Proven Practice

Installing and Configuring the JBOSS Application Server for IBM Cognos 8

Product(s): IBM Cognos 8.3, JBOSS Application Server

Area of Interest: Infrastructure

DOC ID: AS21 Version 8.3.0.0

Copyright

This document is maintained by the Best Practices, Product and Technology team. You can send comments, suggestions, and additions to BestPractices-ProductandTechnology@cognos.com

TABLE OF CONTENT

1 Introduction

1.1 Purpose

This document is for those who have limited experience with JBoss and who wish to set up a JBoss Application Server environment. The document consists of detailed instructions that explain the steps required. The primary goal is to set up a basic environment for testing purposes and not necessarily a high performance production environment.

Except where noted, the primary focus of this document will be to cover the setup steps required for IBM Cognos 8.3

1.2 Scope

The instructions in this document will work cross platform however the examples shown will be based on a Windows install. UNIX installations require slight modifications to syntax but should otherwise be identical. For example, regarding the syntax for variables, use ${VARIABLE} for UNIX and %VARIABLE% for Windows. Consult your UNIX documentation for more information regarding shell commands, syntax and scripting.

This document will take you through the steps to install and setup JBoss Application Server with IBM Cognos 8 in a single server environment.

1.3 Definitions, Acronyms, and Abbreviations

Term	Definition
JVM	Java Virtual Machine A software "execution engine" that safely and compatibly executes the byte codes in Java class files on a microprocessor (whether in a computer or in another electronic device). The JVM is responsible for the hardware and operating system independence of the J2SE platform, the small size of compiled code (bytecodes), and platform security.
J2SE	Java 2 Platform, Standard Edition There are two principal products in the J2SE platform family: J2SE Runtime Environment (JRE) and J2SE Development Kit (JDK).
JRE	Java Runtime Environment The JRE provides the Java APIs, Java virtual machine, and other components necessary to run applets and applications written in the Java programming language. It is also the foundation for the technologies in the Java 2 Platform, Enterprise Edition (J2EE) for enterprise software development and deployment. The JRE does not contain tools and utilities such as compilers or debuggers for developing applets and applications
JDK	Java Development Kit

	The JDK is a superset of the JRE, and contains everything that is in the JRE, plus tools such as the compilers and debuggers necessary for developing applets and applications.
J2EE	Java 2 Platform, Enterprise Edition Combines a number of technologies in one architecture with a comprehensive Application Programming Model and Compatibility Test Suite for building enterprise-class server-side applications. The Java 2 Platform, Enterprise Edition (J2EE) defines the standard for developing multitier enterprise applications. The J2EE platform simplifies enterprise applications by basing them on standardized, modular components, by providing a complete set of services to those components, and by handling many details of application behavior automatically, without complex programming.
JMX Console	The JBoss JMX Console runs in a web browser. It displays the components of the running server instance, including classes and deployed applications.

1.4 References

Ref. ID	Author/Paper	Location
ASCG05	ASCG05_Installing_Cognos8.doc	Customer Support
	IBM Cognos 8 Installation and Configuration Guide	IBM Cognos 8 install kit

1.5 Assumptions

Before continuing, make sure the following prerequisites have been met.

- That you have the necessary licenses and files (appropriate for your environment) to perform the installation and any applicable updates. Install kits from internal sources in IBM Cognos are not available for external distribution. Customers can obtain install kits from JBoss.org or JBoss.com.
- That you have the necessary access rights to perform the installation. It is best if the user used to install JBoss Application Server is the same user used to setup and run IBM Cognos 8. Root access is not a requirement for the installation on UNIX. On Windows, the user should be a member of the Administrators group, if intending to install as a service. Refer to http://wiki.jboss.org for details.
- That you have the necessary system resources to perform the installation. Running with less than 768MB of RAM for the Max Heap Memory is not suggested (although it may be possible for testing purposes only). You should allot 350 to 400 MB of disk space for the application server installation. More space will be required for additional servers, application files, and logging.
- JBoss supports both JDK 1.4.2 and 1.5.0. The Application Server install does not provide a JVM. Also, you cannot use the JRE install. You must install the full JDK before installing JBoss.
- That you have the customer documentation available as a resource. You should have both the IBM Cognos 8 documentation as well as the JBoss documentation.
- That you are familiar with the operating system (OS) with which you are using. This document assumes you are familiar with the OS. This includes user commands at the command line, syntax and scripting.
- That you are familiar with IBM Cognos 8. You should already know how to setup and run the product using Tomcat.

2 Product Installation

2.1 Steps to Install JBoss 4.0.4

Before installing JBoss Application Server, make sure the prerequisites listed in section 1 have been met.

Important: Do not use spaces in the JBoss install path!

Whether installing on Windows or a UNIX platform, do not use an installation path containing spaces. This is a JBoss requirement.

The JBoss install can be used on Windows or UNIX platforms and is available in two formats: ZIP file or JAR file.

2.1.1 JBoss Install from ZIP File

The ZIP file, jboss-4.0.4.GA.zip, is the base 4.0.4 install, and can be downloaded from the main JBoss site, http://www.jboss.org.

On Windows, you can use WinZip to unzip the file to the desired location on your machine.

On UNIX platforms, you can use the unzip utility to extract the install. Copy the ZIP file to the intended install directory for JBoss and enter the following:

```
unzip jboss-4.0.4.GA.zip
```

The install will be extracted and ready for configuration. Do not use a location with spaces in the path.

2.1.2 JBoss Install from JAR File

The JAR file, jboss 4.0.4.GA-Patch1-installer.jar, contains a full install of JBoss. Use your JDK to extract and run the install program. You can also use it to patch an existing install. If you have an existing installation and would prefer to upgrade it instead of installing a new setup, then you can use the Patch Install. You should consult the Release Notes for information regarding changes and any functionality that has been deprecated.

Before running the upgrade, you may wish to backup your server directory and any keystores that you may be using for security.

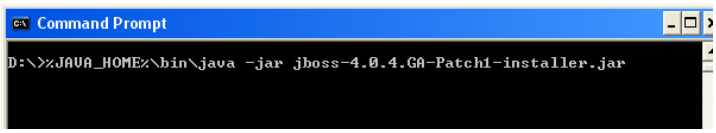
1. To use the installer, open a command prompt and navigate to the location of the JAR file. Run the following command to start the install program.

   Windows:

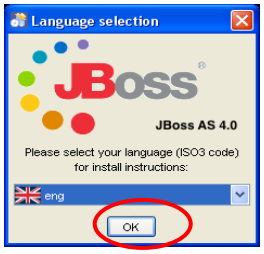
   ```
   %JAVA_HOME%\bin\java -jar jboss-4.0.4.GA-Patch1-installer.jar
   ```

   UNIX:

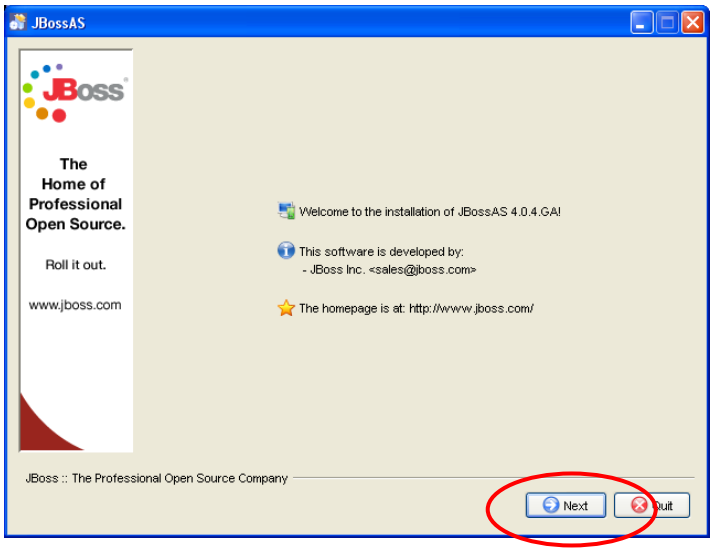
   ```
   $JAVA_HOME/bin/java -jar jboss-4.0.4.GA-Patch1-installer.jar
   ```



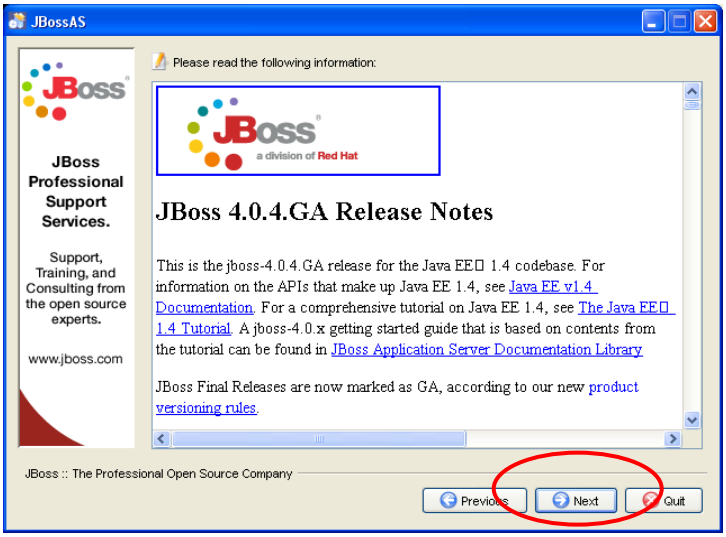
2. An installation language prompt will be displayed. Make an appropriate selection.



