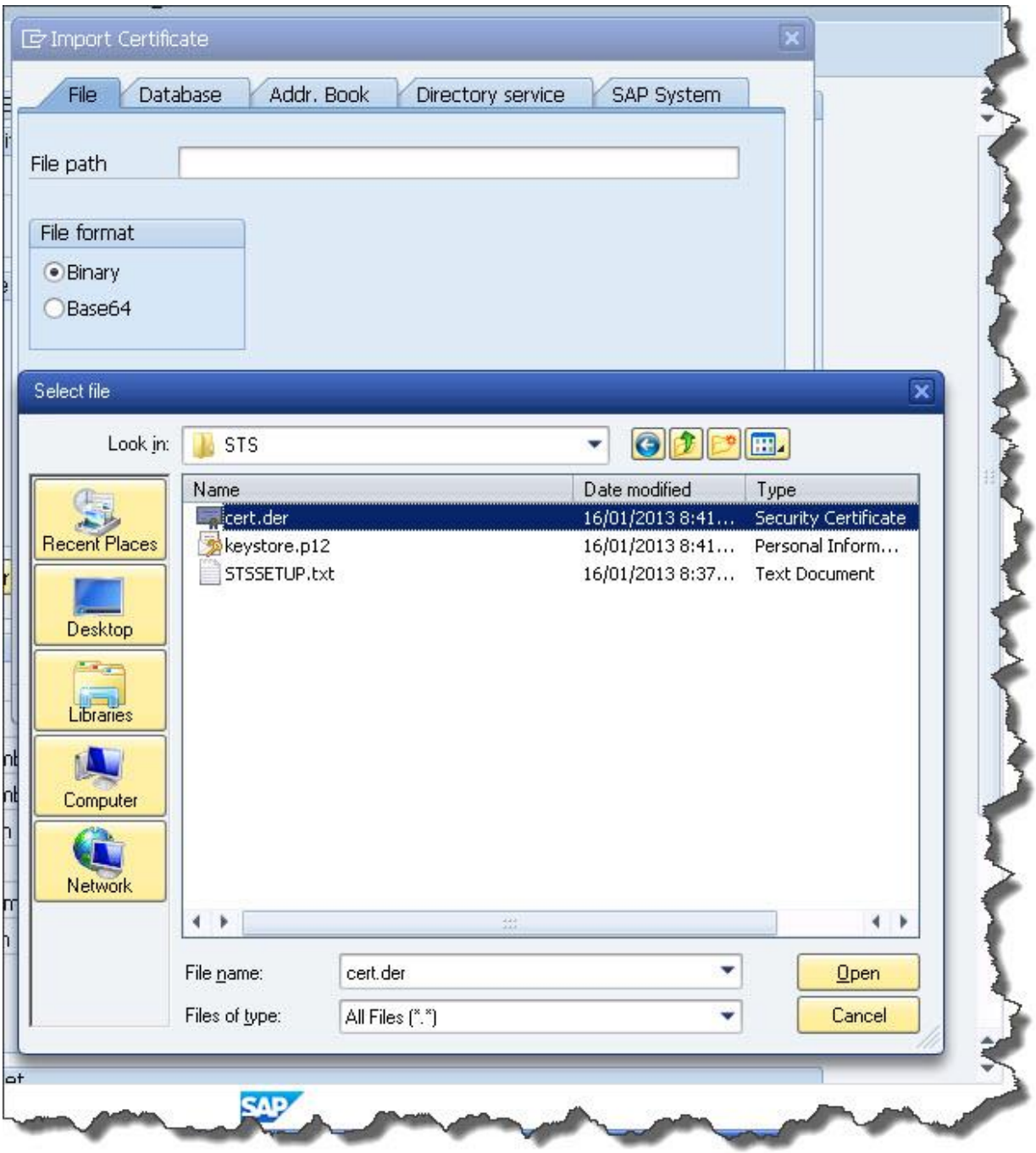
2. Type and run the following command: java -jar "C:\Program files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\java\lib\PKCS12Tool.jar" -alias PATTERNSTS -storepass pattern123 -dname CN=PATTERNSTS.
3. Type and run the following command: keytool -exportcert -keystore keystore.p12 -storetype pkcs12 -file cert.der -alias PATTERNSTS.
4. When prompted to enter the keystore password, type pattern123.

```
C:\Windows\system32>cd "C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessO
bjects Enterprise XI 4.0\win64_x64\sapjvm\bin"

C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0
\win64_x64\sapjvm\bin>java -jar "C:\Program files (x86)\SAP BusinessObjects\SAP
BusinessObjects Enterprise XI 4.0\java\lib\PKCS12Tool.jar" -alias PATTERNSTS -st
orepass pattern123 -dname CN=PATTERNSTS

C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0
\win64_x64\sapjvm\bin>keytool -exportcert -keystore keystore.p12 -storetype pkcs
12 -file cert.der -alias PATTERNSTS
Enter keystore password:
Certificate stored in file <cert.der>
```

5. To view the newly created files, in Windows Explorer browse to C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\win64_x64\sapjvm\bin.

To add the certificate to the BW system

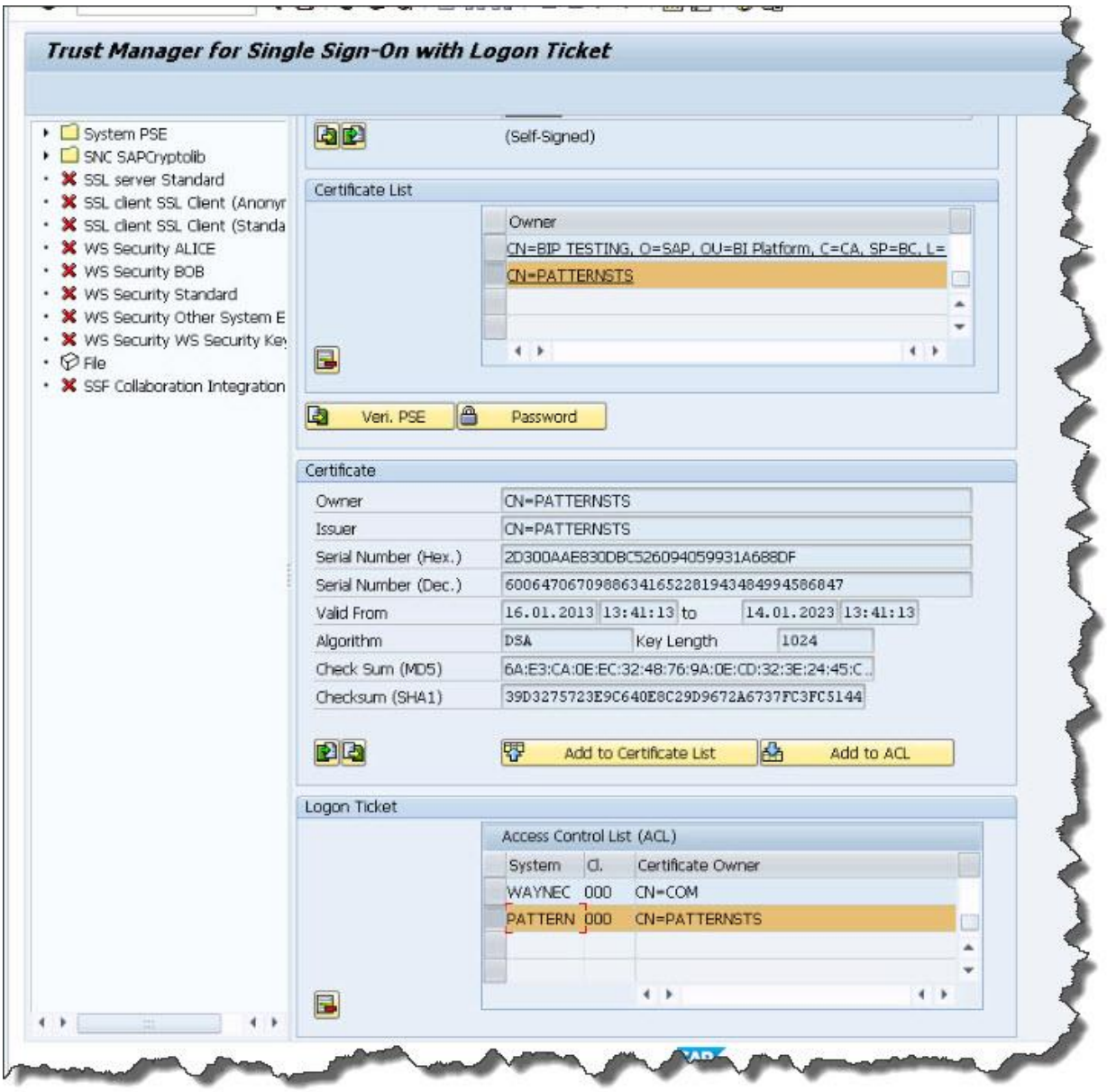
1. Open a SAPGUI connection to the BW server you will be connecting to, and log in with an administrator account.
2. Run the transaction /nstrustsso2.
3. On the menu bar, click **Certificate – Import**.
4. Next to the **File path** box, click the Browse icon, find the file cert.der (created in the previous task), and click Open



5. Ensure the **Binary** format is selected.
6. Click the green check box.
7. Verify the certificate is loaded on the screen as shown here:

8. To add the certificate to the BW servers Certificate List, click **Add to Certificate List**.
9. Click **Add to ACL**.
   The "Add Entry to Single Sign-On Access Control List" dialog box opens,

10. In the System ID box, type PATTERN.
11. In the Client box, type 000.
12. To return to Trust Manager, select the green check box (execute).
    “Trust Manager” displays both keystore entries.

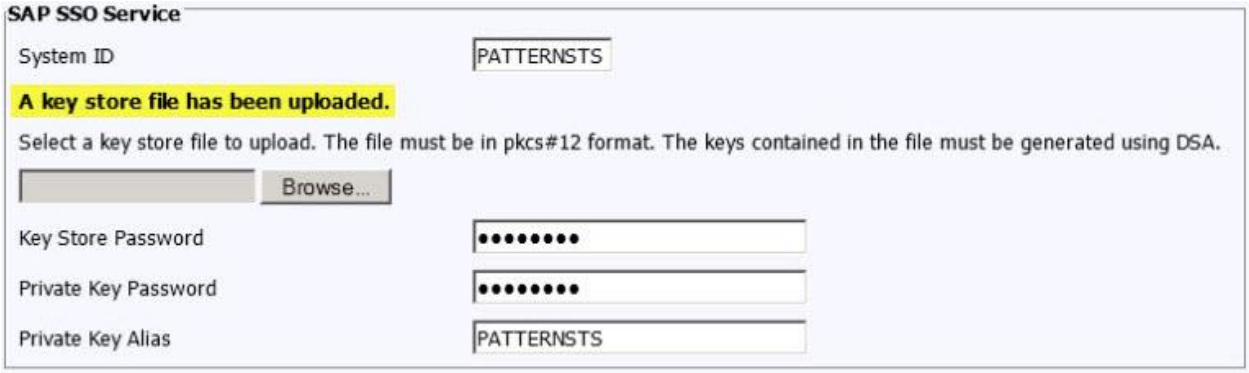


13. To save the entries, on the toolbar click the Save icon.

To configure the CMC to use the SAP SSO Service

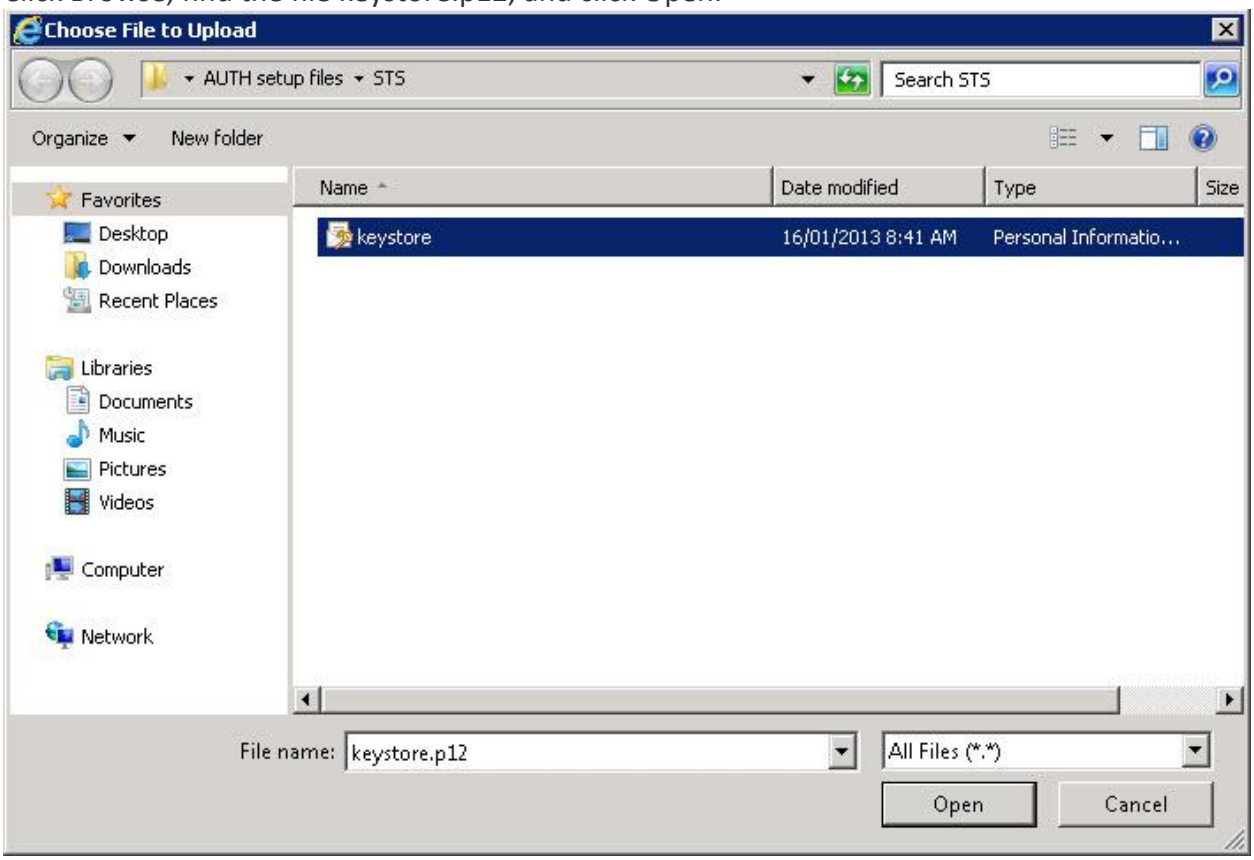
1. In the "Authentication" management area of the CMC, double-click **SAP**.
2. On the **Options** tab, select the default system.

3. In the **SAP SSO Service** area, in the **System ID** box type PATTERN.
   Warning: The System ID field is a single entry that identifies all nodes in the cluster. Multiple certificates should not be added to the BW system. Please refer to SAP Note 1695870 for further details.
4. In the Key Store Password box, type pattern123.
5. In the Private Key Password box, type pattern123.
6. In the *Private Key Alias*box, type PATTERNSTS.

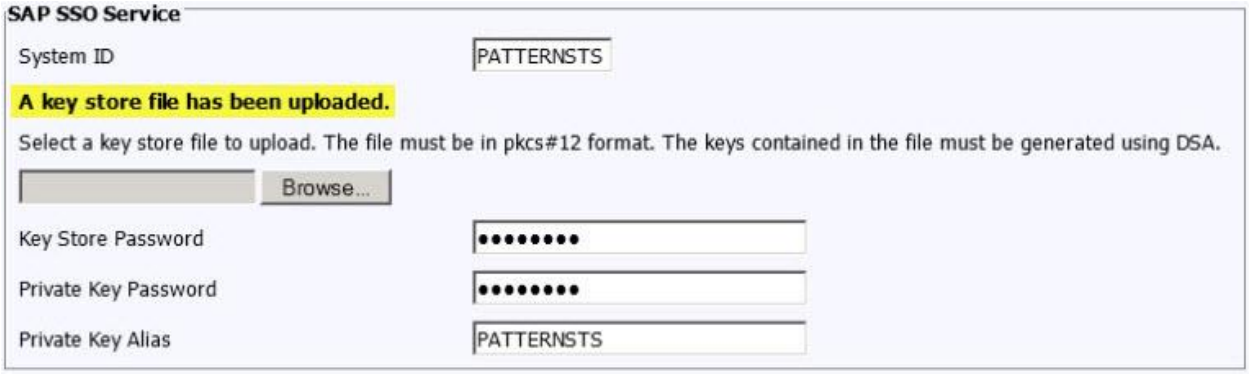


Note that the system indicates the following: "No key store file has been uploaded".

7. Click Browse, find the file keystore.p12, and click Open.



8. Click **Update** to commit the settings.
   Note that the system indicates the following: "A key store file has been uploaded".



9. Restart the SIA.

Setting up the Windows Active Directory (AD) server

Workflow and additional information

- Verify Active Directory installation.
  Check that Active Directory is installed on the machine. If Active Directory is not installed on the machine: install Active Directory as a new forest.
- Configure the Active Directory Domain Services.
- Add new users and groups to Windows AD.
  - Create a user account.
  - Create a group account.

When you create the group, you will need to set the "Group scope" and "Group type" options.
For more information about the "Group scope" option, see the "Understanding group scope" section in Understanding Group Accounts.
For more information about the "Group type" option, see the "Understanding group types" section in Understanding Group Accounts.

To verify Active Directory installation

Verify if the Active Directory Server is installed on Windows 2008.

Warning: Microsoft Active Directory (AD) requires DNS to resolve AD resources. Promoting a Windows 2003 server to AD Domain Controller (DC) installs and configures the DNS if one does not already exist.

1. Go to **Network Properties** and view the status of the Local Area Connection.

2. Click **Properties**, then **TCP/IPv6**, and then **Properties** again.
3. Ensure that the preferred DNS server is set to the correct DNS server IP.