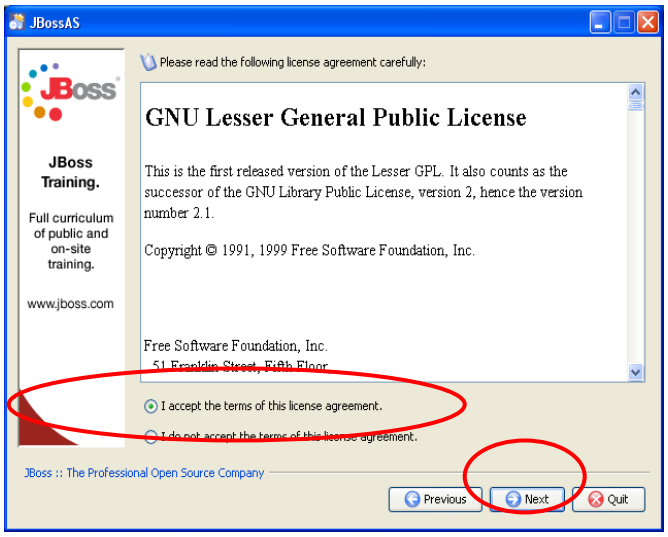
3. The Welcome page will be displayed.



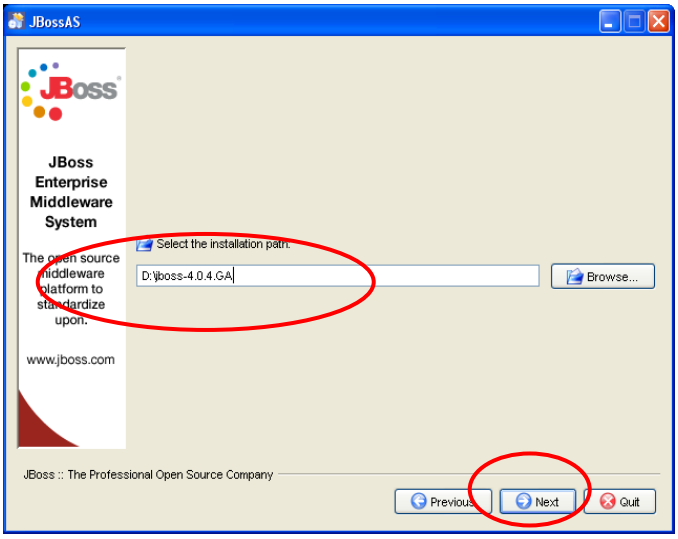
4. Optionally, read the Release Notes for JBoss 4.0.4.



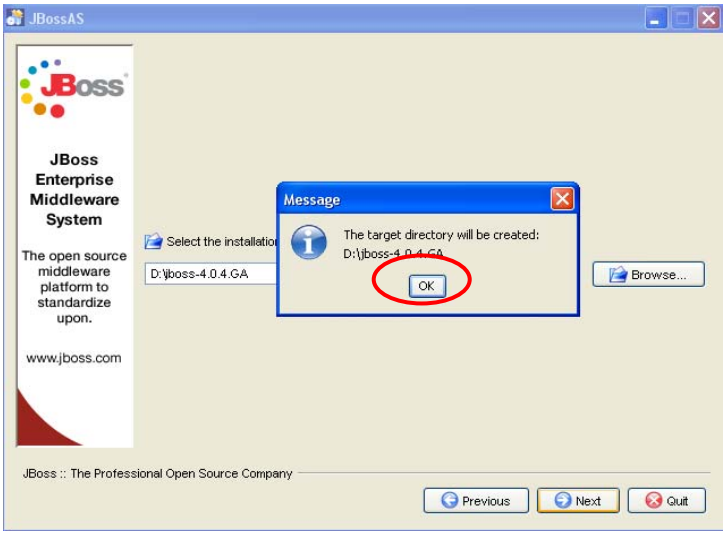
5. Read and accept the License agreement.



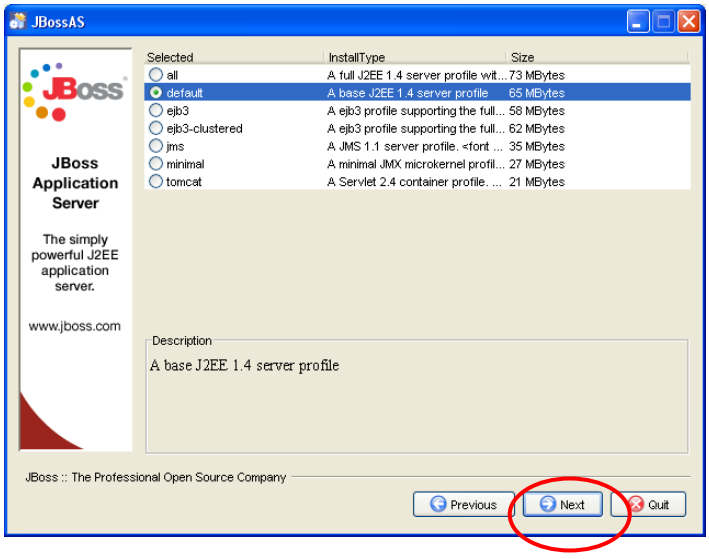
6. Enter an appropriate install location. Do not use spaces in the install path.



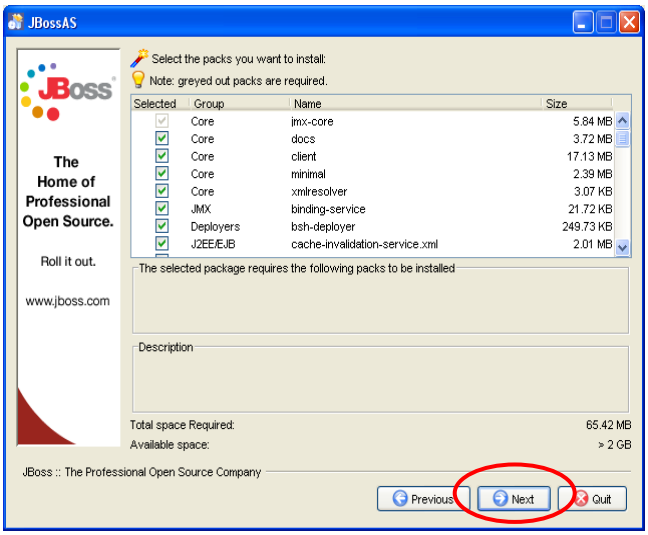
If the directory does not exist, you will be prompted to confirm its creation. .



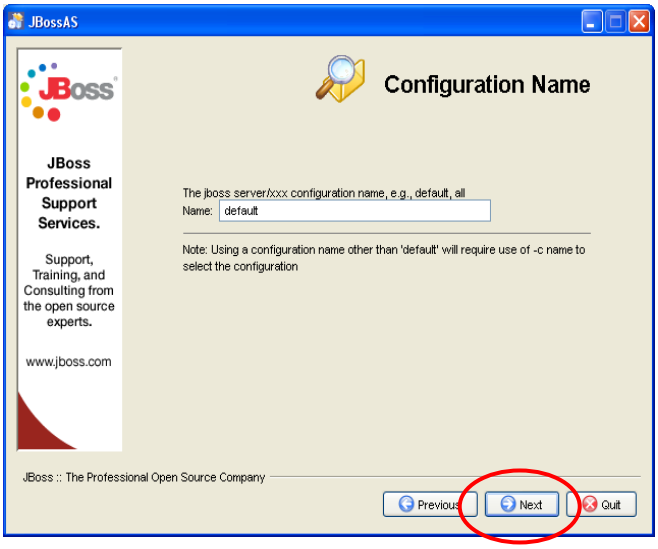
7. Optionally, select the install type. The default is acceptable.



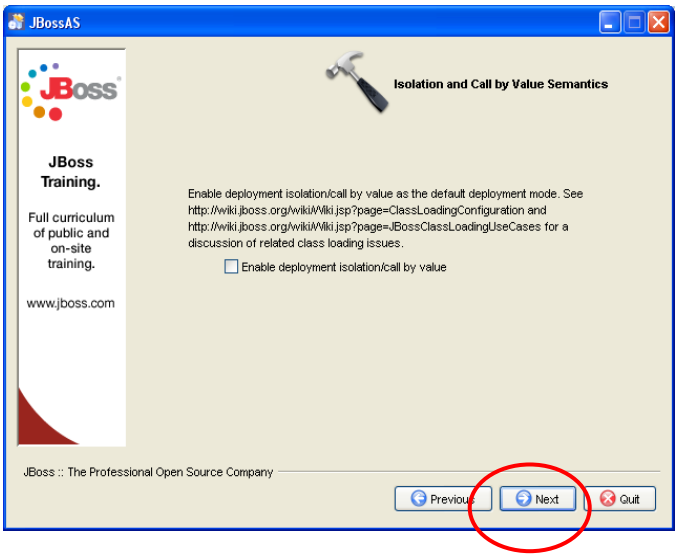
8. Various JBoss components will be listed. Accept the default selections.



9. Optionally, change the name of the server from “default”.

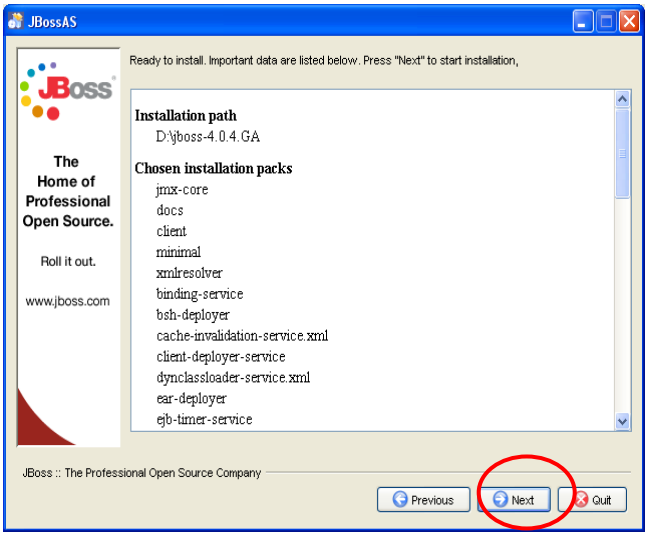


10. Optionally, enable deployment isolation and call by value. It is not required.

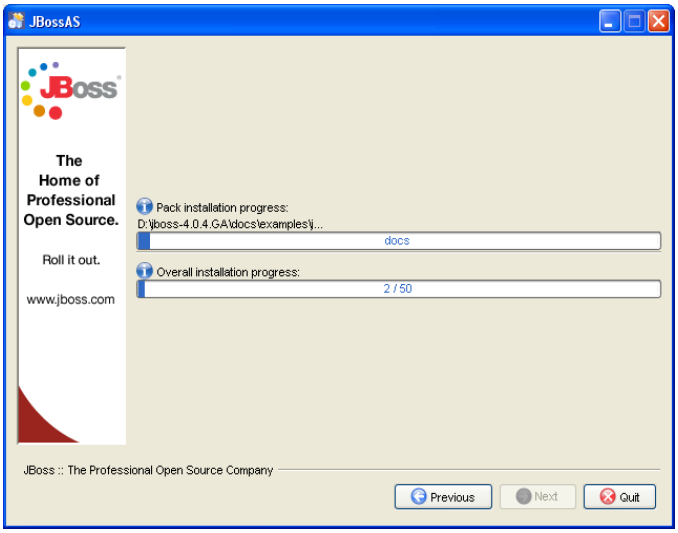


11. Optionally, Secure the JMX interfaces. It is not required.

12. The summary page will be displayed. Return to the previous pages if you need to alter any installation settings.

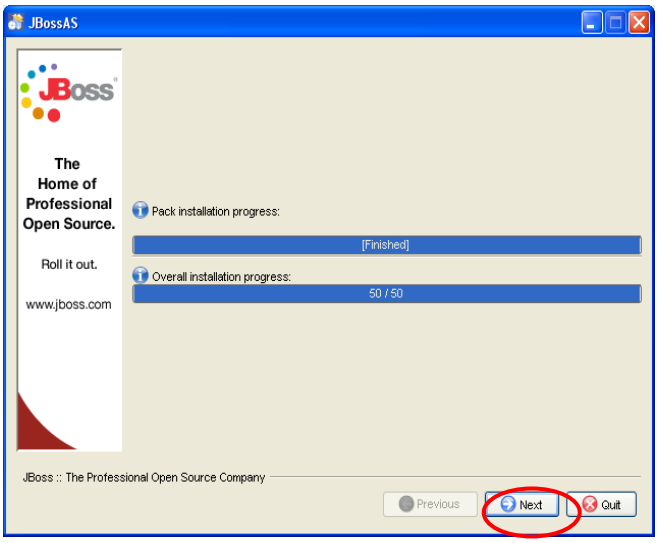


13. The installation will now be performed and the progress dialog will be displayed.

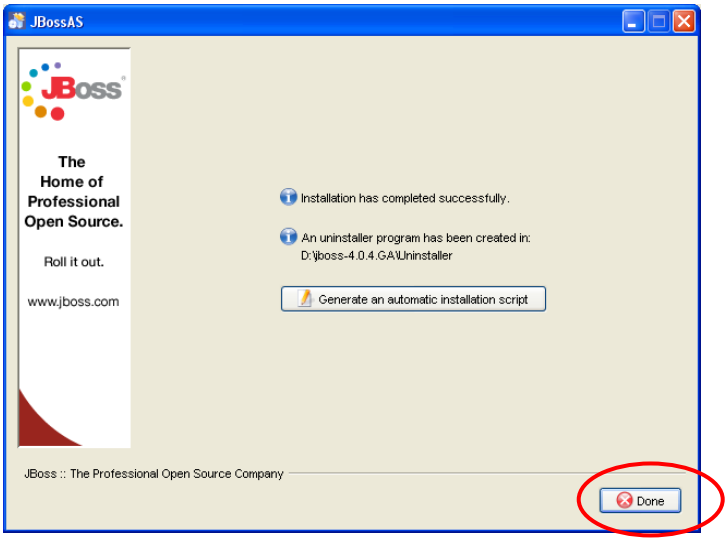


The installation will take a few minutes to complete.

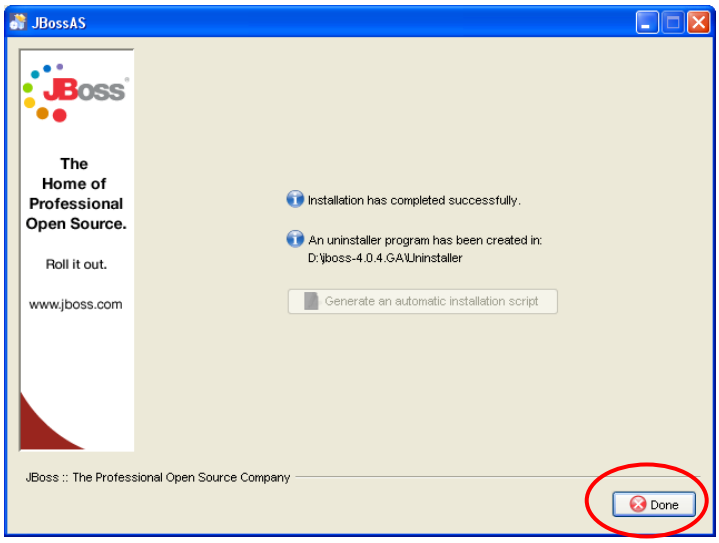
14. Once completed verify there are no errors indicated before continuing.

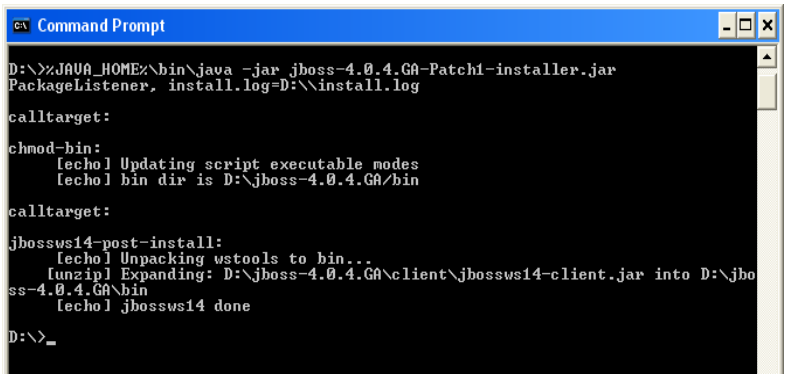


15. You will be prompted to create an installation script. This script is not necessary for IBM Cognos 8.

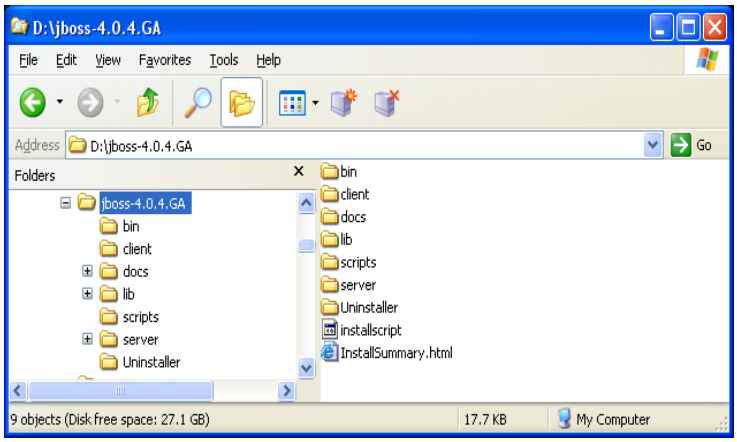


16. You may now exit the installation program.





Verify that the install completed successfully. Navigate to the install location, you should find the following folder structure. JBoss Application Server is now installed.



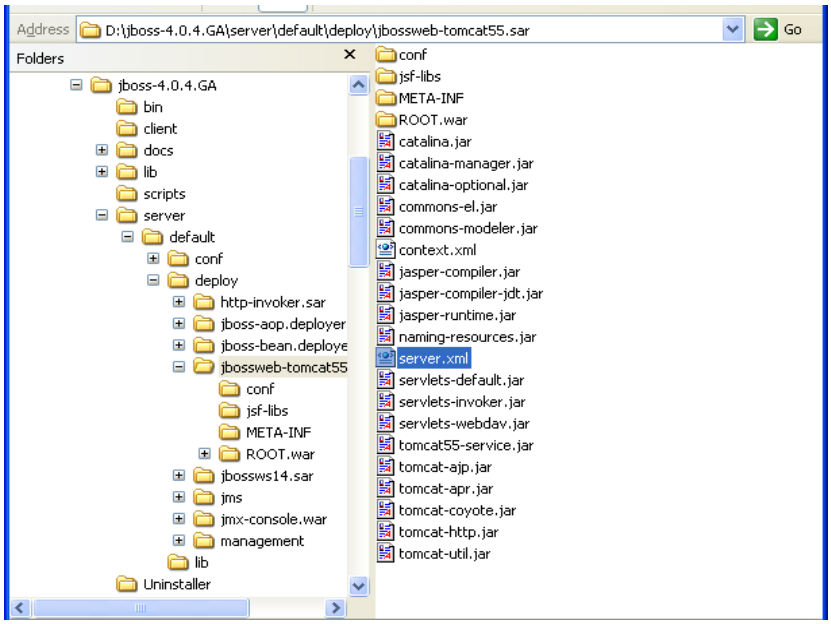
3 Configuring JBoss

JBoss 4.0.x is packaged with Tomcat 5.5. The default port used by the engine is 8080.