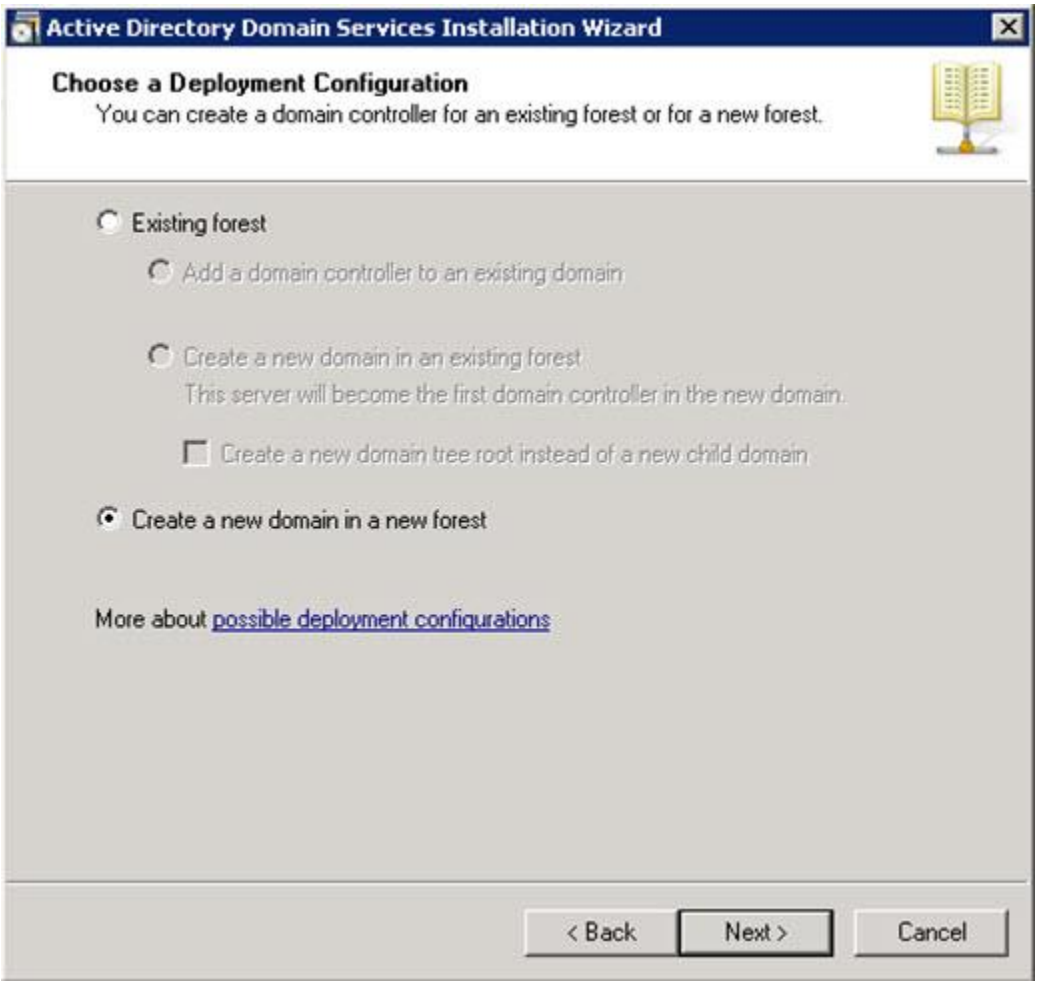
```
Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . : dhcp.pgdev.sap.corp
   IPv4 Address. . . . . . . . . . . : 10.165.30.78
   Subnet Mask . . . . . . . . . . . : 255.255.252.0
   Default Gateway . . . . . . . . . : 10.165.28.1
```

4. If the Windows 2008 server already has the Active Directory installed, go directly to the "To configure basic groups and users in the Active Directory server" section. Otherwise, you must perform the steps below prior to configuring the Active Directory Server.

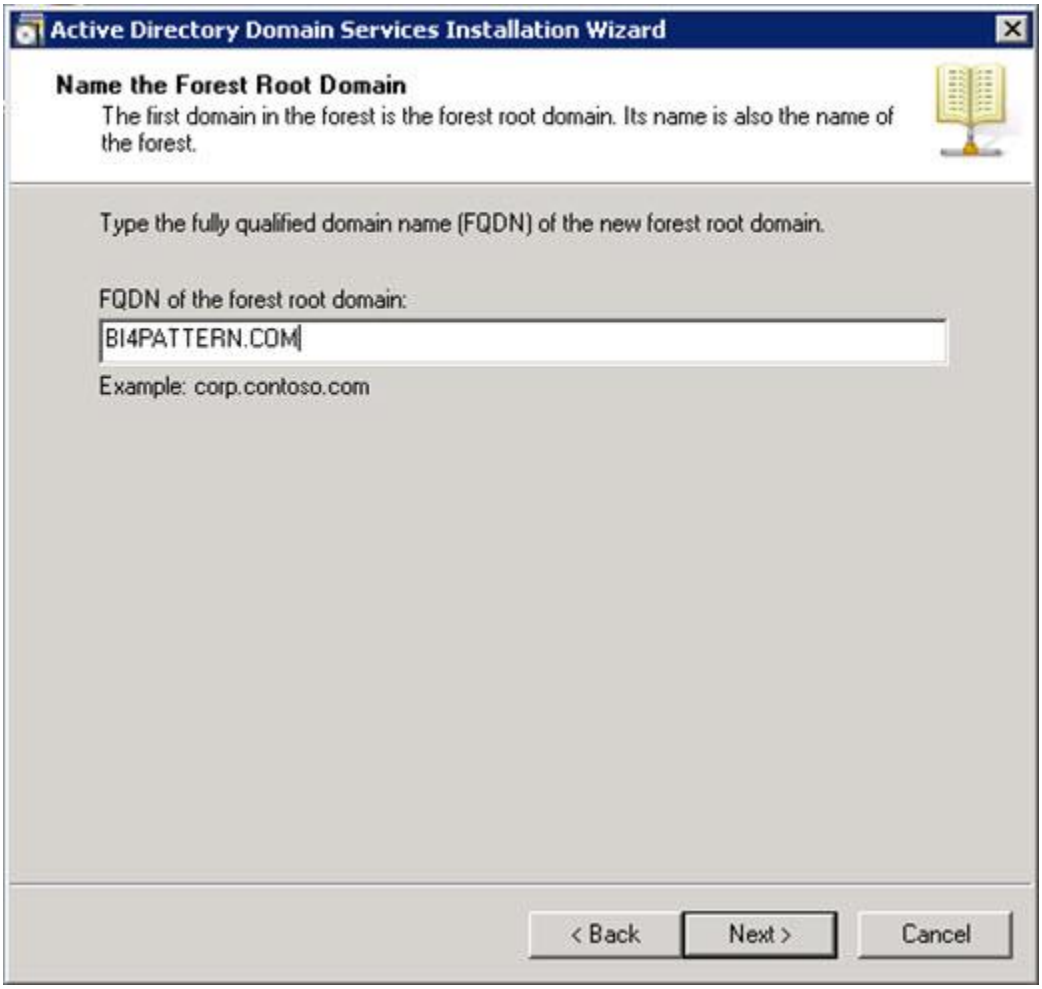
To install Active Directory as a new forest

If Active Directory is not installed on the machine, install and configure the Active Directory Domain Services.

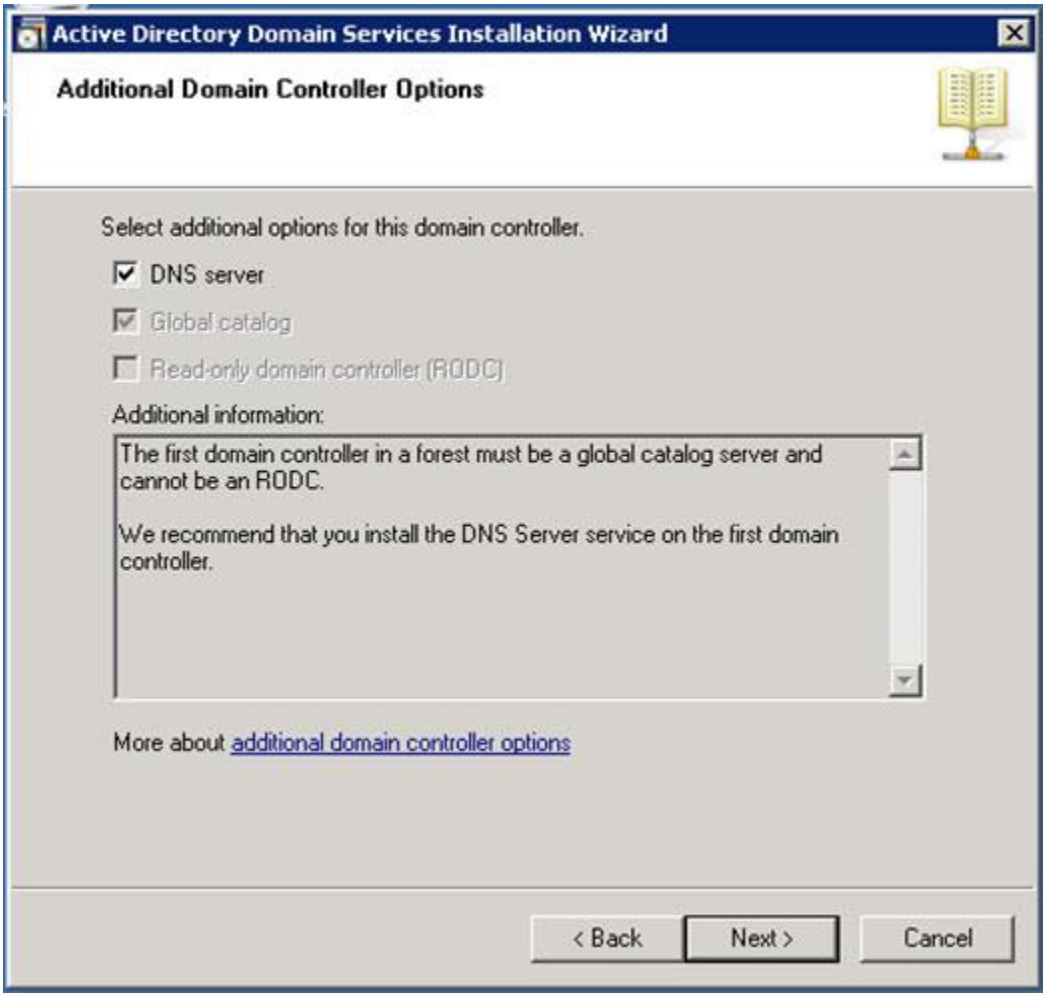
1. Run the Active Directory Domain Services Installation Wizard by typing DCPROMO.EXE from the run line.
   The "Active Directory Domain Services Installation Wizard" opens.
2. Click **Next** twice.
3. On the "Choose a Deployment Configuration" page, ensure **Create a new domain in a new forest** is selected.
   The configuration setting shown here are necessary to create a new forest and domain.



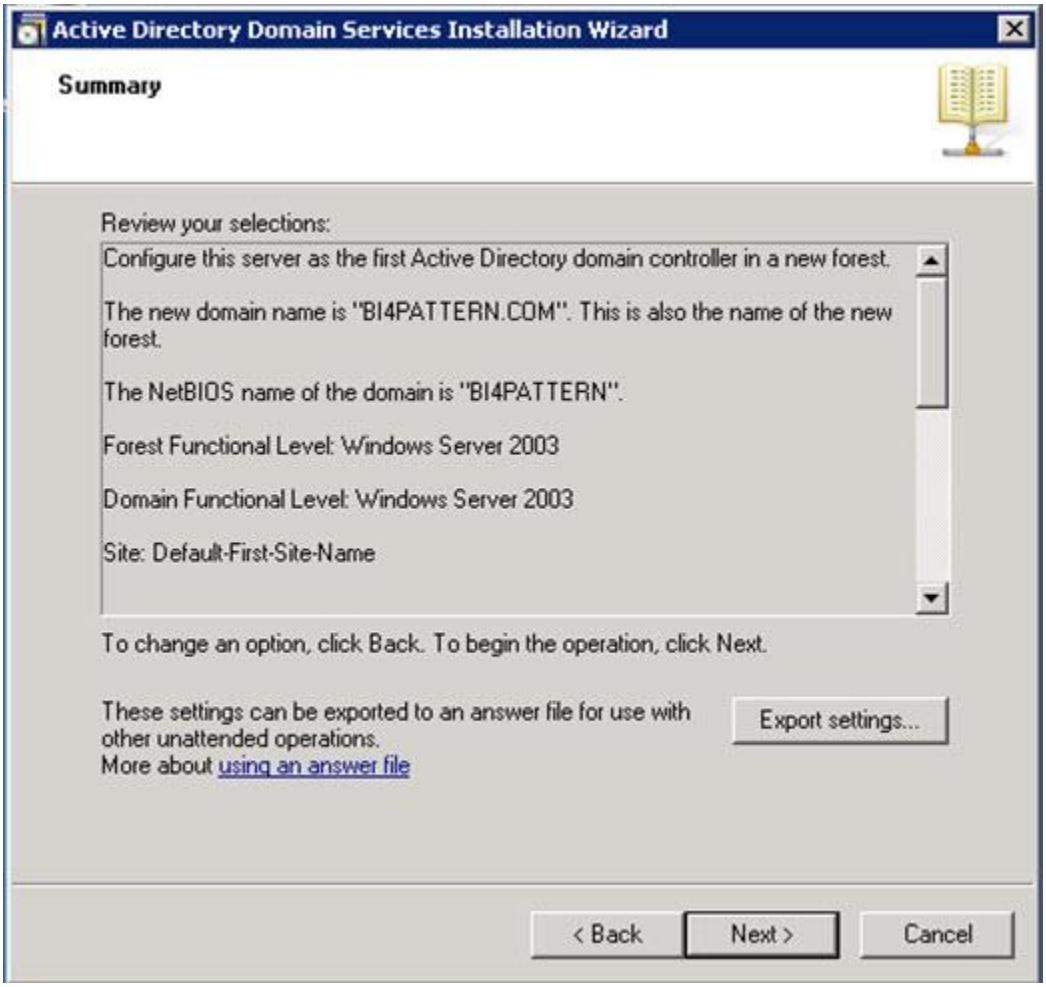
4. Click Next.
5. In the FQDN of the forest root domain box, type BI4PATTERN.COM., and click Next.



6. Type the name used for your Domain NetBIOS name, and click Next.
7. Select the Forest functional level, and click Next.
8. Select the Domain functional level, and click Next.
9. On the "Additonal Domain Controller Options" page, select the options to be installed on the domain controller.
   In this example, DNS server is selected.

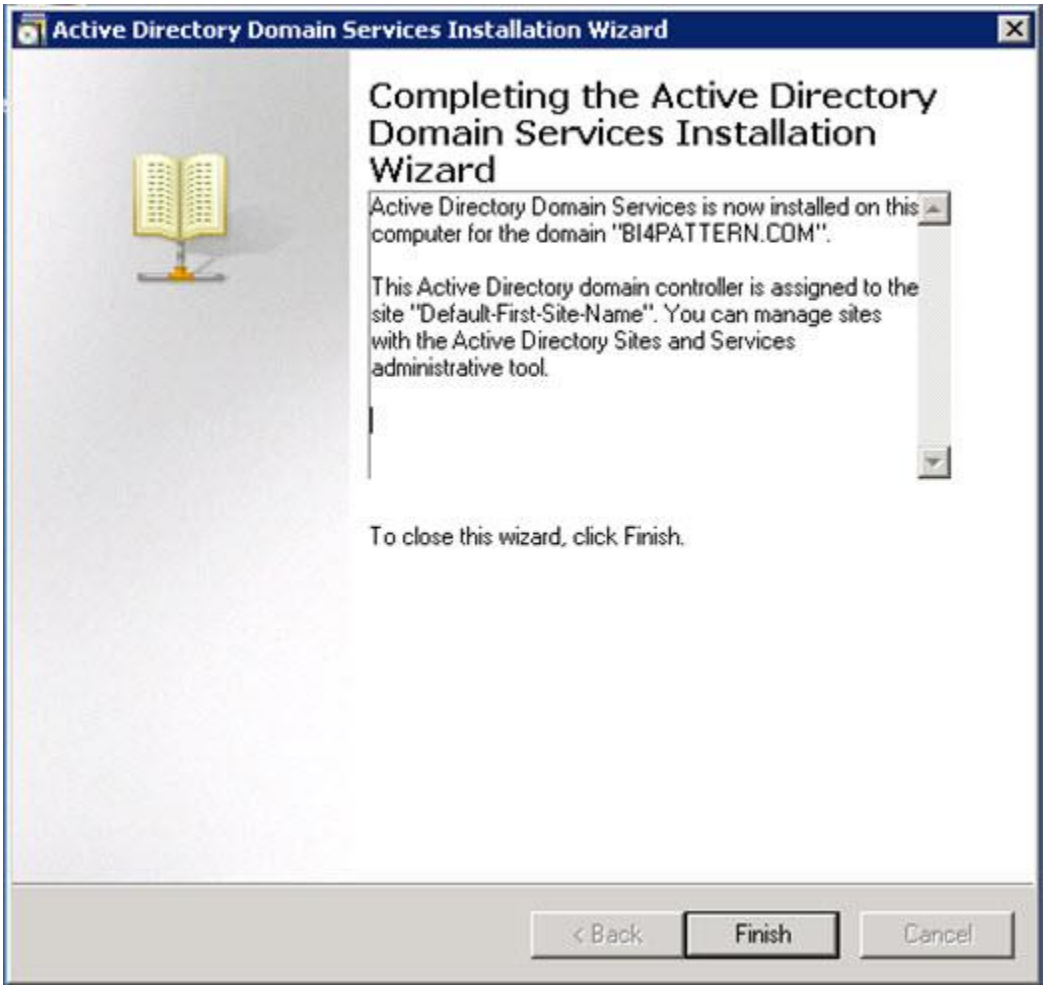


10. Proceed through the pages, accepting the default settings, until you reach the "Restore Mode Administrator Password" page.
11. Type a password, and click **Next**.
12. Verify that all the information is correct.



13. To set up the domain controller, click Next.
    This process may take a few minutes to complete.

14. Click **Finish** to close the wizard.



15. Restart the machine.
16. After the machine has restarted, ensure you can connect using the host name (for example, SUBDOMAIN4\Administrator).

To add users and groups to Windows AD

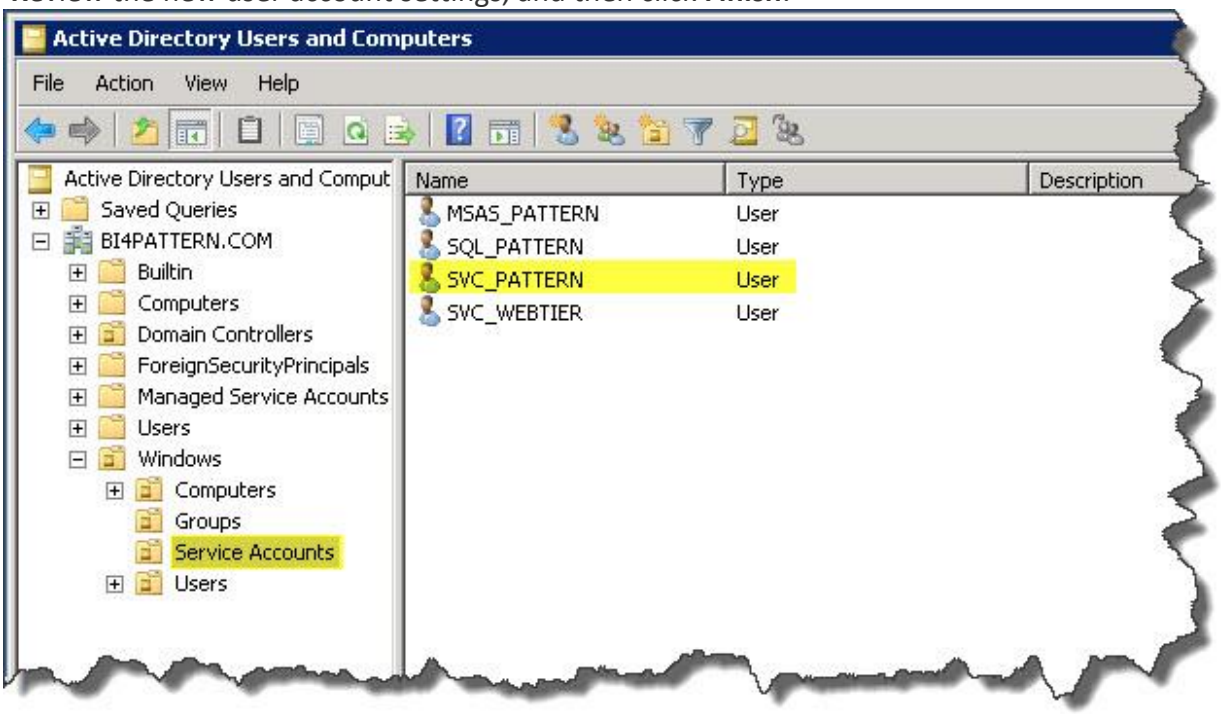
Step 1: To create a user account

This procedure is used to create a new domain user account in the "Active Directory Users and Computers" MMC.

Note: Membership in **Domain Admins**, or equivalent, is the minimum requirement needed to perform this procedure.

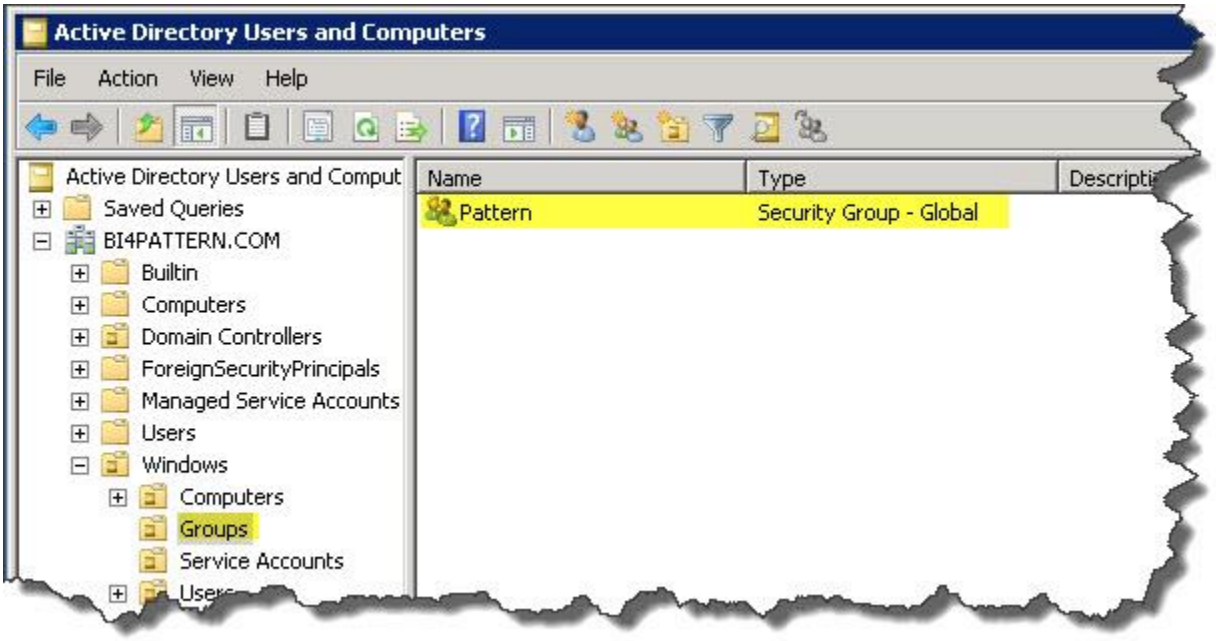
1. Click **Start** > **Administrative Tools** > **Active Directory Users and Computers**.
   The "Active Directory Users and Computers" MMC opens.

2. If it is not already selected, click the node for your domain. For example, in our example the domain is DC=BI4PATTERN,DC=COM; in that case you would click **BI4PATTERN.COM.**
3. In the "Details" pane, right-click the folder where you want to add a user account, click **New** and select **User**.
4. In the **First name** box, type the user's first name.
5. In the **Initials** box, type the user's initials.
6. In the **Last name** box, type the user's last name.
7. In the **Full name** box, modify the name to add initials or reverse the order of the first and last names as needed.
8. In the **User logon name** box, type the user logon name, and then click **Next**.
9. Type the user's password, select the appropriate password options, and then click **Next**.
10. **R**eview the new user account settings, and then click **Finish**.

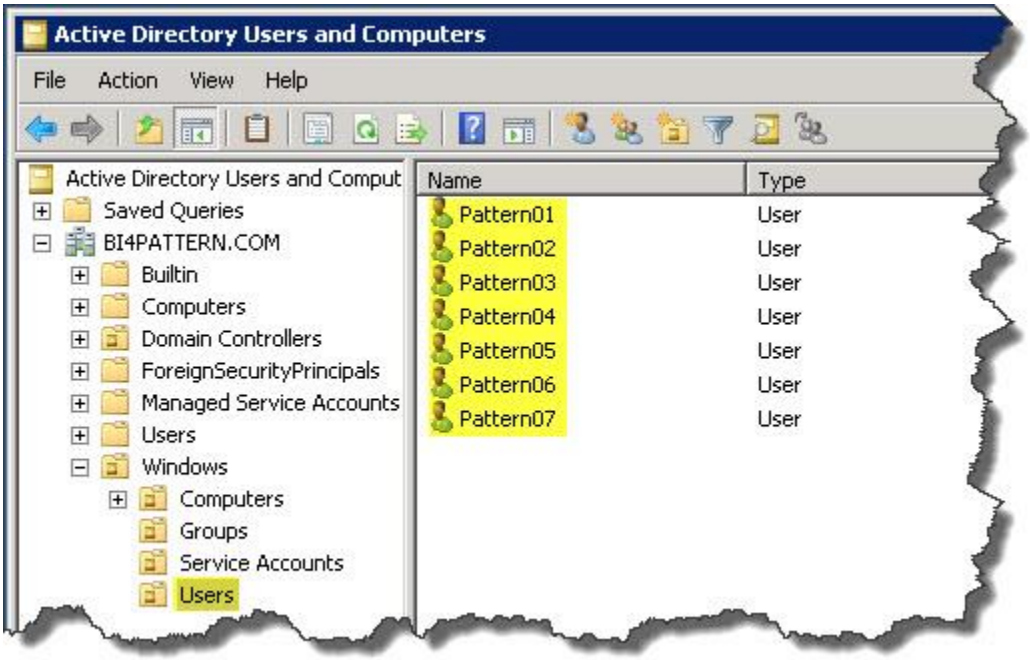


Step 2: To create a new group account

1. To open the "Active Directory Users and Computers" MMC, click **Start** > **Control Panel**, double-click **Administrative Tools**, and then double-click **Active Directory Users and Computers**.
2. Right-click the folder where you want to create a new group, click **New** and select **Group**.
3. Type the name of the new group.
   By default, the name that you enter is also entered as the pre-Windows 2000 name of the new group.
4. To create the group, click **OK**.



5. In Group scope, click one of the available options.
6. In Group type, click one of the available options.
   For this pattern, the following new Windows AD Users have been added for use with SAP BusinessObjects authentication:
   - User: `Pattern01` Password: `Pattern123`
   - User: `Pattern02` Password: `Pattern123`
   - User: `Pattern03` Password: `Pattern123`
   - User: `Pattern04` Password: `Pattern123`
   - User: `Pattern05` Password: `Pattern123`
   - User: `Pattern06` Password: `Pattern123`
   - User: `Pattern07` Password: `Pattern123`



Setting up the Windows AD plug-in

About the Windows AD security plug-in

Note: This page shows how to set up the windows AD plug-in for use with the CMC. For information about setting Java authentication, see Setting up Manual Java Authentication. For information about setting up SSO using Vintella, see Setting up Single Sign On using Vintela.

The Windows AD security plug-in lets you map user accounts and groups from the Windows AD domain to the BI platform. The plug-in enables the system to verify all login requests that specify Windows AD authentication. Users are authenticated against the Windows AD domain and have their membership in a mapped Windows AD group verified, before they are granted an active BI platform session by the CMS. User lists and group memberships are dynamically maintained by the system.

To simplify administration, the BI platform supports Windows AD authentication for user and group accounts. Before users can use their Windows AD user name and password to log in to the system, their Windows AD account must be mapped to the BI platform. When mapping a Windows AD account, you can choose to create a new account or link to an existing BI account.

Using Windows AD authentication

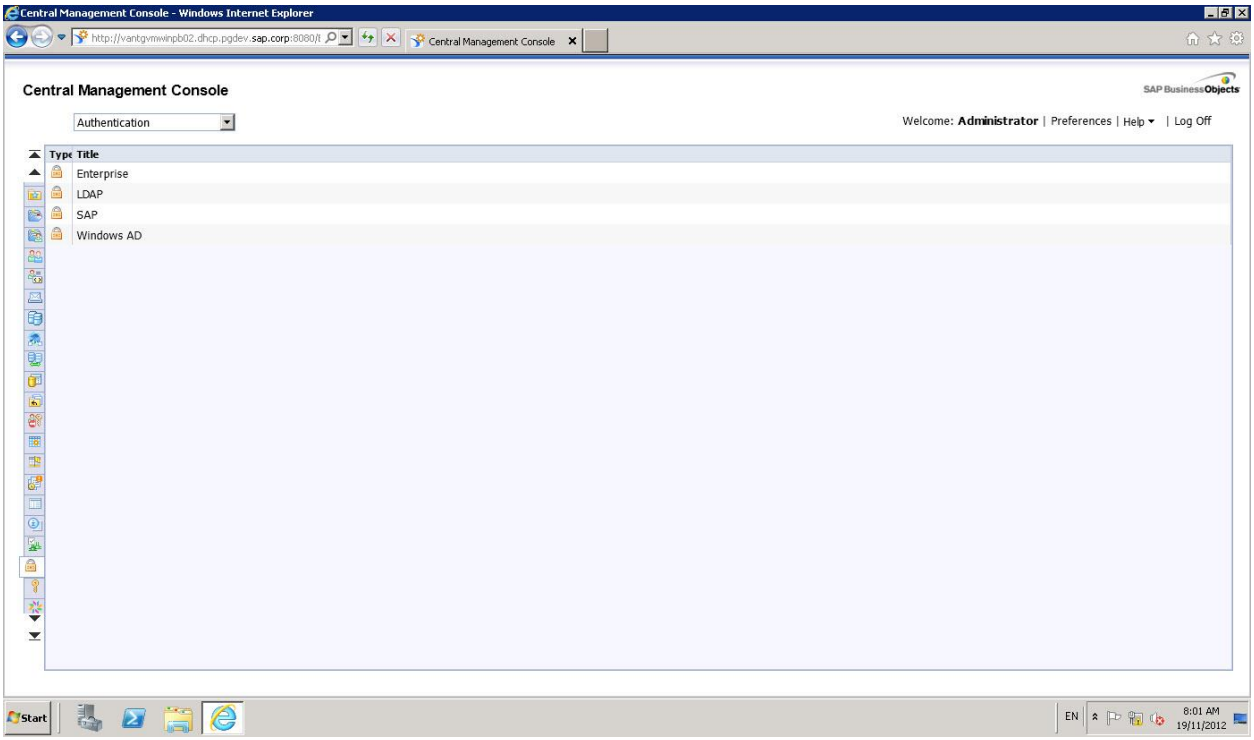
When BI platform is installed, the Windows AD authentication plug-in is installed automatically, but by default it is not enabled. To use Windows AD authentication, you must ensure that you have your respective Windows AD domain set up, as shown here.

Prerequisites

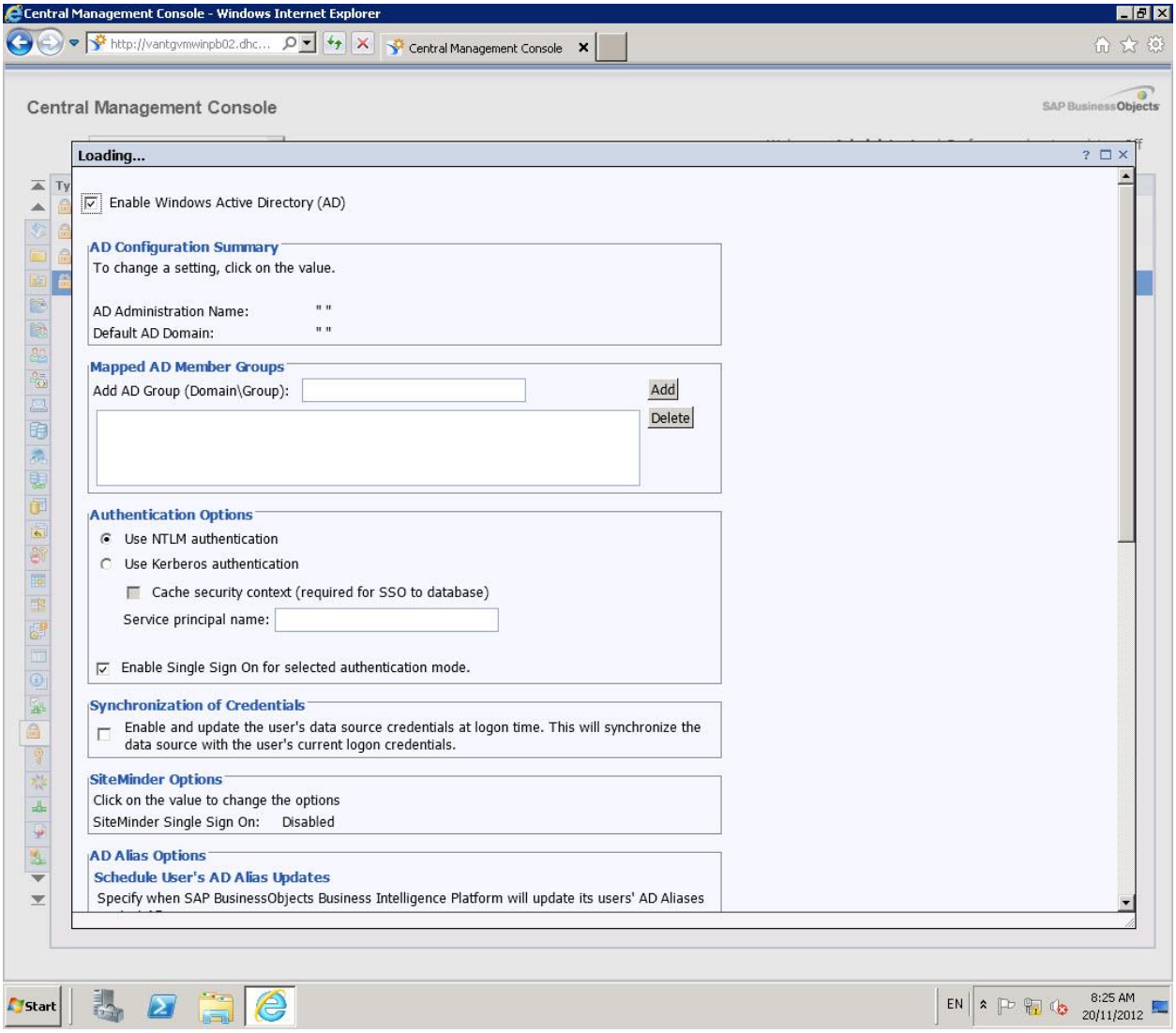
Note: You will need to ensure the following before beginning with the configuration of the Windows AD plug-in.