It is recommended that you make a copy of the default server instance and rename it. Do not use spaces in the name. For example, call it cognos. You can then change the server.xml file to use port 9300 or another port not already in use. By doing this, you will always have a copy of the initial server instance as a backup.

Also, if you already have Oracle DB Server installed on your machine, the listener will be set to listen on 8080, by default. To change the default port for JBoss, navigate to the following location.

<jboss-4.0.4-install-dir>\server\<instance_name>\deploy\jbossweb-tomcat55.sar

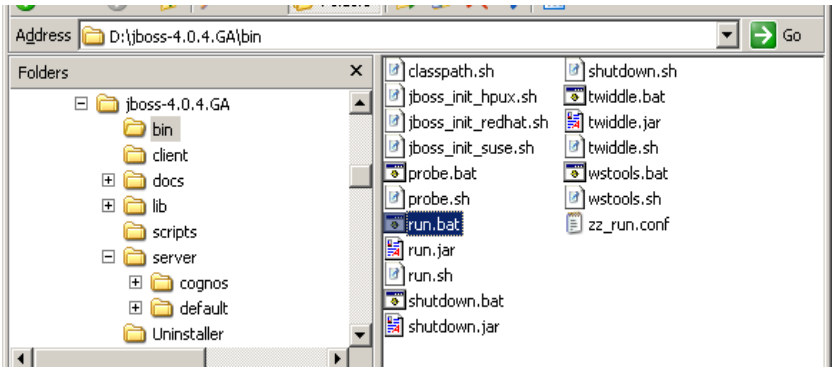


Open server.xml and search on port 8080.

```
<Service name="jboss.web"
      className="org.jboss.web.tomcat.tc5.StandardService">

      <!-- A HTTP/1.1 Connector on port 8080 -->
      <Connector port="8080" address="${jboss.bind.address}"
         maxThreads="250" strategy="ms" maxHttpHeaderSize="8192"
         emptySessionPath="true"
         enableLookups="false" redirectPort="8443" acceptCount="100"
         connectionTimeout="20000" disableUploadTimeout="true"/>
```

Change this to another port number not already in use. Save and close.

Before using JBoss with IBM Cognos 8, you should modify the memory settings. Navigate to the <jboss_install_root>\bin directory and open the run.bat file. (run.sh for UNIX)



Scroll down until you find the JAVA_OPTS variable. The default settings for minimum and maximum heap size are –Xms128m –Xmx512m. You should increase these values, taking into consideration available resources and anticipated machine load. The default for IBM Cognos 8 is the small configuration size: **–Xms192m –Xmx768m**.

An argument for log4j is also required. Add **-Dlog4j.defaultInitOverride=true** to the JAVA_OPTS variable. An example is provided below.

```
rem Sun JVM memory allocation pool parameters. Modify as appropriate.

set JAVA_OPTS=%JAVA_OPTS% -Xms256m -Xmx768m -
Dsun.rmi.dgc.client.gcInterval=3600000 -
Dsun.rmi.dgc.server.gcInterval=3600000 -Dlog4j.defaultInitOverride=true
```

Also, JBoss includes a file called run.conf that can be used to set variables. It is located in the <jboss_install_root>\bin directory, and its use is optional. If you do not wish to use it, rename the file or back it up in an alternate location.

4 Starting and Stopping JBoss

The JBoss startup scripts are located in the bin directory. For example, if the application server was installed in the D drive, then the scripts would be found in D:\jboss-4.0.4.GA\bin.

4.1 Starting the Server

The startup script is called run.bat (run.sh for UNIX) and can be found in %JBOSS_HOME%\bin. Before starting JBoss, you should set the JAVA_HOME environment variable. The JDK used when running JBoss Application Server **must** be the same as the one used for running IBM Cognos Configuration. Refer to section 6 for more information regarding setup.

If running the default server, simply type in run.bat in the command prompt. If running a specific server instance, you would enter

```
run.bat –c instance_name
```

For example, if you created a server called cognos, you would use the following command to start it.

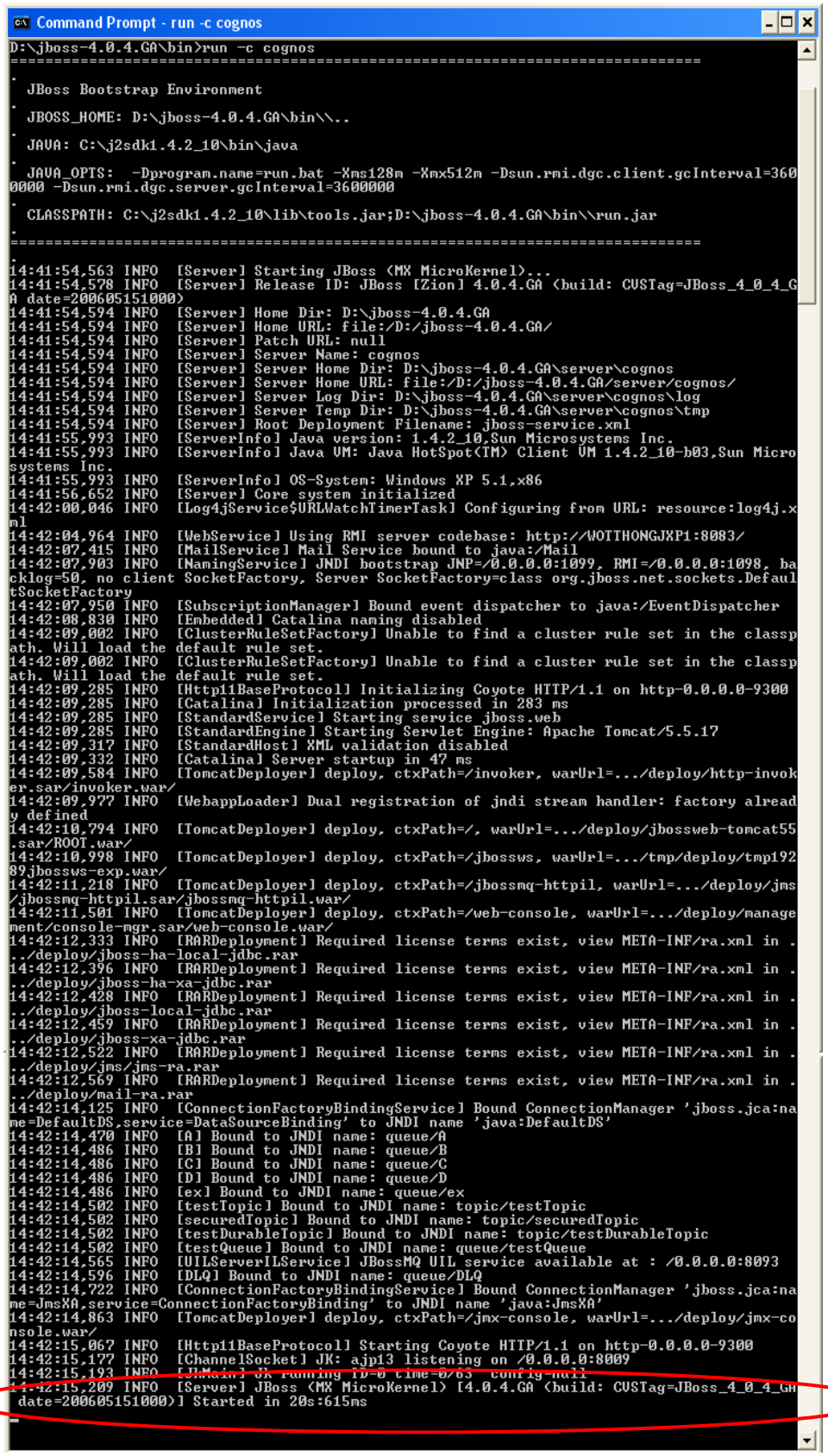
```
run.bat –c cognos
```

Note: the startup may take several minutes, depending on machine resources.

When you see messages similar to those below, it indicates that JBoss has started.

```
14:54:10,420 INFO  [Http11BaseProtocol] Starting Coyote HTTP/1.1 on http-0.0.0.0-9300
14:54:10,561 INFO  [ChannelSocket] JK: ajp13 listening on /0.0.0.0:8010
14:54:10,592 INFO  [JkMain] Jk running ID=0 time=0/94  config=null
14:54:10,607 INFO  [Server] JBoss (MX MicroKernel) [4.0.4.GA (build:
CVSTag=JBoss_4_0_4_GA date=200605151000)] Started in 19s:884ms
```

To stop JBoss, you can simply enter Ctrl-C in the prompt, and it will start the shutdown. You will be prompted to terminate the batch job. Enter Y and click Enter.



5 General Environment Setup

5.1 Install Database Client(s)

Ensure that all necessary client software is installed and available to the user account that will run the application server. This includes access to the database that you will use for the Content Manager as well as your reporting database(s). The database that will be used as the Content Manager data store must be created and a userID / password must be given appropriate rights to the database.

For UNIX, make sure the appropriate environment variables are set for the database client. This can be accomplished by setting your environment in the terminal session, or via the use of scripts. You should verify access to the database using an appropriate tool (ex. sqlplus) to ensure the client software is installed and configured correctly.

This environment **must** be available to the user running the application server and IBM Cognos 8. It should be set up in such a way that it is set automatically and will be available if the server is restarted.

Important: Ensure that any java database client files are in place prior to proceeding so that they will be included in the application archive file that will be built later in this document. (For example, ojdbc14.jar for Oracle Database clients must be copied to *<Cognos8_install>*/webapps/p2pd/WEB-INF/lib.)

Refer to the IBM Cognos 8 Installation Guide for more information on setting up database clients.

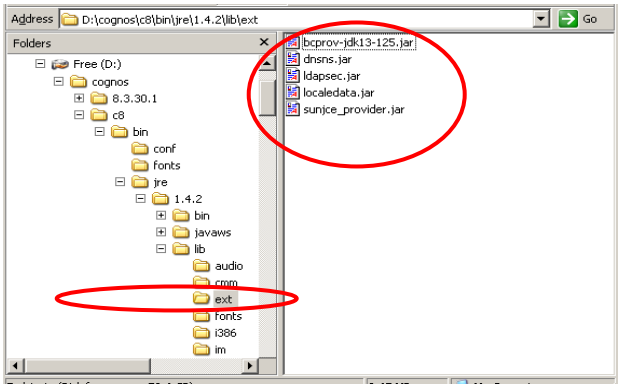
5.2 Install Security Provider File

IBM Cognos Configuration requires that a security provider file be copied to the JDK used by the application server. For JBoss, the user must ensure that a supported Java Development Kit (JDK) has been installed on the system. The full JDK must be installed and not just the JRE.

The user must copy the bouncy castle jar file (bcprov-jdk13-125.jar) provided with the IBM Cognos 8 install to the $JAVA_HOME/jre/lib/ext directory. You can find the security provider file under *<C8_install_path>*/bin/jre/1.4.2/\lib/ext on all platforms.

Warning: To ensure that the application server environment is not disrupted, do not overwrite any existing files. You may wish to copy the original $JAVA_HOME/jre/lib/ext directory to a backup location prior to copying the IBM Cognos 8 files.

Example: IBM Cognos 8 Java Directory on Windows



6 IBM Cognos Configuration

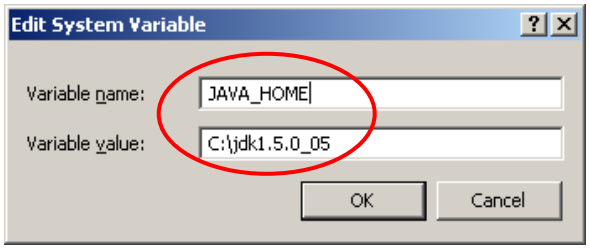
6.1 Setup the Environment

6.1.1 Set Java Home

Prior to launching IBM Cognos Configuration or generating new encryption keys, you must set the environment variable JAVA_HOME to point to the JDK to be used by the application server. The JDK used when running IBM Cognos Configuration **must** be the same as the one used for running JBoss Application Server.

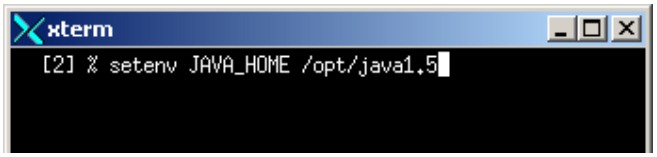
For most simple installations, it is recommended that the value be set as a global system environment variable (Windows) or in a script (UNIX). A reminder for UNIX users: be sure to set the variables correctly which may necessitate the "export" command as well. Different platforms and different shell environments use slightly different syntax to accomplish this task.

Example: Windows Global System Environment Variable



On UNIX, the JAVA_HOME variable can be set for the terminal session, in the user profile or whatever means is appropriate for your environment.

Example: UNIX Terminal Window (C shell)



6.1.2 Set the Library Path

When running IBM Cognos 8 on an application server, the library path must be modified to include the Cognos 8 bin directory location. The library path variable is used to locate the IBM Cognos 8 library files.

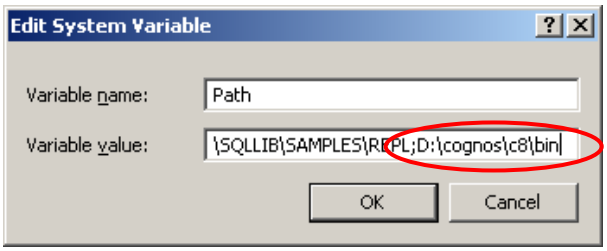
For most simple installations, it is recommended that the value be set as a global system environment variable (Windows) or in a script (UNIX). On UNIX, the library path can be set for the terminal session, in the user profile or whatever means is appropriate for your environment.

> Tip: If you intend to install multiple instances of IBM Cognos 8 on a single server, set the library path variable within the application server instance scope and not as a global variable to ensure that each instance has a unique value.

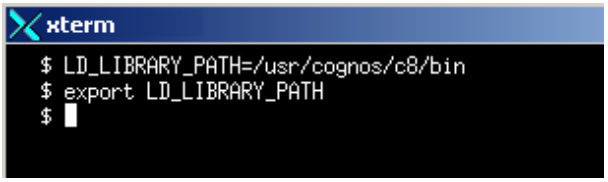
The <*c8_location*>/bin must be appended to the appropriate environment variable for the operating system you are running.

Operating system	Environment variable
Windows	PATH
AIX	LIBPATH
Solaris and Linux	LD_LIBRARY_PATH
HP-UX	SHLIB_PATH

Example: Windows Global System Environment Variable



Example: UNIX Terminal Window (Bourne shell)



6.2 Launch IBM Cognos Configuration

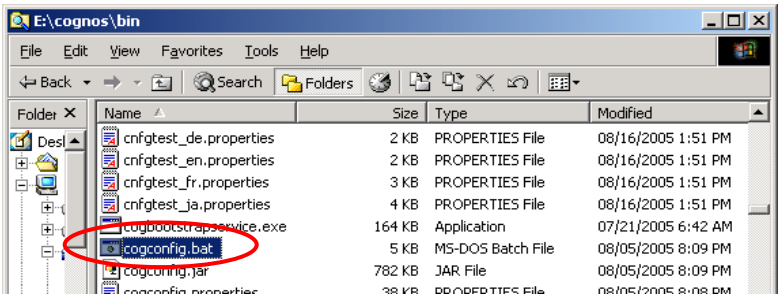
The following steps demonstrate a single server installation.

If you are performing a distributed installation:

- Follow the steps as indicated starting with the Content Manager component install. Complete all related tasks and start IBM Cognos 8 Content Manager. Leave it active and running.
- Once the IBM Cognos 8 Content Manager is running, repeat the steps for the Application Tier Components install, making the appropriate changes and starting the IBM Cognos 8 Application Tier Components.
- Make sure the Application Tier Components are running. Repeat the steps making the appropriate changes to configure the IBM Cognos 8 Gateway component.

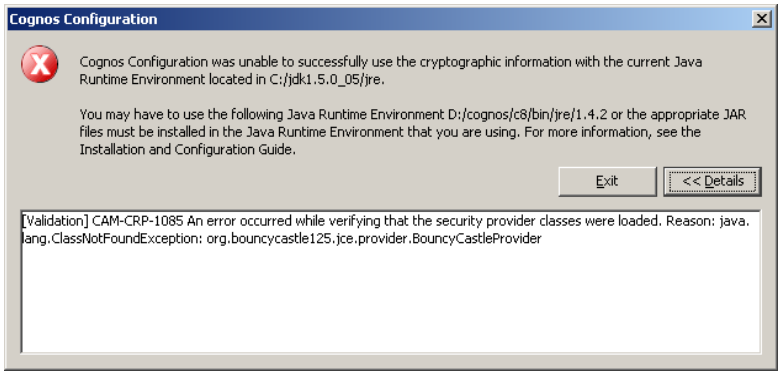
To start IBM Cognos Configuration after setting the JAVA_HOME environment variable, navigate to the <C8 installation>\bin directory and run the batch file *cogconfig.bat* (Windows) or the script *cogconfig.sh* (UNIX).

Example: Windows cogconfig.bat file



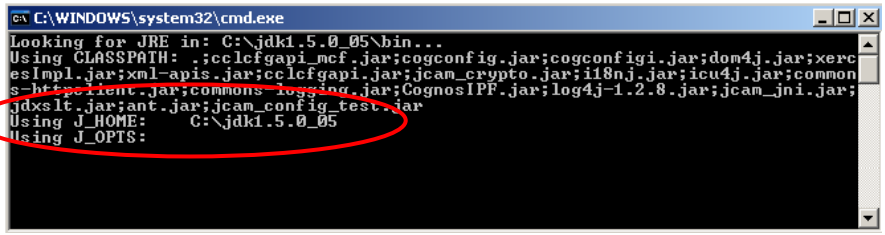
Example: UNIX cogconfig.sh script

If the security provider file was not copied to the correct location, you may encounter an error similar to the example below.

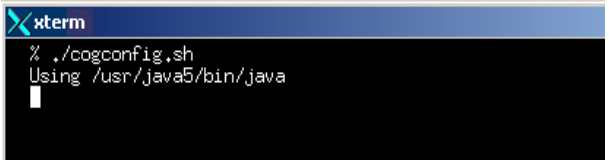


The batch file (Windows) or script file (UNIX) will also indicate which JDK was found based on the JAVA_HOME environment variable. This should be checked to ensure the correct one is being used.