- The machine running the CMS has been added to the Windows AD Domain in which you wish to connect to.
- A service Account has been created in Windows AD which will be used for AD Authentication

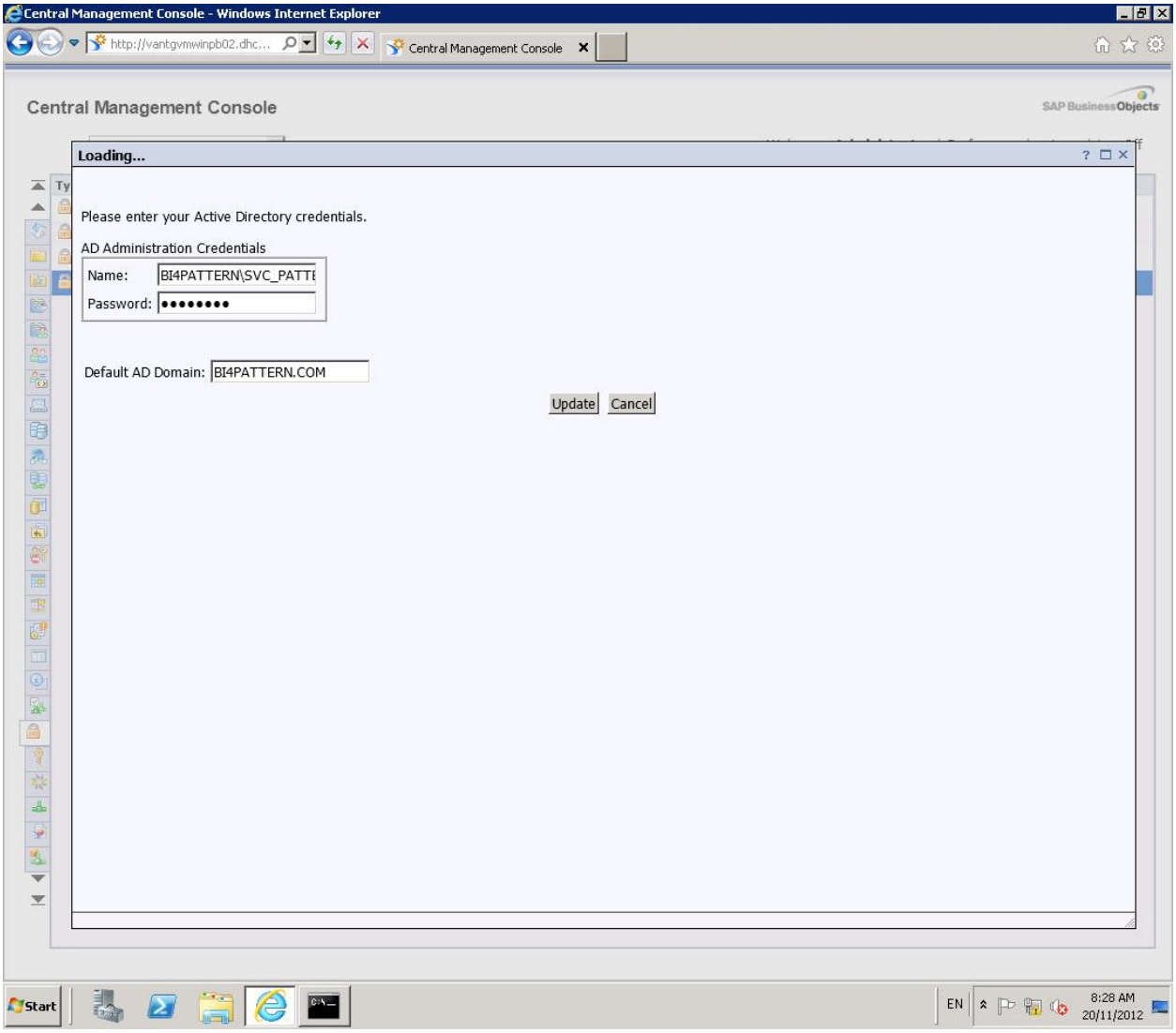
1. Open the CMC, and in the "Authentication management" area, double-click **Windows AD**.



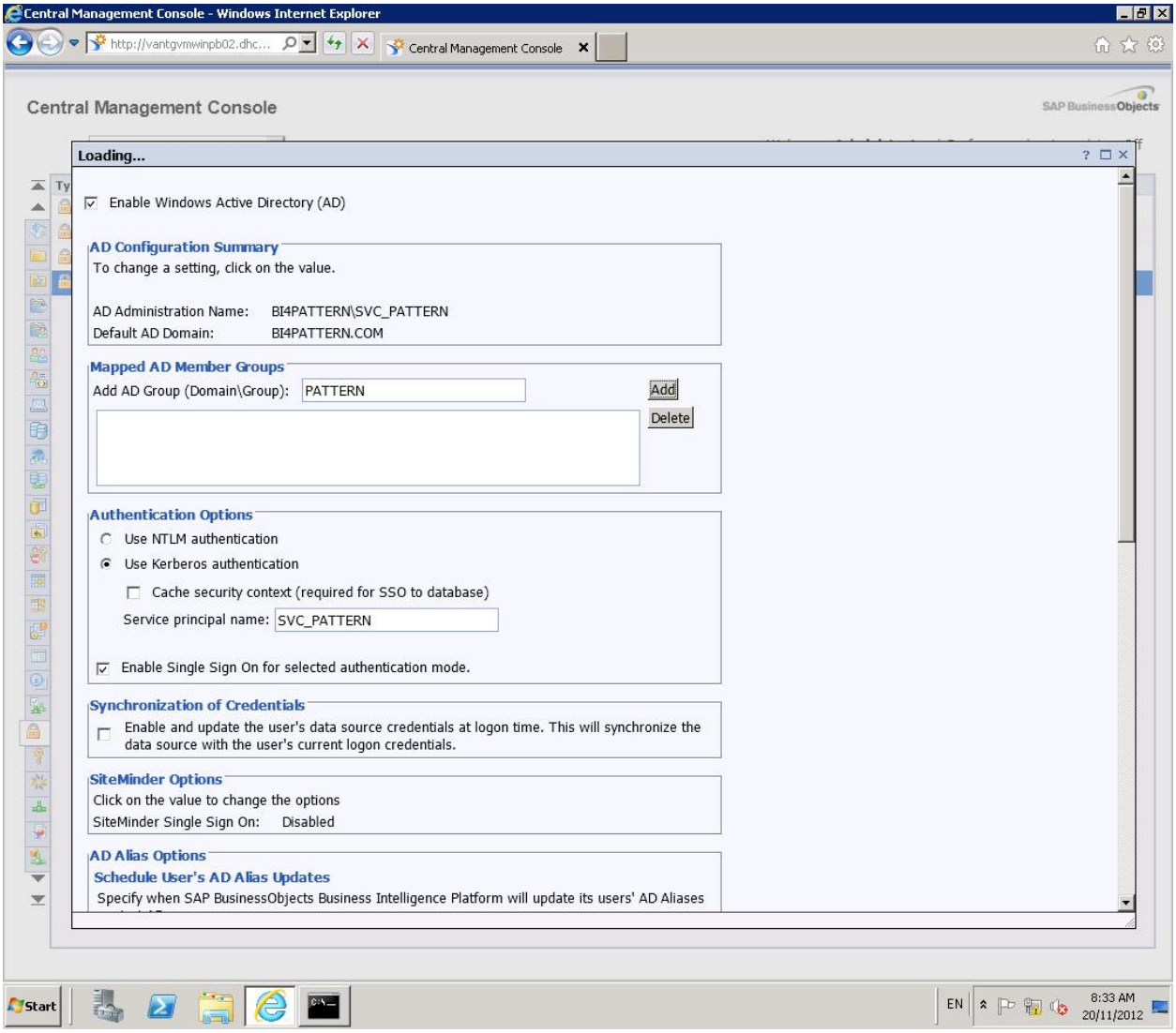
2. To configure the Windows AD plug-in, click the quotes next to the **AD Administration Name** box.



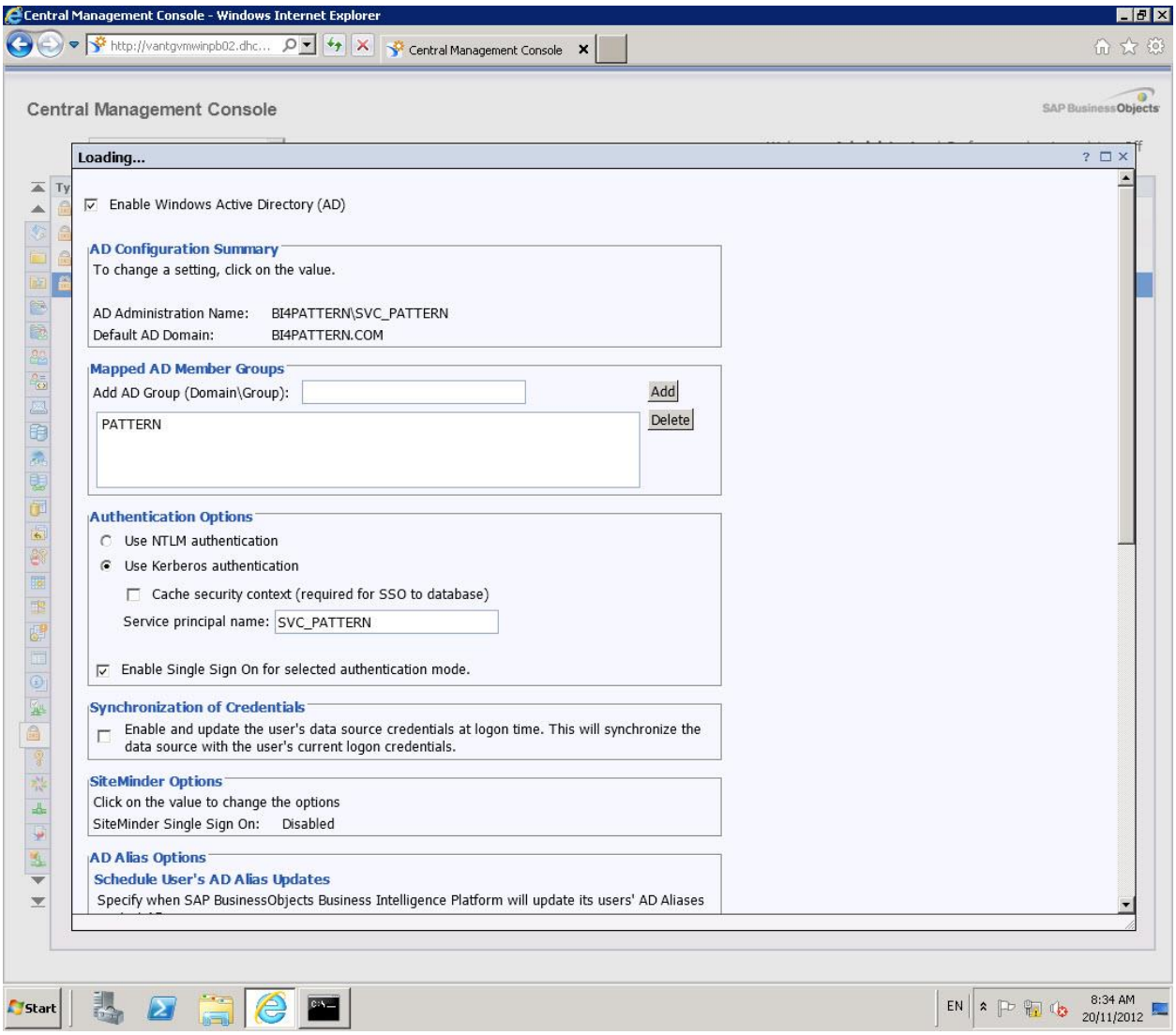
3. In the **Name** box and **Password** box, type the credentials of the account that will be responsible for connecting the Business Intelligence Platform to the Windows AD domain.



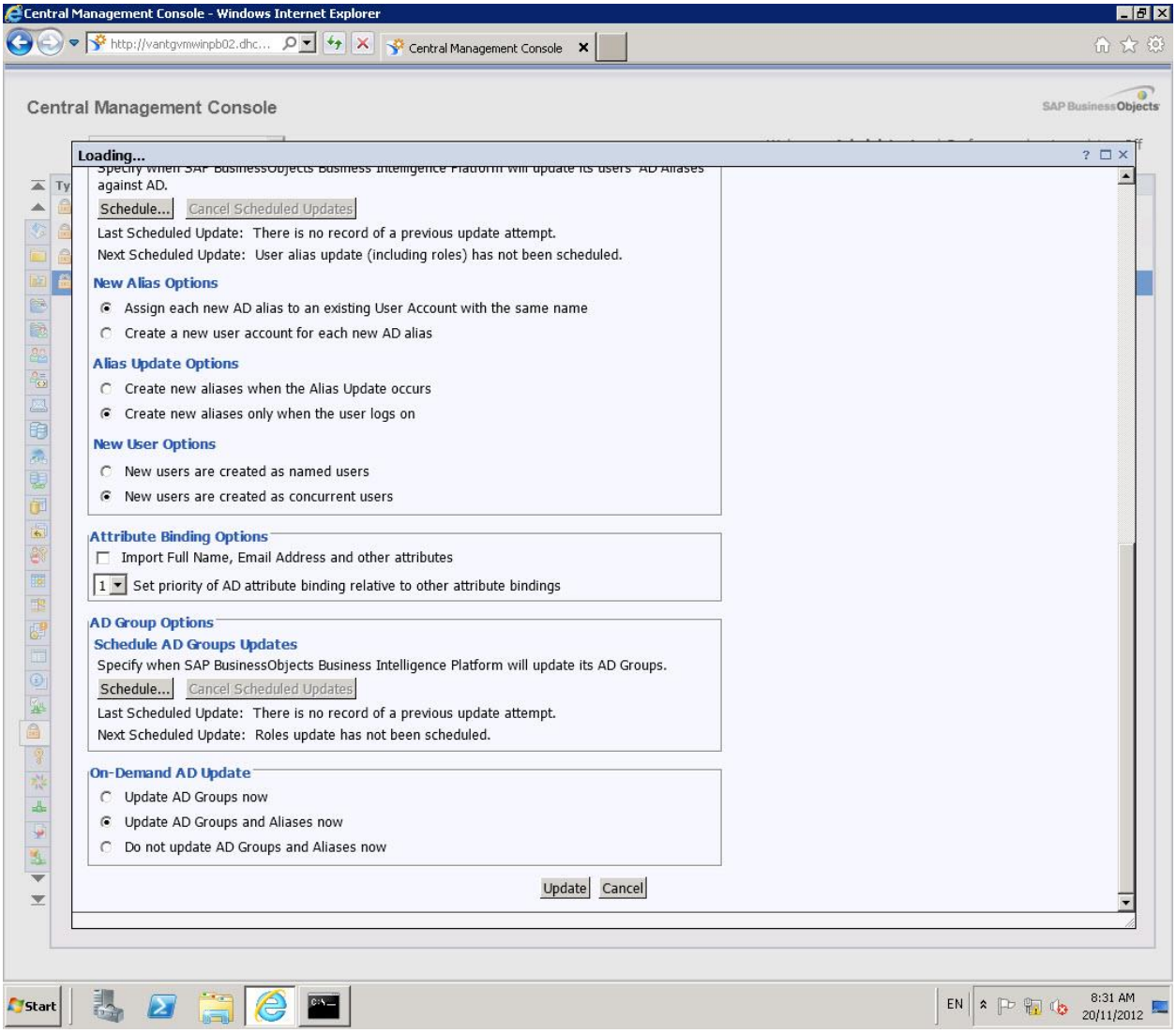
4. In the **Default AD Domain**, type BI4PATTERN.COM, and click **Update**.
5. In the **Add AD Group (Domain\Group)** box, type the name of the group located in Windows AD that you want to map to the BI Platform. (PATTERN in this example)



6. To commit the group name, click **Add**.



7. To verify that the group has been added, click **Update**.



Kerberos

Kerberos is a network authentication protocol developed at MIT. Its main purpose is to allow applications to authenticate each other. In addition, it provides confidentiality and integrity for data transmitted between applications.

How Kerberos Works

A Kerberos domain or *realm* consists of several entities who cooperate to communicate securely. These are:

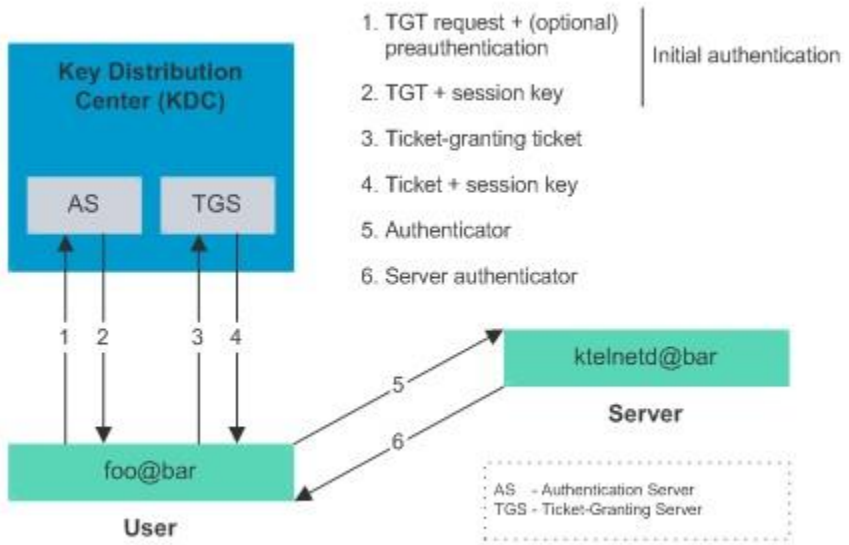
1. *Users* - principals who wish to access services.

2. *Servers* - principals who supply services to users. Note a server may also be a user of another service.
3. *The Key Distribution Center (KDC)* - The KDC is responsible for coordinating access to services by users (by providing the *Ticket Granting Service (TGS)*), and for performing the initial authentication (by providing the *Authentication Service (AS)*) (See below). The KDC is the controller of all secure interactions, and as such is a *trusted* entity.
   A *principal* authenticates itself in Kerberos by using a principal name of the form principal-name@realm and a password. This is typically used to send an encrypted message to the *Authentication Service (AS)*, which can then authenticate the principal and send back a session key and *Ticket Granting Ticket (TGT)*. The TGT is like a certificate of identity which allows the principal to gain later access to one or more services. Once the user has supplied their password and obtained the TGT from the AS, authentication to any other service can happen automatically without the user having to resupply their password. For this reason, Kerberos is sometimes called a *Single Sign-On (SSO)* service.

   For more information about using Kerberos with SSO, see Kerberos and SSO.