Example: Batch file output on Windows – check J_HOME value

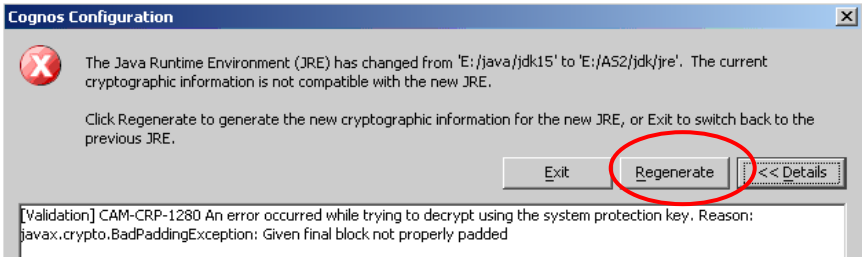


Example: Script output on UNIX



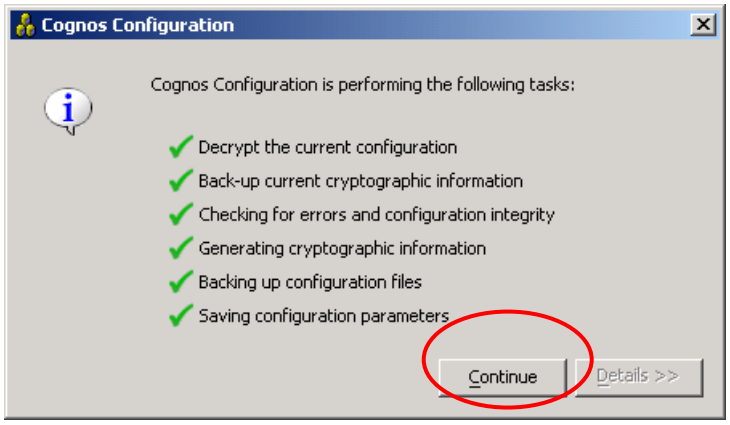
If IBM Cognos Configuration was run previously and there are existing encryption keys, then you may encounter a warning dialogue. This dialogue indicates that an alternative JDK vendor or version was used previously and the keys are not compatible with the current JDK vendor or version.

Example: Existing Encryption Keys



If the correct JDK is referenced, then you may select the option to automatically regenerate new encryption keys.

Example: Regenerate Encryption Keys



Ensure that all steps complete successfully during the regeneration process prior to proceeding. If the automatic regeneration of the encryption keys fails for any reason, it may be necessary to follow the manual key recreation steps outlined in the IBM Cognos 8 Installation and Configuration Guide.

6.3 IBM Cognos Configuration Settings

The default values in IBM Cognos Configuration represent the out-of-box Tomcat solution. There are a number of settings that must be changed to suit your application server environment. Obviously there are many other options that you may have to alter that will not be covered in this document. Refer to the IBM Cognos 8 Installation and Configuration Guide for details.

6.3.1 Change URI Values

An IBM Cognos 8 URI contains the following elements:

For a Content Manager or Dispatcher URI's

protocol://host_name_or_IP:port/context_root/alias_path

For a Gateway or Web content URI

protocol://host_name_or_IP:port/virtual_directory/gateway_application

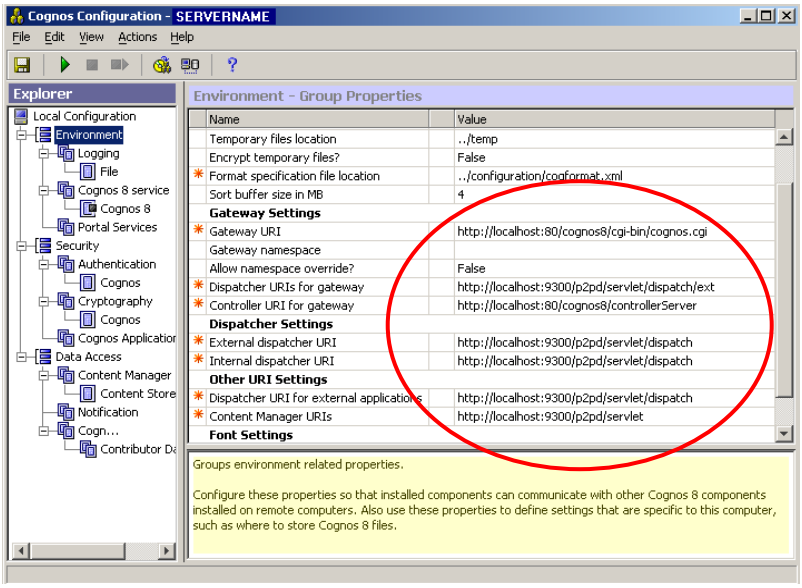
OR

protocol://host_name_or_IP:port/context_root/alias_path

Element	Details
Protocol	This element specifies whether standard (http) or secure (https) communication is used when transmitting or receiving information.
Host Name or IP	The host name is the name of the server as it is identified on the network. You may use an IP address if name resolution is not possible. You must change the localhost element of a URI to a server name, fully qualified domain name, or IP address in a distributed installation. In a mixed environment of UNIX and Windows servers, ensure that host names can be resolved to IP addresses by all servers in the environment. Also ensure that the application server is configured to listen on the value entered.
Port	This element specifies the port on which the host system has a socket open to listen for requests. The value entered must match the value in your Web server, Tomcat, or application server configuration. The port number used by the IBM Cognos 8 Dispatcher and Content Manager is the JBoss port that was set in the server.xml file.
Context Root	The context root element is used by the Web server, Tomcat, or the application server to route requests to the appropriate Java application. The context root can only be changed if you are using an application server. In a distributed IBM Cognos 8 environment, the context root for all application deployments must be the same, with the exception of the Servlet Gateway application, which will have a unique value. The context root must be a single entity, i.e. it may not contain slashes (“/”).
Alias Path	This portion of the URI must not be modified or IBM Cognos 8 components will not function correctly. The value is defined and used internally by IBM Cognos 8.
Virtual Directory	This element must indicate the virtual directory alias exactly as it is defined in your Web server configuration. For example, in the default Gateway URI of http://localhost:80/cognos8/cgi-bin/cognos.cgi, the virtual directory is cognos8/cgi-bin.
Gateway Application	The Gateway URI must include a reference to the gateway application. For example, if you are accessing IBM Cognos 8 components using a Common Gateway Interface (CGI), then the default gateway application would be cognos.cgi.

In the IBM Cognos Configuration Explorer window, under Environment, set the appropriate values for all URI entries used in your environment. The port number used by the IBM Cognos 8 Dispatcher and Content Manager is the JBoss port that was set in the server.xml file.

Example: Single Server – IBM Cognos Configuration Default Values (Tomcat)

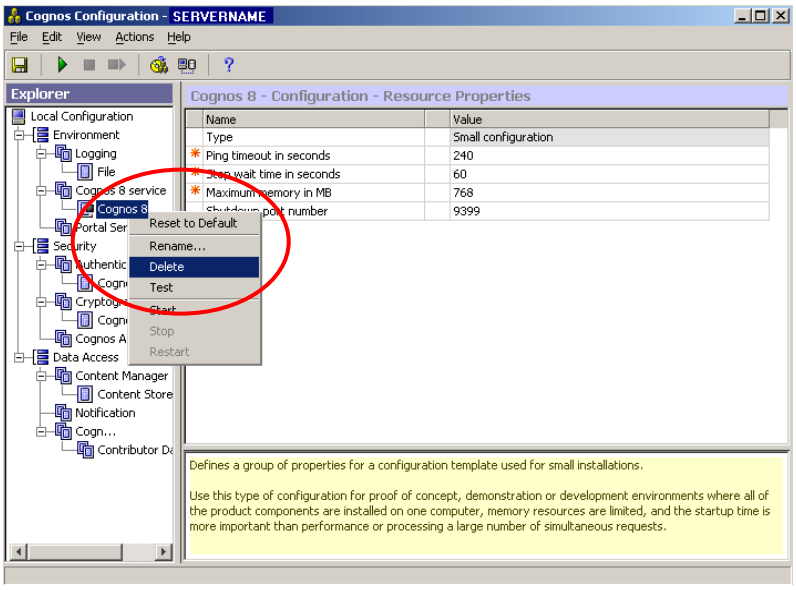


6.3.2 Delete the Tomcat Service Configuration

By default, an IBM Cognos 8 service entry will be defined in IBM Cognos Configuration. This configuration setting is only used to run the application using the Tomcat install provided with the IBM Cognos 8 installation. It should be removed when configuring Cognos 8 to run on an application server.

To delete the entry, right-click on the IBM Cognos 8 service and select the “Delete” menu item.

Example: Delete the IBM Cognos 8 Service



You will then be prompted to confirm the removal of the IBM Cognos 8 service. This service can be added to IBM Cognos Configuration at a later date, should you wish to run under Tomcat instead of JBoss.

6.3.3 Remaining IBM Cognos Configuration Changes

Refer to the IBM Cognos 8 Installation and Configuration Guide for details.

Navigate to the Content Manager Content Store field and enter the appropriate values for your environment. The default uses MS SQL Server. Please see the IBM Cognos 8 customer documentation for information on creating other Content Store types for other supported vendors.

At this time you should make any other changes within IBM Cognos Configuration that are necessary for proper operation in your environment. Depending on your setup, no other changes may be required.

6.3.4 Save IBM Cognos 8 Configuration Changes

Once all the configuration changes have been made, you can save the configuration.

During the Save operation, encryption keys will be created using the JDK referenced by the JAVA_HOME variable. Other actions such as backing up the configuration files will also take place.

Reminder:

- For an Application Tier Components only install, the Content Manager must be up and running in order for the Save operation to complete successfully.
- For a Gateway component only install, the Content Manager and the Application Tier must be up and running in order for the Save operation to complete successfully.