   A *ticket* is a credential that enables a principal to gain access to a service. A principal obtains tickets from the *Ticket Granting Service (TGS)*using the TGT obtained from the AS as described above. The ticket is used to create an *authenticator*, which is then sent to the service being requested to authenticate the user. The authenticator is then used to establish a session key for secure communication. Optionally, the user can also request to authenticate the server. If this happens, the server uses information in the user's authenticator to send back a *server authenticator*, which the user can use to verify the server's authenticity.

Conceptual Overview of Kerberos



For more information on the Kerberos protocol, including the Kerberos V RFCs, see Kerberos Papers and Documentation.

Where Kerberos is used

Kerberos is used in Windows to provide authentication services for Windows domains. Kerberos authentication is also integrated with some UNIX operating system logins (e.g. Solaris), and can be used for authentication in LDAP. Kerberos forms the basis of security in the Distributed Computing Environment (DCE), and can be used to implement a CORBA security service.

Setting up Manual Java Authentication

Prerequisites

Warning: Before you configure manual Java authentication, you must follow the steps for Setting up the Windows AD plugin.

Workflow and additional information

- Configure the Service Account for use with the Active Directory (AD) plug-in.
    a. Create Service Principal Names (SPNs) for the Service Account.
    b. Set delegation for the Service Account.
- Configure the BI platform for use with the Service Account.
    a. Add the SPN to the CMC.
    b. Set the Server Intelligence Agent (SIA) to run as the service account.
    c. Verify that the service account and Windows AD login accounts are working.
- Configure Manual AD authentication to the Java Application Servers.
    a. Create the bsclogin.conf file.
    b. Create the krb5.ini file.
- Configure the BI Launch Pad for manual AD login.
  Set the **Authentication** menu in BI Launch Pad to be visible.
- Set the Application Server to the bscLogin.conf and krb5.ini files.

Warning: For more detailed information about this topic, see the following SAP Knowledge Base Article: https://apps.support.sap.com/sap/support/knowledge/preview/en/1631734

To configure the Service Account for use with the AD plug-in

Before setting up Manual Java Authentication, a few steps must be completed in Windows AD to prepare for use with Kerberos.

Step 1: To create Service Principal Names (SPNs) for the Service Account

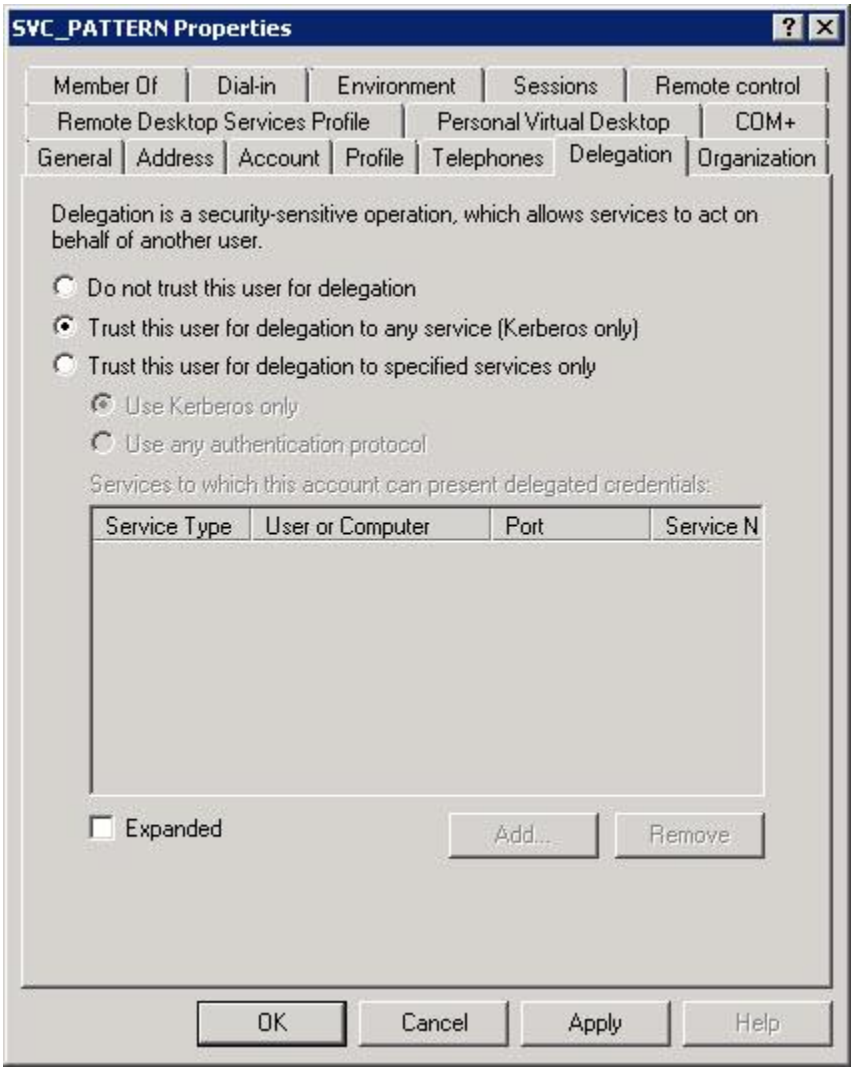
1. Open the CMC, and set a general SPN that you will enter into the SPN field of the Active Directory page of the CMC:
   setspn --a BICMS/SVC_PATTERN.BI4PATTERN.COM SVC_PATTERN
2. Set the following SPN's for SSO (If needed):
   setspn --a HTTP/vantgvmwinpb02 SVC_PATTERN
   setspn --a HTTP/vantgvmwinpb02.BI4PATTERN.COM SVC_PATTERN
   setspn --a HTTP/vantgvmwinpb02.dhcp.pgdev.sap.corp SVC_PATTERN
   setspn --a HTTP/vantgvmwinpb03 SVC_PATTERN
   setspn --a HTTP/vantgvmwinpb03. BI4PATTERN.COM SVC_PATTERN
   setspn --a HTTP/vantgvmwinpb03.dhcp.pgdev.sap.corp SVC_PATTERN

Once completed running, the **SETSPN --l SVC_PATTERN** command will display the following:

```
C:\Users\svc_pattern>setspn -l svc_pattern
Registered ServicePrincipalNames for CN=SVC_PATTERN,OU=Service Accounts,OU=Windows,DC=BI4PATTERN,DC=COM:
        BICMS/SVC_PATTERN.BI4PATTERN.COM
        HTTP/vantgvmwinpb03.dhcp.pgdev.sap.corp
        HTTP/vantgvmwinpb02.dhcp.pgdev.sap.corp
        HTTP/vantgvmwinpb03
        HTTP/vantgvmwinpb02
        HTTP/vantgvmwinpb03.BI4PATTERN.COM
        HTTP/vantgvmwinpb02.BI4PATTERN.COM
```

Step 2: To set delegation for the Service Account

1. Right-click the SVC_PATTERN service account, and click Properties.
2. On the Delegation tab, click Trust this user for delegation to any service (Kerberos only).



To configure BI platform for use with the Service Account

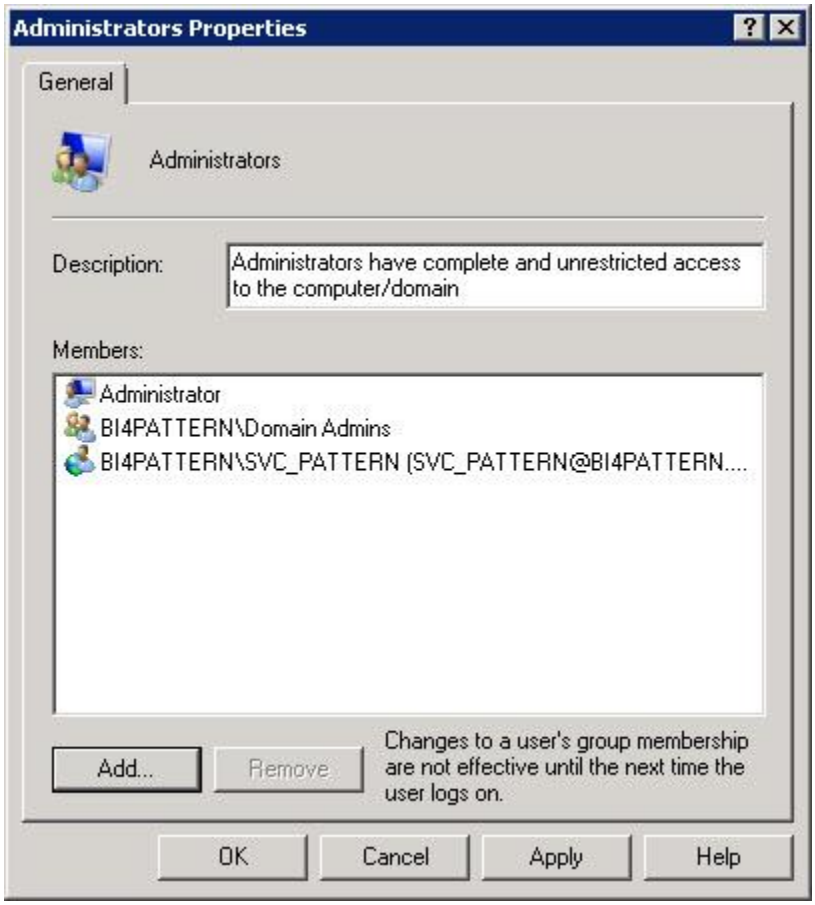
Step 1: To add the SPN to the CMC

1. In the CMC, under **Authentication**, go to the Windows AD plug-in section, and configure the Authentication options as shown here:

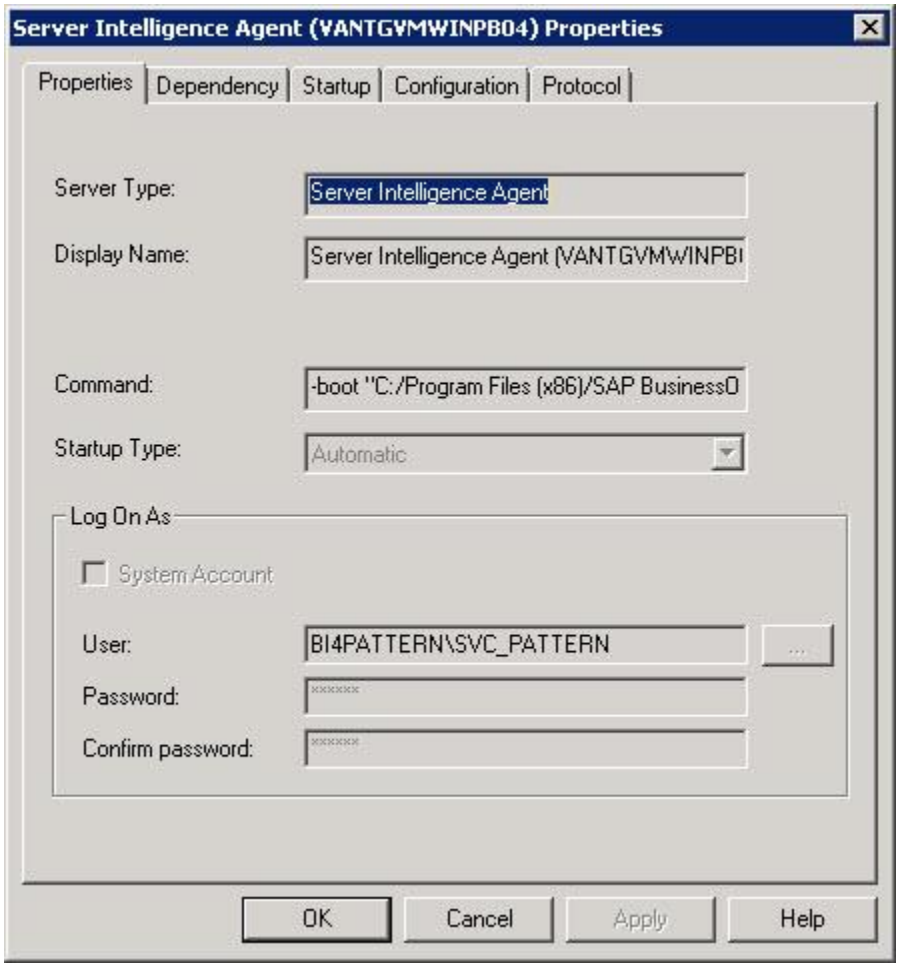
2. To commit the changes, click Update.

Step 2: To set the Server Intelligence Agent (SIA) to run as the service account

1. Add the service account to the local administrators group on any server where the SIA will be running as the service account.



2. In the CMC, stop the SIA.
3. When the SIA is stopped, access the properties of the SIA and change the System Account credentials in **Log On As** area to the credentials for the Service Account.



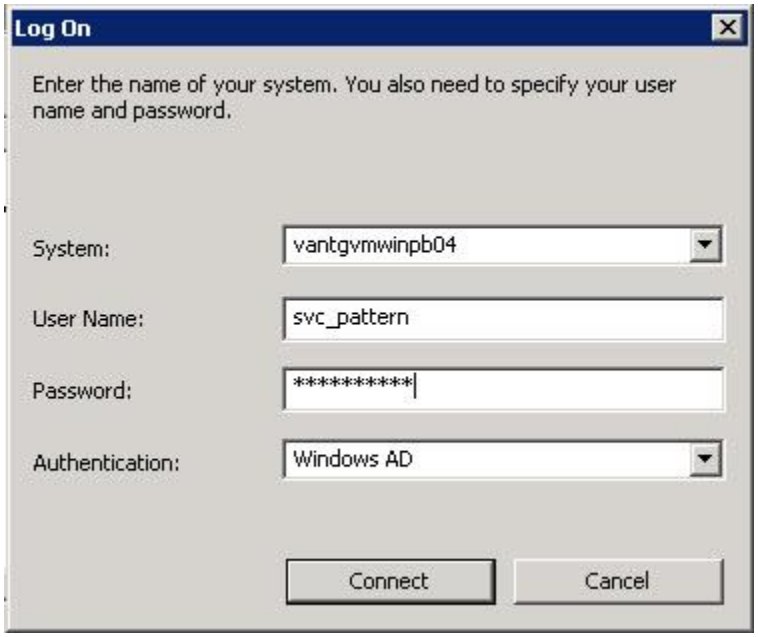
4. Click **Ok**, and start the SIA.

Step 3: To verify that the service account and Windows AD login account are working

Follow these steps to check if you can log in through the client tools. These next steps test an AD log in using the Central Configuration Manager's (CCM) Manage Servers tool.

1. Open the CCM, and click on the **Manage Servers** icon.
2. Ensure the name in the System field is correct, and in the Authentication drop-down list select **Windows AD**.
3. Log in with an AD user account that exists inside the CMC.

   AD users that do not reside in the default domain must log in to client tools as domain\username.



4. Check that no error message appears.

   A white screen with no services indicates issues with permissions, which are not a concern at this point. Provided no error message appears, the service account and Windows AD login account is working.

To configure Manual AD authentication to Java Application Servers

Two files must be created when using the Java SDK: bsclogin.conf and krb5.ini. You must create those files new, and place them in the C:\windows folder on any Windows Application Server. Java will seek that path by default on a windows server. Because Windows 2008 servers by default hide extension suffix for known extension types, be sure to not end either file with a .txt or other extension.

Step 1: To create the bsclogin.conf file

bsclogin.conf is used to load the Java login module and trace login requests.

1. On each of the web Application Servers, go to the C:\Windows folder, create a new text file, and save it as bsclogin.conf.
2. Add the following lines to the file, and save it:

```
com.businessobjects.security.jgss.initiate {
com.sun.security.auth.module.Krb5LoginModule required debug=true;
};
```

Step 2: To create the krb5.ini file

krb5.ini is used to configure the KDC's (Kerberos Key Distribution Center, its domain controllers) that will be used for the java login requests.

1. On each of the web Application Servers, go to the C:\Windows folder, create a new text file, and save it as krb5.ini.
2. Add the following lines to the file, and save it:

Warning: If connecting to a Windows AD domain other than the one specified in this Pattern, the settings in this file will be different than shown here. The KBA at the start of this topic can be used for obtaining the correct information.

```
[libdefaults]
default_realm = BI4PATTERN.COM
dns_lookup_kdc = true
dns_lookup_realm = true
udp_preference_limit = 1
default_tgs_enctypes = rc4-hmac
default_tkt_enctypes = rc4-hmac
[realms]
BI4PATTERN.COM = {
kdc = vantgvmwinpb01.BI4PATTERN.COM
default_domain = BI4PATTERN.COM
}
```

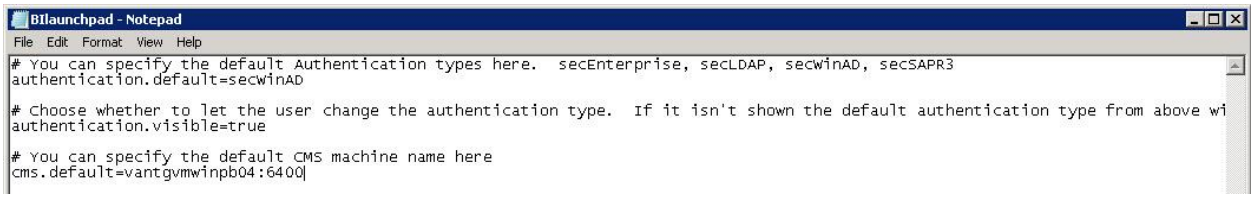
To configure the BI Launch Pad for manual AD login

The Authentication menu in the BI Launch Pad is needed for manual AD log ins; however, by default the menu is hidden. These steps show how to set the Authentication menu to be visible.

Note that .properties files are used instead of .xml files in Business Intelligence Release 4. The .properties files are stored in a custom folder that is safe from being overwritten during patch installations.

1. Go to C:\Program Files (x86)\SAP BusinessObjects\Tomcat6\webapps\BOE\WEB-INF\config\custom.

2. Create a text file named BIlaunchpad.properties, add the following lines to the file, and save it:
   authentication.visible=true
   authentication.default=secWinAD
   cms.default=vantgvmwinpb04:6400

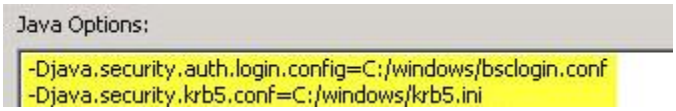


3. Restart Tomcat to ensure the Authentication menu in BI Launch Pad is visible.

To set the Application Server to the bscLogin.conf and krb5.ini files

To have AD users log in to BI Launch Pad and the CMC, you must ensure your application server has access to bscLogin.conf and krb5.ini.

1. Navigate to the Tomcat Configuration utility, and click the Java tab.
2. Add the following lines to the tomcat java options:
   Djava.security.auth.login.config=c:\windows\bsclogin.conf
   -Djava.security.krb5.conf=c:\windows\krb5.ini



3. Restart Tomcat to load the files into memory.

Setting up Single Sign On using Vintela

Prerequisites

Before you configure SSO Authentication, ensure you have followed the steps for Setting up the Windows AD plugin and Setting up Manual Java Authentication.

Workflow

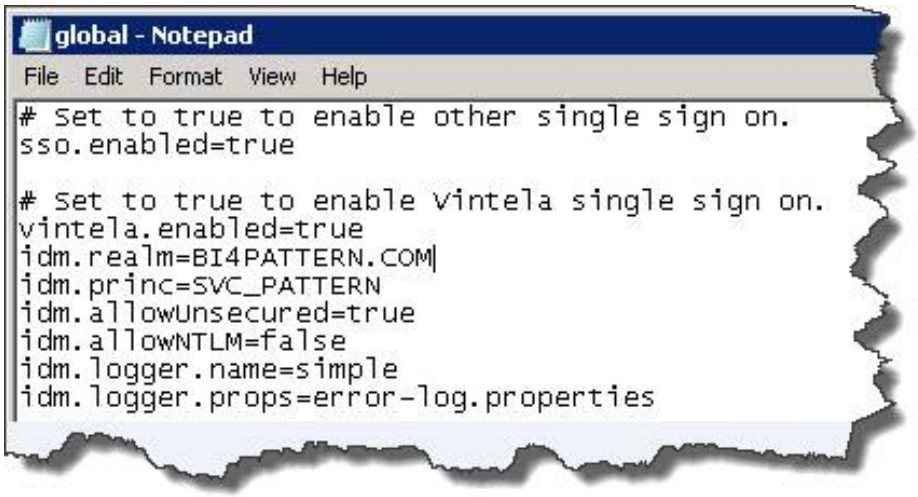
- Create a custom global.properties file.#Setting_up_Manual_Java_Authentication
  This file allows the Vintela filter to start.
- Add Java options.
  These allow Vintela to load properly.

To set up SSO using Vintella

Step 1: To create a custom global.properties file

1. Go to C:\Program Files (x86)\SAP BusinessObjects\Tomcat6\webapps\BOE\WEB-INF\config\custom.
2. Create a text file named global.properties, and add the following lines:
   Note:
   - Best practices suggest you enter the username with exact lowercase and capitals as seen used in AD.
   - Use only capital letters in your domain name.
   - Remove white spaces at the end of each line.
   - Be sure to give the file a .properties extension.

   sso.enabled=true
   siteminder.enabled=false
   vintela.enabled=true
   idm.realm=BI4PATTERN.COM
   idm.princ=SVC_PATTERN
   idm.allowUnsecured=true
   idm.allowNTLM=false
   idm.logger.name=simple
   idm.logger.props=error-log.properties



3. Save the file.

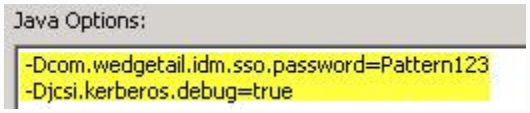
Step 2: To add Java options

1. Go to the Tomcat Configuration utility, and click the Java tab.
2. Add the following lines to the tomcat java options:

   Note:

   - `wedgetail.sso.password` is the password for your service account.
   - The `DJCSI.kerberos.debug` options will enable a startup trace of the vintela filter.

   -Dcom.wedgetail.idm.sso.password=password
   -Djcsi.kerberos.debug=true

3. Restart Tomcat to load the files into memory.

Adding SAP BusinessObjects Explorer

SAP BusinessObjects Explorer overview

SAP BusinessObjects Explorer (Explorer) is not included in the main BI platform installation and is instead an add-on component. When installing Explorer, the Service Pack for Explorer must match the Service Pack used across the BI platform 4.0 landscape. Therefore SAP BusinessObjects Explorer SP4 must be installed, as shown in this section.

The Explorer installation consists of four components:

- Explorer Servers
- Web Tier
- CMS Add-On
- Search Integration

Although it is possible to do a full installation of all four Explorer components to a single host, in this pattern the components are installed separately.

Explorer installation summary

Explorer has four services, and they are installed to a single host:

- Explorer Master Server
- Explorer Index Server
- Explorer Exploration Server
- Explorer Search Server

The Central Management Server (CMS) Add-On is installed to each of the two servers where the CMS is installed. The Web Tier portion is installed on each of the two dedicated web application servers.

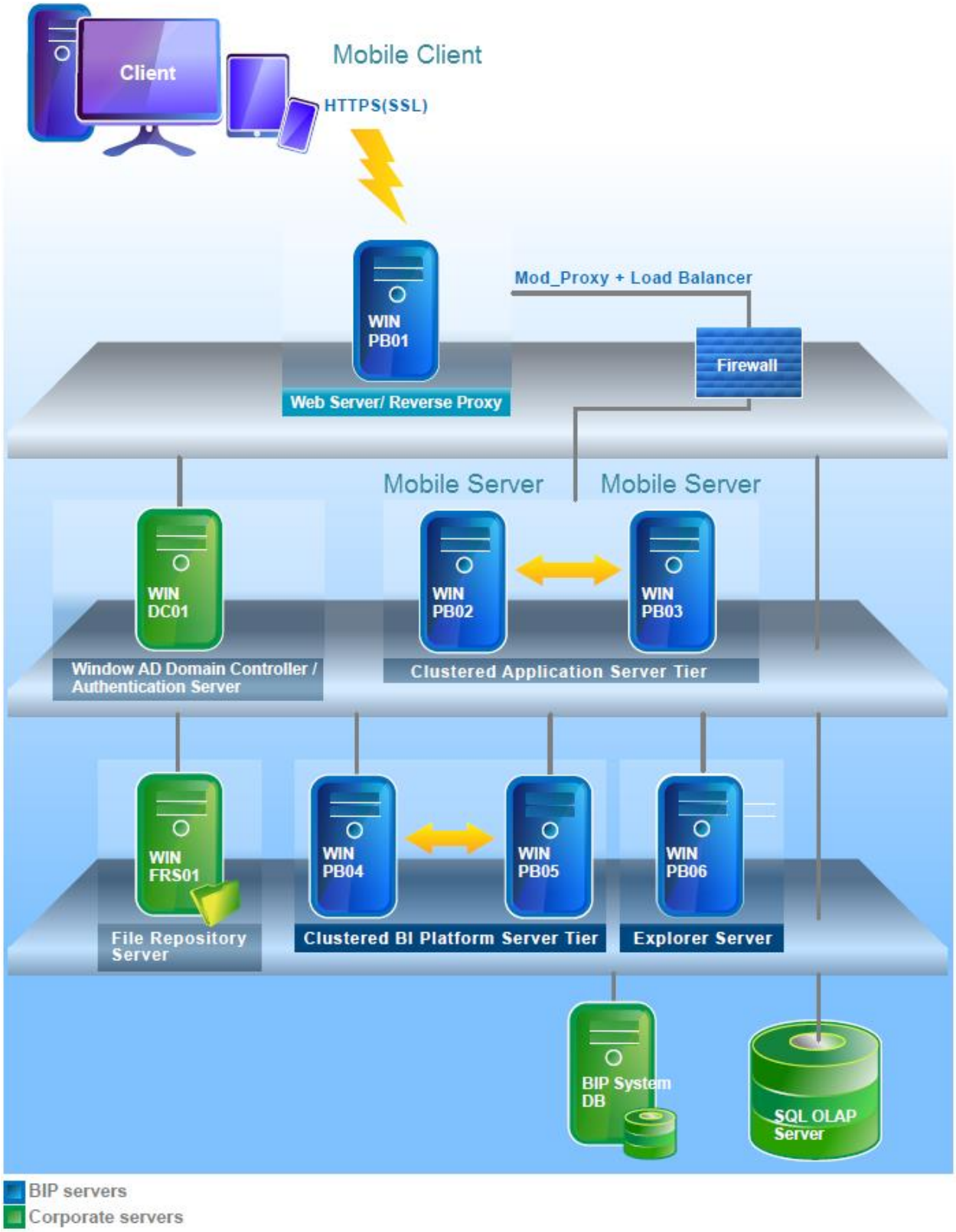
Install Type	Server Name
Explorer Servers	vantgvmwinpb06.dhcp.pgdev.sap.corp
CMS Add-On & Search	vantgvmwinpb04.dhcp.pgdev.sap.corp
	vantgvmwinpb05.dhcp.pgdev.sap.corp
Web Tier	vantgvmwinpb02.dhcp.pgdev.sap.corp
	vantgvmwinpb03.dhcp.pgdev.sap.corp

Setting up SAP BusinessObjects Mobile

Introduction

This pattern uses the following three SAP BusinessObjects Mobile components:

- SAP BusinessObjects Mobile client.
- SAP BusinessObjects Mobile server.
- SAP BusinessObjects Business Intelligence (BI) platform.


Client
Mobile Client
HTTPS(SSL)
WIN PB01
Web Server/ Reverse Proxy
Mod_Proxy + Load Balancer
Firewall
Mobile Server
Mobile Server
WIN DC01
Window AD Domain Controller / Authentication Server
WIN PB02
WIN PB03
Clustered Application Server Tier
WIN FRS01
File Repository Server
WIN PB04
WIN PB05
Clustered BI Platform Server Tier
WIN PB06
Explorer Server
BIP System DB
SQL OLAP Server
BIP servers
Corporate servers

Warning:

- The mobile components are part of the SAP BusinessObjects Business Intelligence platform installer.
- The following steps show how to install and deploy the SAP BusinessObjects Mobile solution on a distributed Web-tier solution.
- This pattern uses iOS as the Mobile client.

Prerequisites

To configure the system shown in the diagram, you will need these tools and configurations:

1. Access to BI Mobile and Explorer services.
2. Access to BI Mobile through Enterprise or Active Directory users.
3. Ability to load balance between Application Server Tier.
4. Ability to work through a Firewall.

Workflow and further information

1. Install the SAP Business Intelligence Mobile Server.
2. Because this pattern uses a Web-Tier installation, the Mobile Servers must be enabled. During the installation of the web-tier, you will select which features to install.
3. Install the Mobile Plug-in.
4. The Mobile Plug-in is needed by the CMS.
5. Configure Tomcat to enable the Mobile client.
6. You must add a category to enable Mobile to display reports.
7. Install the SAP BusinessObjects Mobile app (client).
8. This is done through the Apple App Store.

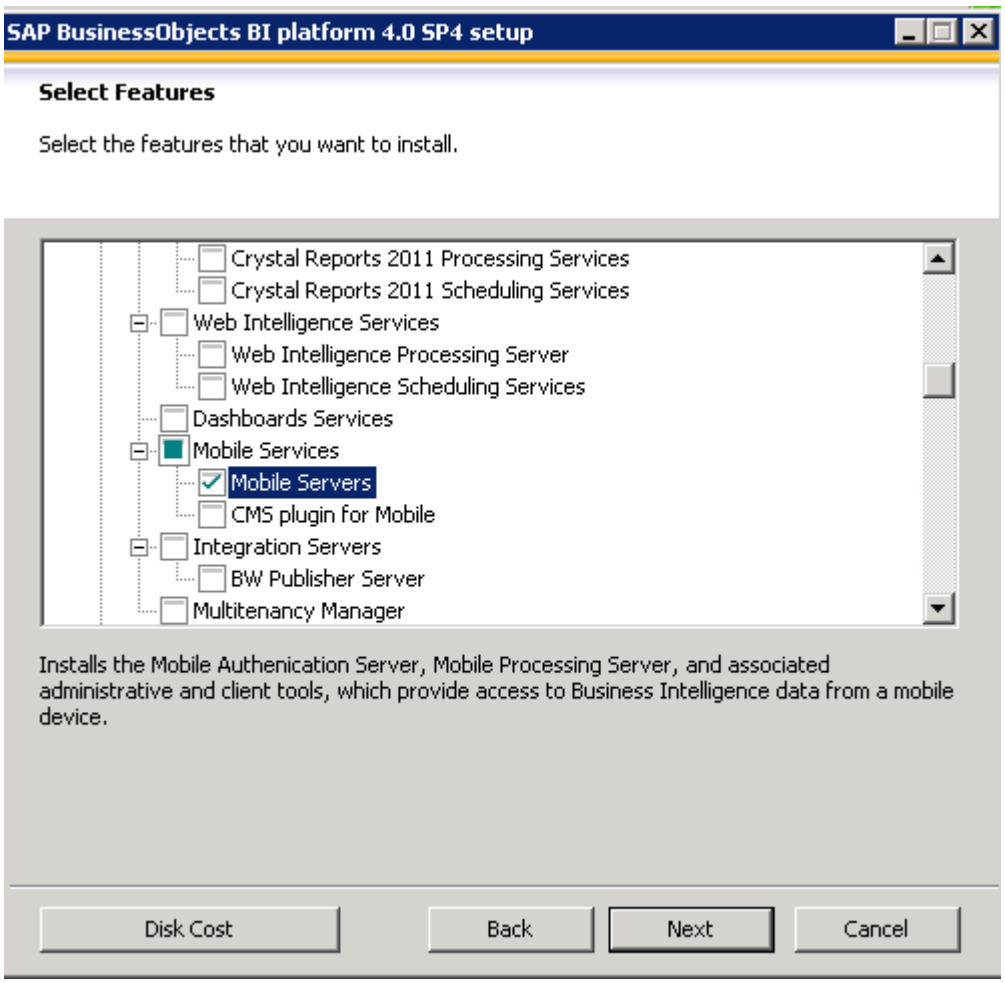
For information about using Mobile with AD authentication, a Load Balancer, and Firewals, see "Considerations" at the end of this topic.

To install the SAP Business Intelligence Mobile Server

Warning:

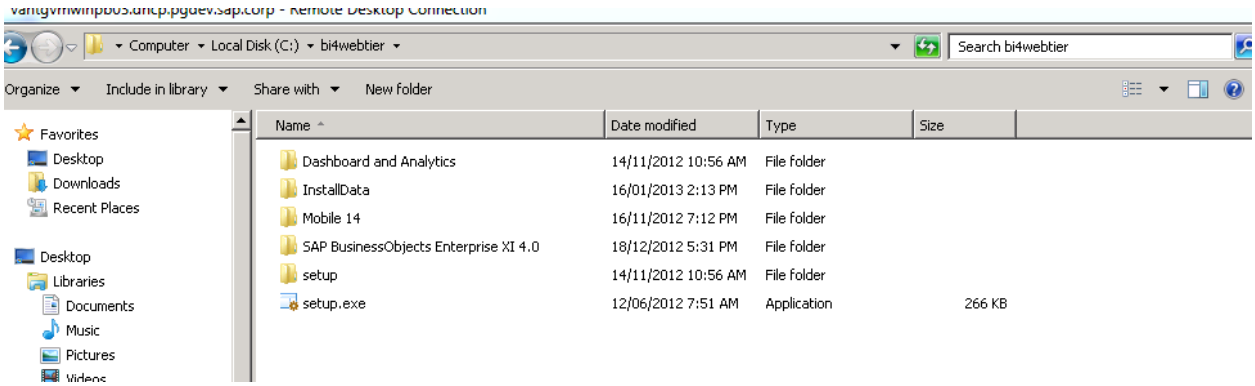
Mobile services must be installed on the web-tier to offer the client connectivity to the Enterprise system. If the feature "Mobile Services" is not enabled during the first installation, you can modify the installation and add the component later.

1. On the server that has the Web-Tier go to click Start > Control Panel > Programs and Features > SAP BusinessObjects BI Platform 4.0 SP4 , and then click Uninstall/Change. The "SAP BusinessObjects BI platform 4.0 SP4 setup" wizard opens. Select the option to modify or change.
2. On the "Select Features" page, select the **Mobile Servers** check box.

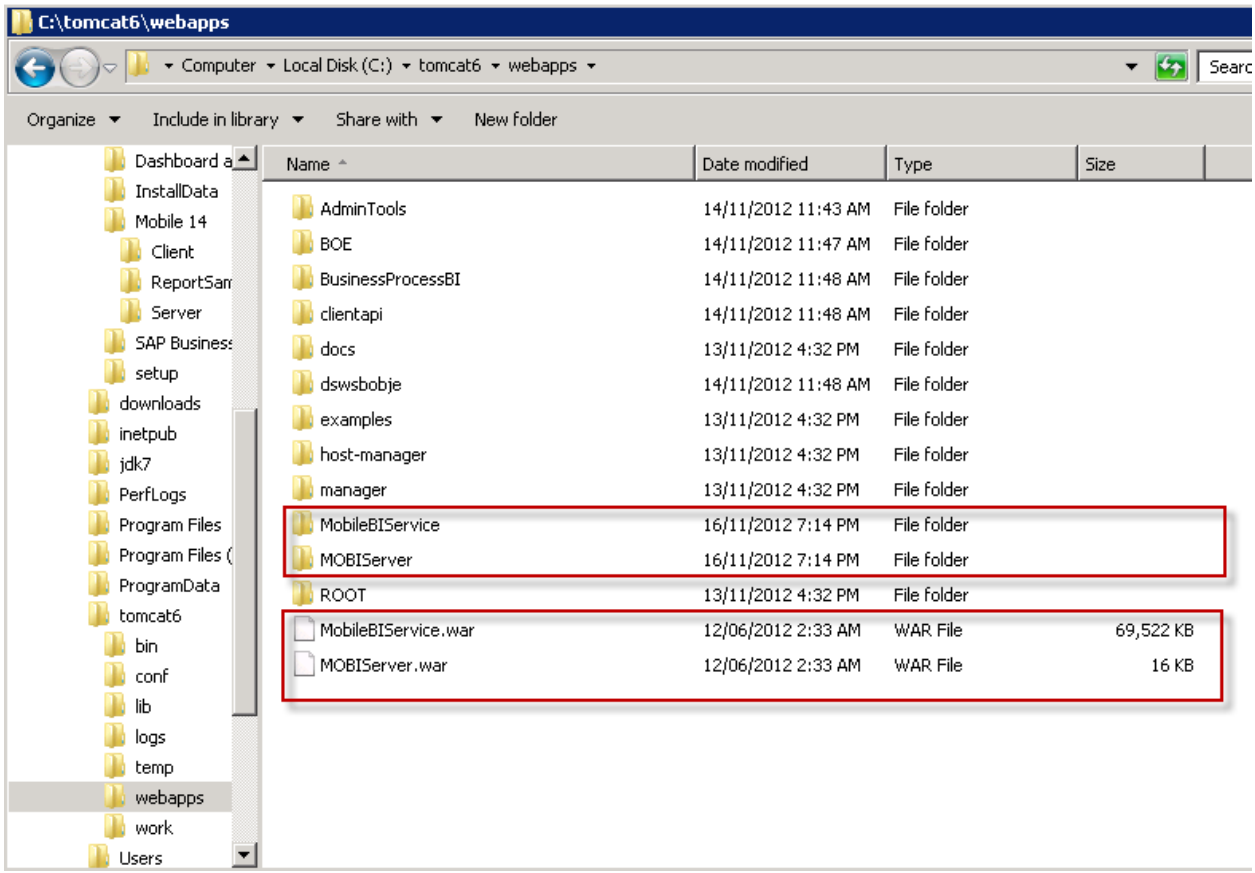


Warning: Make sure the SIA and other required services are selected in the Select Features screen when adding the Mobile Servers to the application tier. If unselected, a required service may be inadvertently uninstalled from the server.