6.4 Build Application Files Wizard

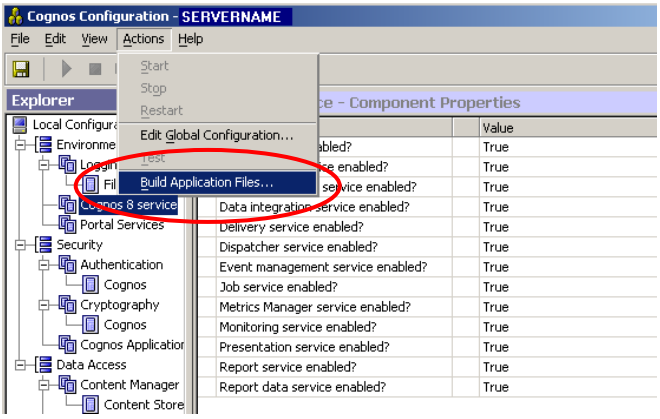
6.4.1 Start the Build Application Files Wizard

The IBM Cognos Configuration Build Application Files Wizard can be run to create and package all the files that are necessary to deploy the Cognos 8 application to the application server.

> **Note:** The packaged application does not contain any of the configuration information entered in the IBM Cognos Configuration tool and does **not** have to be rebuilt or redeployed should you wish to make configuration changes. Make and save the appropriate changes, then stop and restart the application server instance for the changes to be recognized.
>
> It does, however, contain a reference link to the actual IBM Cognos 8 installation directory, and you should not manually rename or move the Cognos 8 install. Since the IBM Cognos 8 install path is embedded in the application, it should not be used to deploy into multiple application server installs or the one-to-one relationship will not be maintained.

The Wizard can be initiated by selecting the Build Application Files menu item located in the Actions menu.

Example: Initiating the Build Application Wizard



6.4.2 Select the Application Archives to be Built

The first step of the wizard allows you to select the type of application that you are building. The options may vary depending on the IBM Cognos 8 components that you have installed. The main application, "Cognos 8" represents either or both the Content Manager and Application Tier Components.

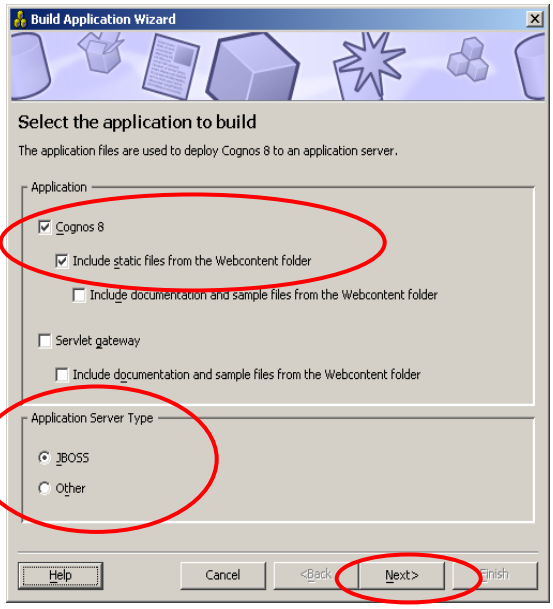
If you are going to use the application server as a Web Server and service the IBM Cognos 8 static content (images, javascripts, etc) from the application server, then select the option to include the static files in the application. If you are using a separate Web Server or the Servlet Gateway, then it is not necessary to include this content and the resulting application file will be much smaller and faster to deploy.

If the Gateway component is installed, the Servlet Gateway can be selected, built and deployed to your application server to replace the Web Server and gateway combination.

You may select to build the main IBM Cognos 8 application, the IBM Cognos 8 Servlet Gateway application, or both applications.

Important: For JBoss, you **must** select the JBoss option button under the Application Server Type section, before proceeding. Otherwise, you may encounter problems deploying the resulting application.

Example: Build Application Wizard Application Selection



6.4.3 Application File Type, Location and Context Root

If you have elected to build the main IBM Cognos 8 application file, you will be presented with a number of options.

You may select a file type. JBoss supports the EAR file, WAR file and the Expand to folder options.

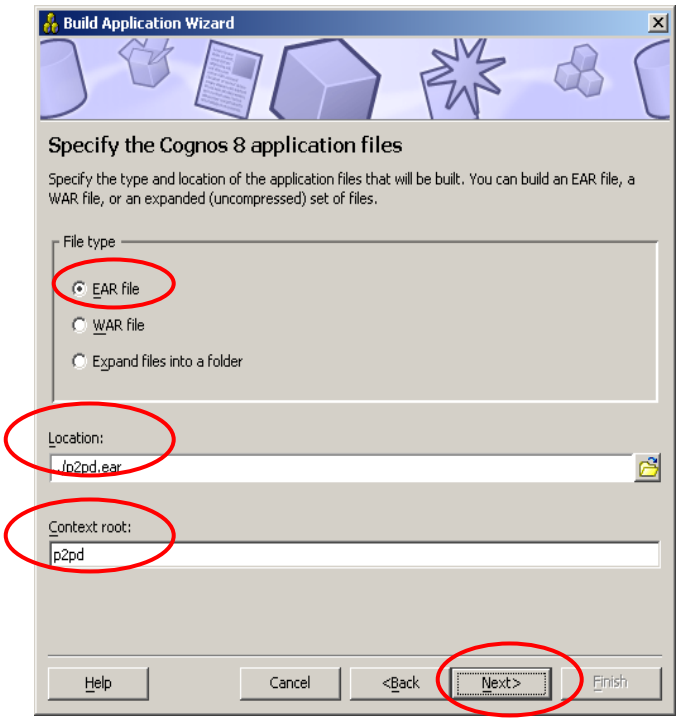
> **Note**: If you intend to use the Expand to folder option when building the p2pd application, you must include the .war extension in the folder name. When building the application, navigate to the <jboss-4.0.4-install-dir>\server\<instance_name>\deploy folder and create a folder called p2pd.war. This is where the application will reside.

The Location entry represents the path and filename of the application file that will be created by the wizard.

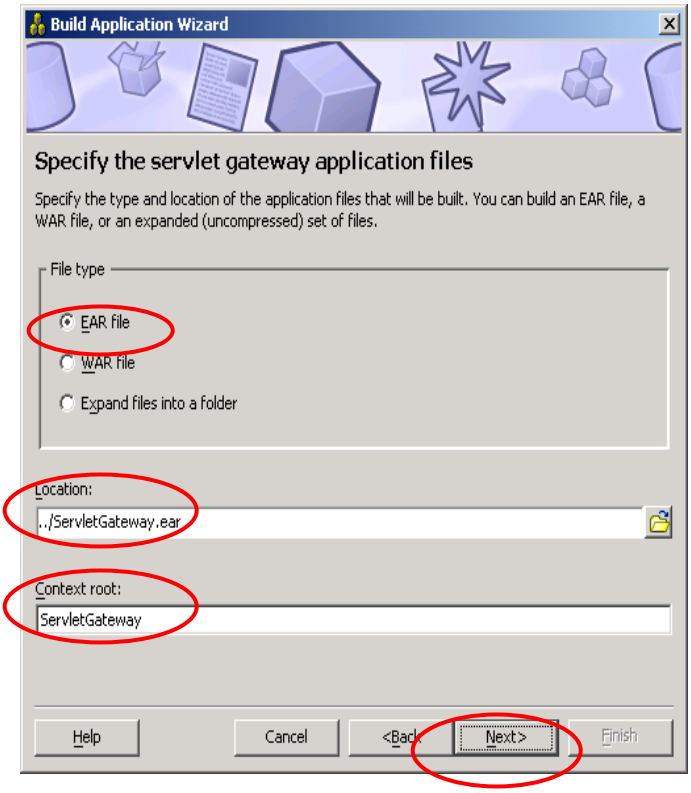
If necessary, you may also change the context root value. The context root value for the IBM Cognos 8 application must be consistent across your entire install, if you are performing a distributed install. In addition, the value entered here must match the value entered in the URI entries on the IBM Cognos Configuration tool, as well as be identical to the context root value that you enter when deploying the application file into the application server.

For EAR files, you can specify the context root in the Context root box. Application servers that use WAR files will use the application file name as the context root. Application Servers using the Expand files into a folder option will use the application's folder name as its context root value.

Example: IBM Cognos 8 application file type selections



Similar to the IBM Cognos 8 application, the IBM Cognos 8 Servlet Gateway will also allow you to specify the file type, location and name of the application file, as well as the context root. Note that the context root in this case is not the same as the context root of the IBM Cognos 8 application above.



The value entered as the context root must match the value entered in the Gateway URI in the IBM Cognos Configuration tool. For example, if using ServletGateway as the context root, the Gateway URI would be:

```
http://<server_name>:<port_number>/ServletGateway/servlet/Gateway
```

Important: If deploying both the IBM Cognos 8 application and Servlet Gateway application on the same machine, do not deploy them to the same JBoss server instance. This would cause class conflicts and other errors. In order to run both applications on the same machine, you must create two separate server instances and then deploy each application to its own instance.

To run multiple server instances, you would need to modify the port numbers for various JBoss settings, otherwise you will encounter port conflicts.

Please refer to the JBoss documentation for more information on how to setup multiple instances on the same machine.