3. Proceed through the wizard to commit this change. Enabling the "Mobile Servers" option creates a folder named Mobile 14 in the SAP BusinessObjects installation folder.



4. Open the Mobile 14 folder, and copy these two .war files to the tomcat6/webapps folder: MobileBIService.war and MOBIServer.war. The .war files will be automatically deployed by Tomcat.



5. To verify that the Mobile Server has been deployed, go to the this page to see if it displays the following result status:http://winpb01:8080/MobileBIService/MessageHandlerServlet?message=GetVersion

```
<?xml version="1.0" encoding="UTF-8" ?>
- <Result status="success">
  - <info>
      <version productVersion="14.0.4.738" internalVersion="1.7" />
    - <settings>
        <setting key="savePassword" value="false" />
        <setting key="offlineStorage.ttl" value="365" />
        <setting key="offlineStorage" value="false" />
        <setting key="offlineStorage.appPwd" value="true" />
      </settings>
    </info>
  </Result>
```

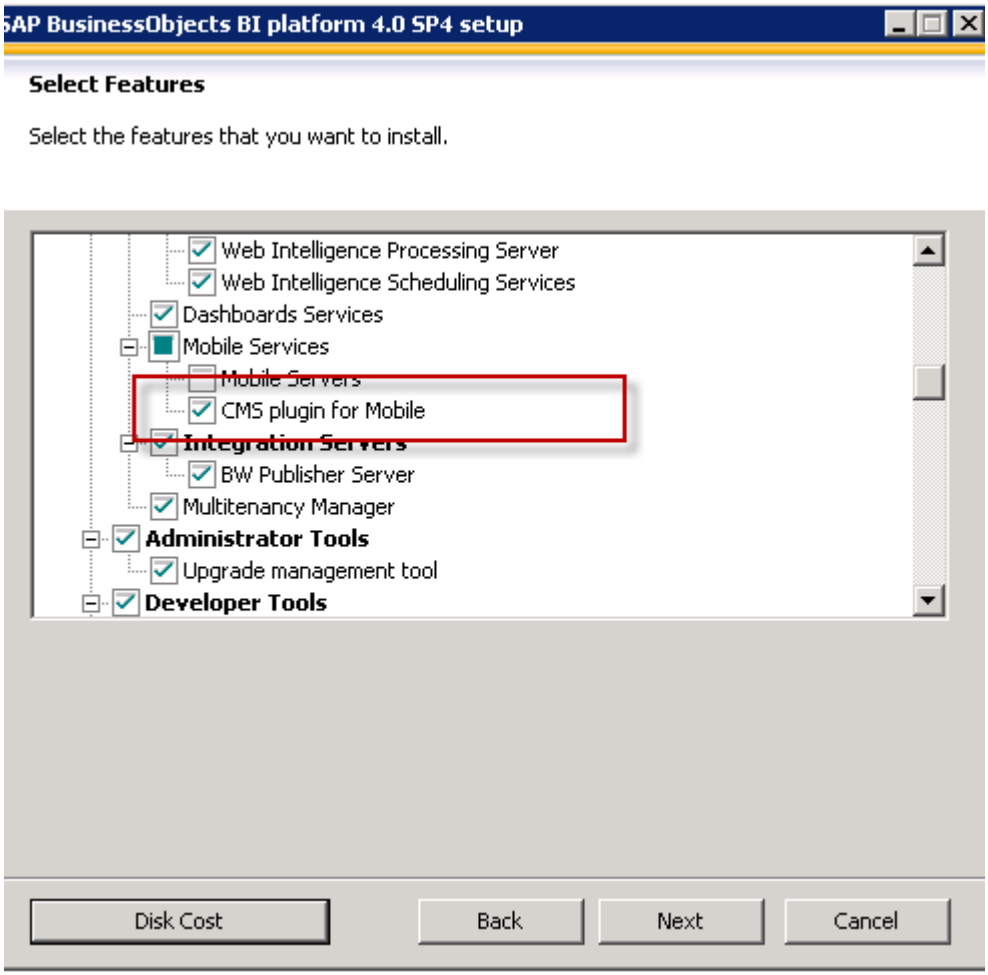

6. SAP BI Mobile Server is now deployed. It will allow you to access reports through a mobile device using the SAP BusinessObjects Mobile app and the SAP BusinessObjects Explorer application, once the remaining components are installed and configured as shown here.

   Warning: With the Support Package 5 release of the SAP BusinessObjects Mobile server, the files MobileBIService.war and MOBIServer.war will be automatically deployed.

To install the Mobile Plug-in

The Mobile Plug-in is required by the CMS.

1. In Windows, click **Start** > **Control Panel** > **Programs and Features** > **SAP BusinessObjects BI Platform 4.0 SP4** , and then click**Uninstall/Change**.
   The "SAP BusinessObjects BI platform 4.0 SP4 setup" wizard opens.
2. On the "Select Features" page, select the **CMS plugin for Mobile** check box.



3. Proceed through the wizard to commit this change.

   Warning: Note that the Mobile Plug-in must be installed on all Central Management Servers (CMS) on your system.

To configure Tomcat to enable the Mobile client

By default, the Mobile will only show reports that are part of the Mobile category. The Mobile category must be created manually.

1. In the Central Management Console (CMC), go to Categories > Manage > New > Category, and type Mobile.

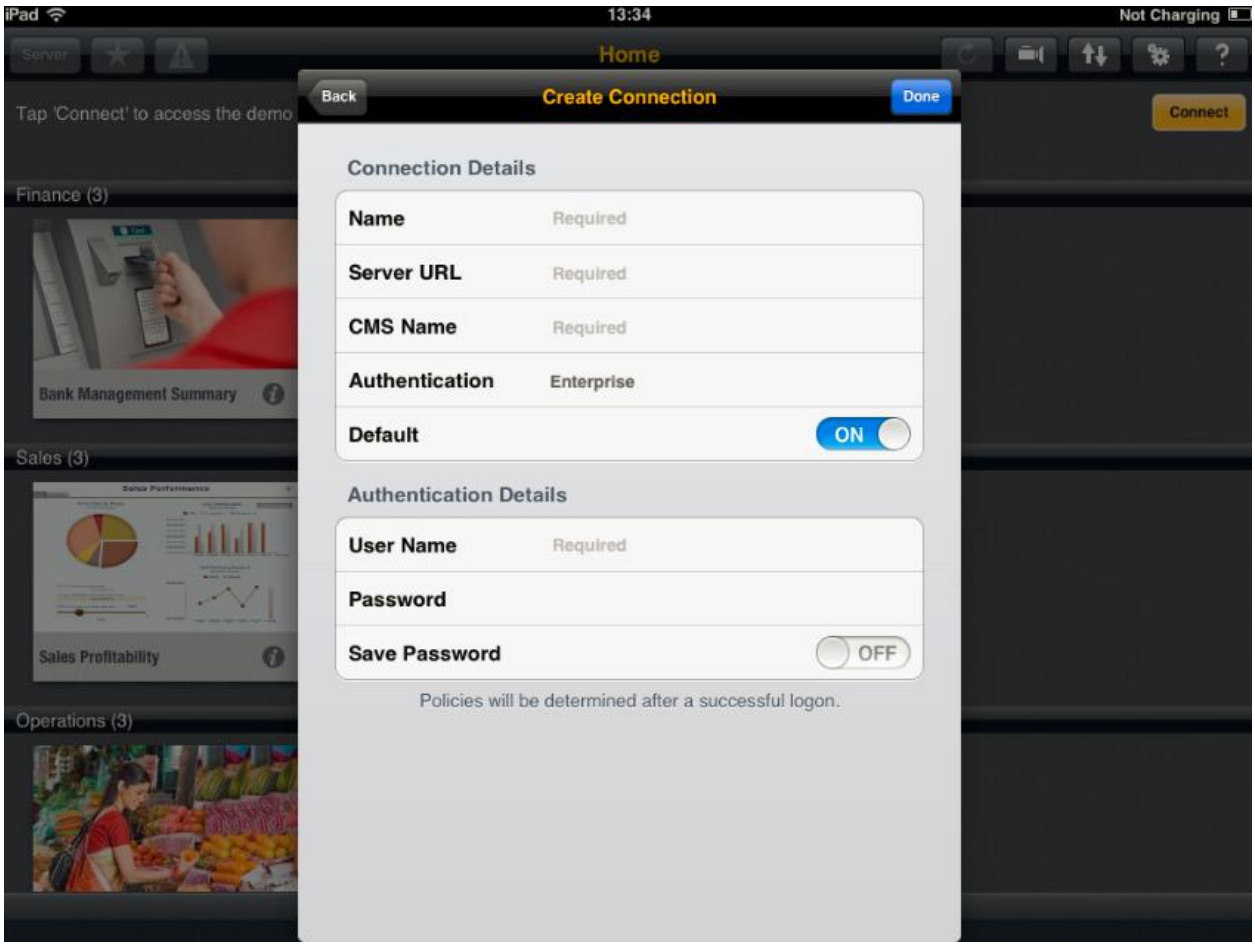
Warning: The category name in the CMC is case sensitive. It must match the category in the config file exactly.

We can now add a report into a category by going to the CMC > Folders > All Folders > Web Intelligence Samples. Right click the report and then select Categories. In Categories, select Mobile.

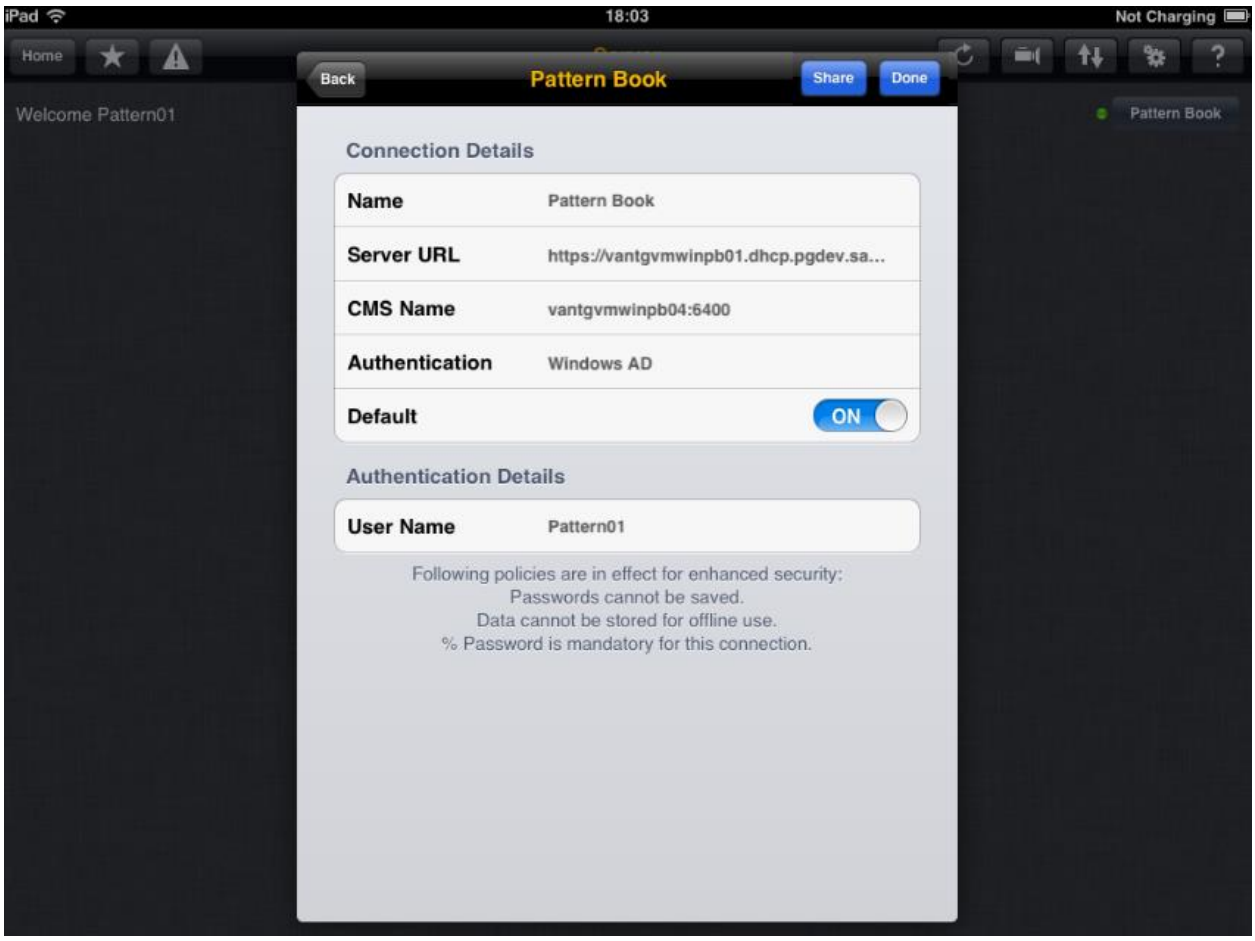
To install SAP BusinessObjects Mobile Client

1. Go the Apple App Store, do a search for “SAP BusinessObjects Mobile”, and download the latest version of the app.

2. On your device, start the application, and go to Settings > Create Connection.
3. Type the credentials needed to connect to the Mobile Server, setting the Server URL to the Web Server and Load Balancer.



4. For the CMS Name, use the hostname and port of a CMS in the cluster.



5. When done, tap Add a Connection.
6. Connect to the server.

   You will see the report that was saved in the Mobile category. Considerations

Setting up Active Directory (AD) authentication with BI Mobile

SAP Mobile does support third-party authentication. There is no explicit setup requirements for AD on Mobile. Provided that BI Launchpad can be accessed through the AD user, this user account can access Mobile reports.

- Note SSO is currently not supported.

Accessing Mobile Reports through a Load Balancer

SAP Mobile supports load balancers and web servers. The supported types of persistence for Mobile reports are as follows:

- Cookie-based persistence
- IP-based Persistence

Working With Firewalls and Mobile

The Mobile Server application deployed on Tomcat will need to communicate with the CMS, Web Intelligence Reporting Server, and the Adaptive Processing Server.

Troubleshooting

Users cannot view the reports but the Enterprise Administrator can

In this case, you must ensure that the users have access to the corporate category that was created.

BI Mobile Reports do not display after upgrading

Ensure that the link shows the same version number as the CMS:

http://*winpb01:8080*/MobileBIService/MessageHandlerServlet?message=GetVersion

Troubleshooting the Windows Pattern

This section provides troubleshooting tips and solutions for more common problems that you may encounter during the Linux pattern setup.

- Explorer Troubleshooting
- Application Server Troubleshooting
- Apache troubleshooting

Explorer Troubleshooting

Wdeploy fails during the post-install steps

Description

During the post install steps of the Explorer Web Tier installation, Wdeploy fails to deploy the .war files, and the following error message appears:

Resolution

To successfully deploy the .war files, stop Tomcat before Wdeploy is run.

Explorer services are not indicated as "Started" in the CMC

Description

After the Explorer installation is completed on all five servers in the Windows Pattern environment, none of the Explorer services start from the CMC, and all four services are indicated as either "Stopped" or "Disabled". And yet the **Task Manager** on the dedicated Explorer Server may show all four Explorer services as running and consuming the normal amount of memory.

Resolution

The Windows Firewall on the dedicated Explorer Server may be blocking communication between the CMS and the Explorer services. To solve the problem, configure the firewall to allow incoming and outgoing traffic for the Explorer services.

Application Server Troubleshooting

Error #1

Problem

BIP web tier installation fails with the following error:

setupexe: /lib/ld-linux.so.2: bad ELF interpreter: No such file or directory

Finished, return code is 126

Cause

32-bit glibc libraries are missing

Resolution

On Red Hat, run the following command as root:

> yum install glibc-2.12-1.47.el6_2.5.i686

Error #2

Problem

BIP web tier installation fails with the following error:

setupexe: error while loading shared libraries: libstdc++.so.5: cannot open shared object file: No such file or directory

Finished, return code is 127

Cause

Compatibility standard C++ libraries are missing

Resolution

On Red Hat, run the following command as root:

> yum install compat-libstdc++-33-3.2.3-69.el6.i68

Troubleshooting Application Server Cluster

Problem

In BI launch pad, the java.lang.NullPointerException error occurs.

Cause

Session failover does not occur correctly

Resolution

1. Create a sample web application to test cluster failover.

a. Log into lnxpb02 as **tomcat**.
b. Create a directory called cluster in the webapps directory to contain the sample application. Run the following commands:
   > cd /opt/apache-tomcat-7.0.25/webapps
   > mkdir -p cluster/WEB-INF
   > cd cluster/WEB-INF
c. Create a web.xml file and add the **distributed** tag. Run the following command:
   > vi web.xml

   Insert the following code block:

```
<?xml version="1.0" encoding="ISO-8859-1"?>
 web-app xmlns="http://java.sun.com/xml/ns/javaee"
 xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://java.sun.com/xml/ns/javaee
http://java.sun.com/xml/ns/javaee/web-app_2_5.xsd"
 version="2.5">
<distributable />
</web-app>
```

d. Create a JSP file to test session failover outside of BIP. Run the following commands:
   > cd /opt/apache-tomcat-7.0.25/webapps/cluster
   > vi test.jsp

   Insert the following code block:

```
<%
   session.setAttribute("a","a");
 %>
 <html>
 <head>
 <title>Test JSP</title>
 </head>

<body>
 <table
width="100%" border="0" cellspacing="0" cellpadding="0">
   <tr bgcolor="#CCCCCC">
     <td width="13%">vantgvmlnxpb02</td>
     <td width="87%"> </td>
   </tr>
   <tr>
     <td>Session ID :</td>
     <td><%=session.getId()%></td>
   </tr>
```

```
</table>
</body>
</html>
```

e. Repeat steps a-d on lnxpb03. In test.jsp, replace "vantgvmlnxpb02" with "vantgvmlnxpb03".
f. Test session failover by accessing the test.jsp file through the load balancer at http://vantgvmlnxpb01/cluster/test.jsp.

   You will see output similar to the following:
   vantgvmlnxpb02
   Session ID : 26743DFB75C097ED1F8E3BC59D76229C.vantgvmlnxpb02

g. Stop the Tomcat instance the session is hosted on, in this case lnxpb02. Run the following command:
   > service tomcat7 stop
h. Refresh test.jsp in the browser and check the session:

   vantgvmlnxpb03
   Session ID : 5E69F09D5A6679AE648F2890CE79B1D3.vantgvmlnxpb03
   Warning: The session has changed so there is a problem with clustering externally to BIP.

2. The solution can be found on the Tomcat wiki at http://wiki.apache.org/tomcat/FAQ/Clustering#Q8.
   Navigate to the following section: The cluster doesn't work under Linux with two nodes on two boxes.
   Does a multicast route to your network interface exist?
3. Run the following command as root on both lnxpb02 and lnxpb03. Type:
   > route add -host 228.0.0.4 dev eth0
4. Next, restart the Tomcat instances on both lnxpb02 and lnxpb03 and test the process again. Run the following command on both machines:
   > service tomcat7 restart

5. Use the sample application to test session failover at http://vantgvmlnxpb01/cluster/test.jsp

   Note the session details:
   vantgvmlnxpb02
   Session ID : BF2462E53AEB9A74C5C8575B86A3A43D.vantgvmlnxpb02
   a. Stop Tomcat on lnxpb02. Run the following command:
   b. > service tomcat7 stop
   c. Refresh test.jsp in the browser.
      Note the session details:
      vantgvmlnxpb03

Session ID : BF2462E53AEB9A74C5C8575B86A3A43D.vantgvmlnxpb0

Warning: Session ID remains the same but the route identifier has changed. This confirms clustering is working externally to BIP.

6. Now test BI launch pad.
    a. First identify which node you are connected to by accessing http://vantgvmlnxpb01/cluster/test.jsp.
    b. Note the session details:
       vantgvmlnxpb02
       Session ID: D84CB1072F4788DECD86CA90E45FBD07.vantgvmlnxpb02
    c. Next, access BI launch pad at http://vantgvmlnxpb01/BOE/BI.
    d. Log in as administrator.
    e. Select the Document list.
    f. Stop Tomcat on the machine we're currently connected to, which is lnxpb02. Run the following command:
    g. > service tomcat7 stop
    h. Click the **Home** tab in BI launch pad and note that it seamlessly transitions without error.
    i. Now return to http://vantgvmlnxpb01/cluster/test.jsp.
    j. Note the session details:
       vantgvmlnxpb03
       Session ID : D84CB1072F4788DECD86CA90E45FBD07.vantgvmlnxpb03

Tomcat Application Server clustering is working as expected.

Apache Troubleshooting

Troubleshooting the Apache web server setup

Problem
Users are unable to connect to Apache through a browser

Cause
Firewall configuration prevents access to the web server from client browsers

Resolution

1. Temporarily disable the firewall for testing purposes.
    a. Log into **lnxpb01** as **root**.
    b. Stop the iptables service. Type:
       > service iptables stop

You should see output similar to the following:
iptables: Flushing firewall rules: [OK]
iptables: Setting chains to policy ACCEPT: filter [OK]
iptables: Unloading modules: [OK]

Warning: Disabling the firewall on your system will make it vulnerable to attacks. On an internal system, the risks are fairly low but you will want to ensure that you enable your firewall protection after you have completed your testing.

The firewall has now been stopped. Attempt to access the system again to see if the problem has been resolved by this change.

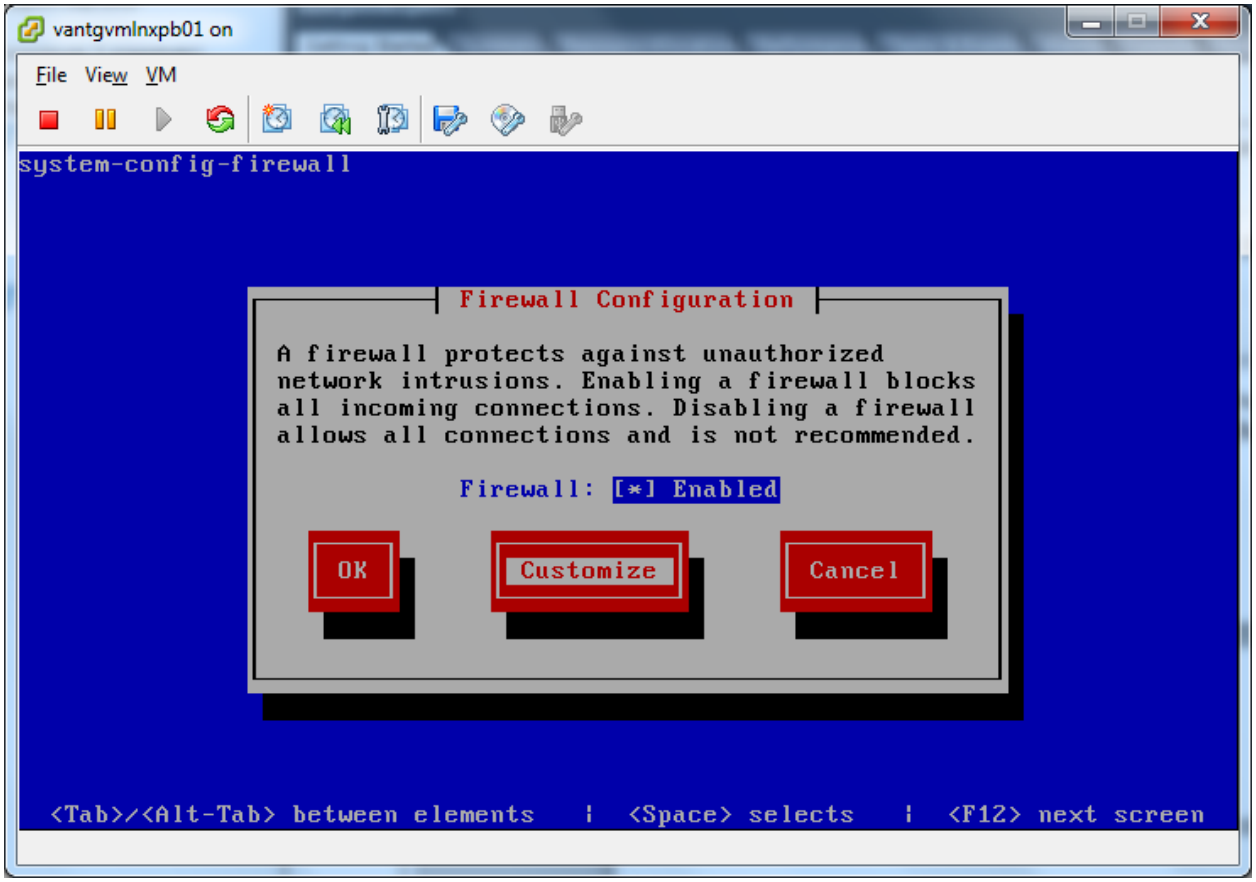
2. Try to connect via both **http** and **https** connections:
   a. http://lnxpb01/
   b. https://lnxpb01/
3. Try pinging the server from your client machine.
   a. Launch the command prompt and run the following command:
      > ping lnxpb01
   b. Ensure that the httpd daemon is running on the Apache machine. Run the following command:
      > ps -ef |grep httpd
   c. Ensure that the http/https ports are open and listening on the Apache machine. Run the following command:
      > netstat -l |grep http
      You will see output similar to the following:
      http://lnxpb01/
      https://lnxpb01/
   d. Check the httpd access logs to see if the connection made it to the httpd daemon. Run the following command:
      > tail -f /var/local/usr/apache/logs/access_log

      You will see output similar to the following:
      10.7.92.208 - - [31/May/2012:11:57:02 -0700|||] "GET / HTTP/1.1" 200 11313

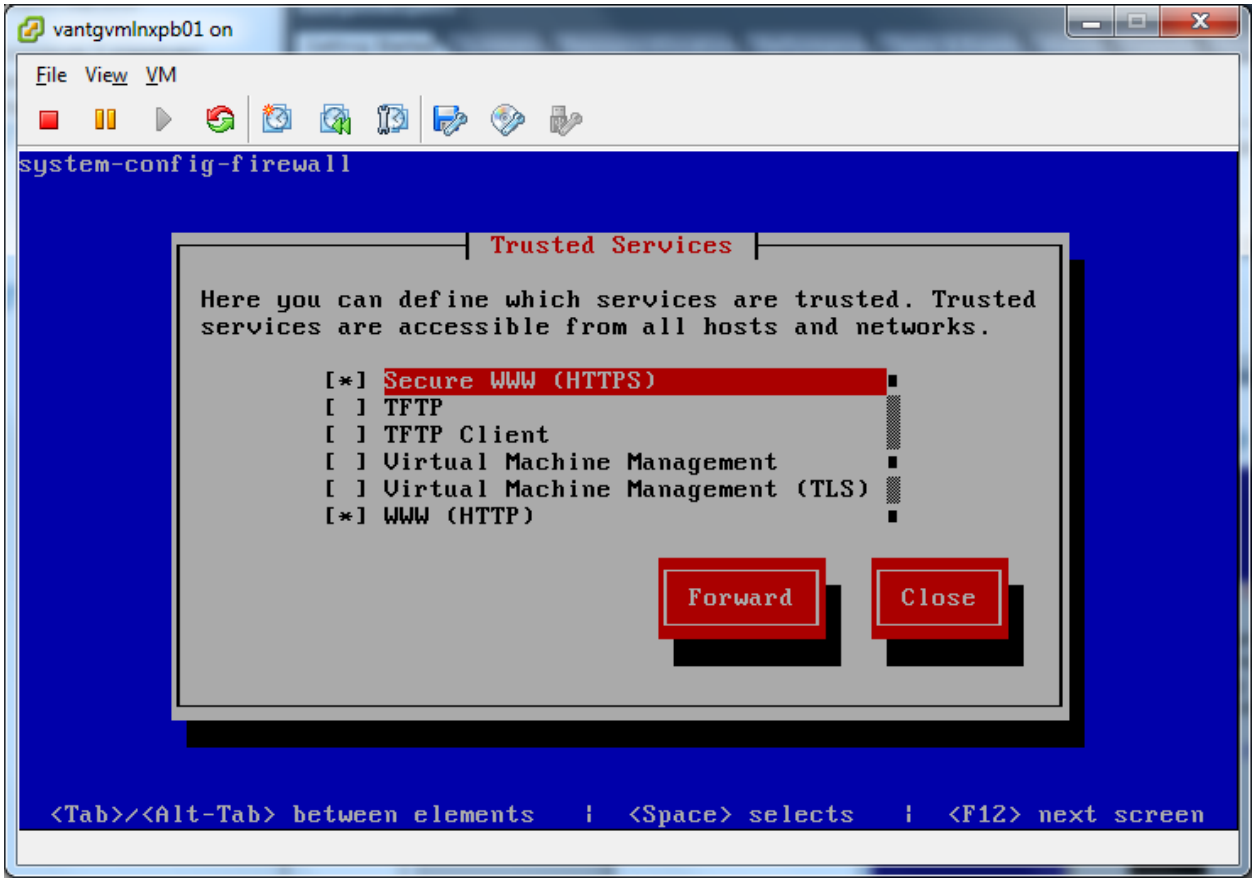
Adding iptables info for Apache process

In this section, you will configure the firewall and define which services can be trusted.

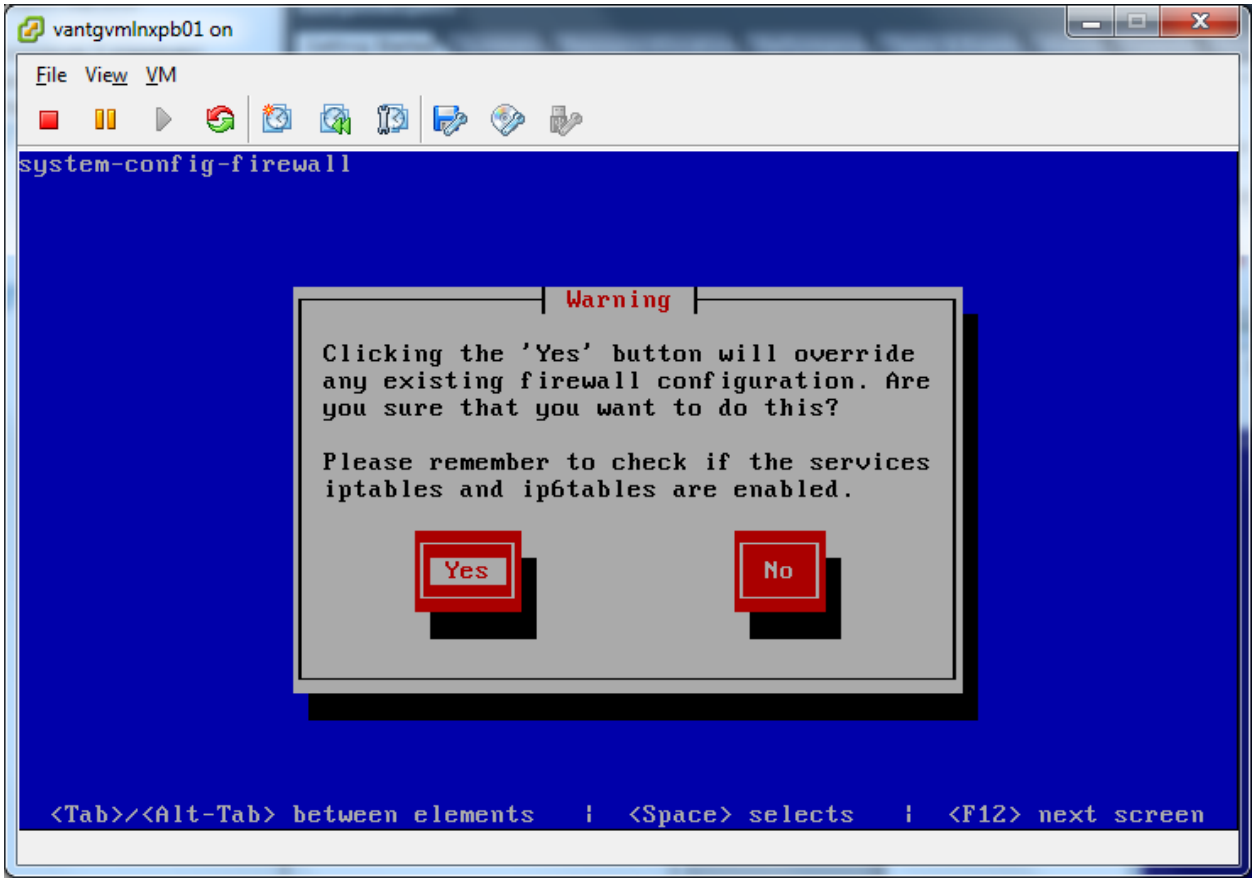
1. Log into lnxpb01 as **root**.
2. Launch the system configuration tool for firewall. Run the following command:
   > system-config-firewall-tui
3. Ensure the **Enabled** option is selected beside **Firewall**. Click **Customize**.



4. Select **Secure WWW (HTTPS)** and **WWW (HTTP)** and click **Close**:



5. Click OK.
6. Click Yes.



7. Verify the firewall is now running. Run the following command:

> service iptables status

You will see output similar to the following:

Table: filter
Chain INPUT (policy ACCEPT)
num target prot opt source destination
1 ACCEPT all – 0.0.0.0/0 0.0.0.0/0 state RELATED,ESTABLISHED
2 ACCEPT icmp – 0.0.0.0/0 0.0.0.0/0
3 ACCEPT all – 0.0.0.0/0 0.0.0.0/0
4 ACCEPT tcp – 0.0.0.0/0 0.0.0.0/0 state NEW tcp dpt:22
5 ACCEPT tcp – 0.0.0.0/0 0.0.0.0/0 state NEW tcp dpt:80
6 ACCEPT tcp – 0.0.0.0/0 0.0.0.0/0 state NEW tcp dpt:2049
7 ACCEPT tcp – 0.0.0.0/0 0.0.0.0/0 state NEW tcp dpt:443
8 REJECT all – 0.0.0.0/0 0.0.0.0/0 reject-with icmp-host-prohibited

Chain FORWARD (policy ACCEPT)
num target prot opt source destination
1 REJECT all – 0.0.0.0/0 0.0.0.0/0 reject-with icmp-host-prohibited

Chain OUTPUT (policy ACCEPT)
num target prot opt source destination

8. Ports 80 and 443 are now open to accept incoming connections. This should allow for your end users to connect in to your system. Test this using one of the following the Web Server URLs:
   - http://lnxpb01/
   - https://lnxpb01/