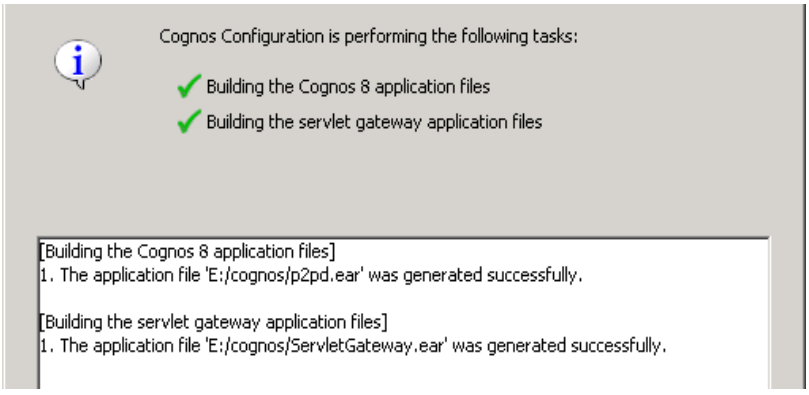
6.4.4 Build Application Files in Progress

After making the appropriate selections, the Build Application File Wizard will indicate its progress as it builds the application.

Example: Building the IBM Cognos 8 application and the Servlet Gateway application

A number of files must be copied, manipulated and packaged into the application file by the wizard so this step may take a few moments to complete based on your selections.

Example: Build of Application Files Completed



This concludes the basic portion of the setup of IBM Cognos 8 for a single server installation.

In a distributed installation, repeat the various tasks as necessary to setup IBM Cognos 8 in preparation for deployment to an application server. A JBoss install must exist and be active on each machine where IBM Cognos 8 components are to be deployed.

7 Single Server Deployment

The steps for IBM Cognos 8 setup and general environment setup should be completed prior to deployment to JBoss. Refer to the IBM Cognos 8 Installation and Configuration Guide for more information.

7.1 Deploy IBM Cognos 8

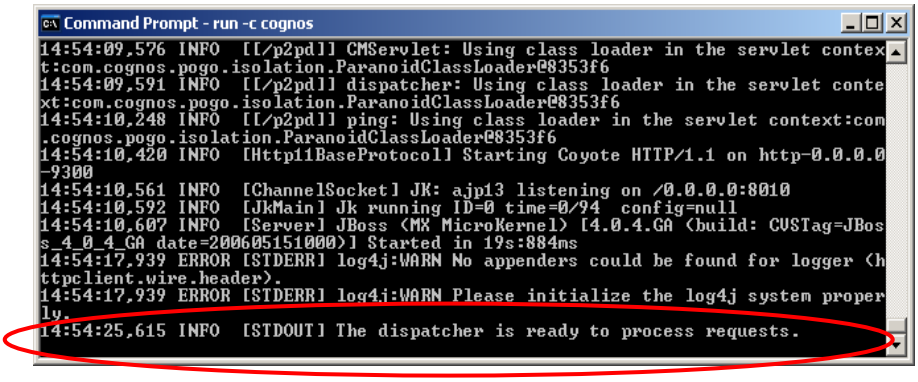
The following steps assume you have already prepared the IBM Cognos 8 application using the Build Application Wizard in IBM Cognos Configuration.

The following steps use the default application name, p2pd. The context root can be changed when generating the EAR file, the WAR file or application directory. Just remember to change this in your IBM Cognos Configuration, as well.

- Place the p2pd application in the <jboss-4.0.4-install-dir>\server\<instance_name>\deploy folder. JBoss will automatically detect the new application and start it.

  Tip: If you are modifying the application (eg. changing or removing JAR files), then the Expand to folder option is best, since you will not have to rebuild it for each change. If you intend to use the Expand to folder option when building the p2pd application, you must include the .war extension in the folder name. When building the application, navigate to the <jboss-4.0.4-install-dir>\server\<instance_name>\deploy folder and create a folder called p2pd.war. This is where the application will reside.

- Start JBoss Application Server. For example, if you created an instance called cognos, use run.bat –c cognos. IBM Cognos 8 is ready to use when you see the message: "The dispatcher is ready to process requests."



7.2 Undeploy IBM Cognos 8

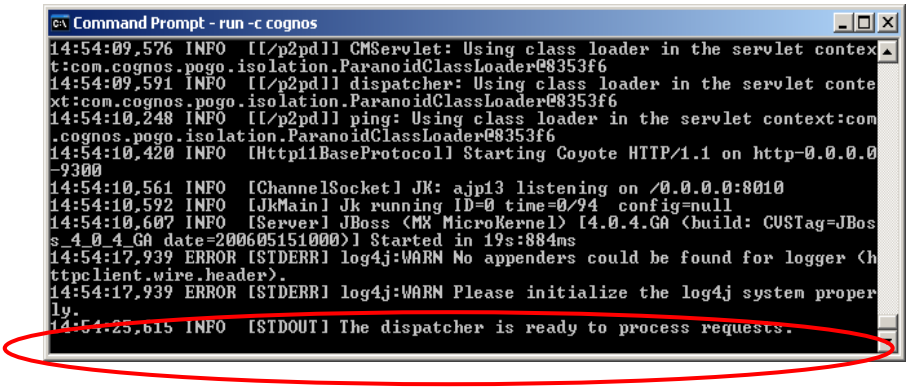
Complete the following steps to remove IBM Cognos 8 from your JBoss Application Server installation.

- Stop JBoss Application Server.
- Delete the p2pd application from the <jboss-4.0.4-install-dir>\server\<instance_name>\deploy directoy.

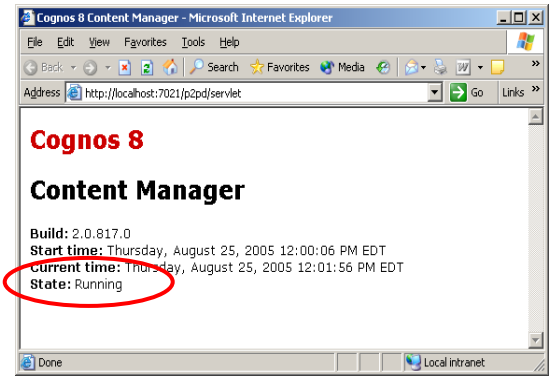
JBoss will detect that it is no longer in the list of applications.

7.3 Verify the Deployed Application

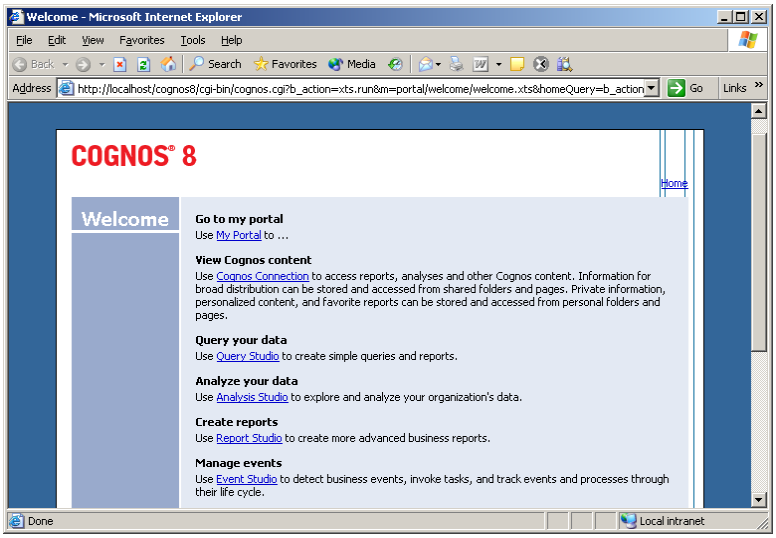
Once the deployment has completed successfully, you should see a message stating “The dispatcher is ready to process requests” in the server’s console. This indicates that CM has started and the Dispatcher for IBM Cognos 8 has been registered to CM and has started. You should also see an active BIBusTKServerMain process running when consulting the active processes on the machine. Use the appropriate utility for your operating system to verify this.



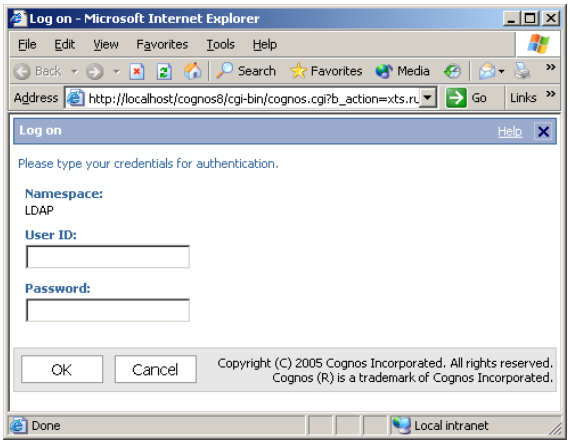
To verify that Content Manager has started, you can check the cogserver.log or open a browser and type in the Content Manager URI. The default is http://localhost:<port_number>/p2pd/servlet if you used p2pd as the context root. If the Content Store was successfully created and CM started, then you should see a page similar to the example below.



One last test to verify that the deployment was successful is to access the Portal. Open a new browser session and enter the URL for IBM Cognos Connection. The default is http://localhost:<port>/cognos8, if you are using a web server. Cognos Connection should open and you should see the Welcome page.



If a 3rd party namespace (eg. LDAP) was configured in IBM Cognos Configuration, then you would be prompted with the login page.



8 Advanced Topics

8.1 Secure Sockets Layer (SSL)

Secure Sockets Layer, or SSL, is a cryptographic protocol used for endpoint authentication and communications privacy over the Internet. Typically, only the server is authenticated (i.e. its identity is ensured) while the client remains unauthenticated. This is called one-way SSL. Two-way SSL, or mutual authentication requires public key infrastructure (PKI) deployment to clients. The protocols allow client/server applications to communicate in a secured manner.

Tip: Before you import keys and certificates to either your JBoss or IBM Cognos 8 keystores, you should back them up. For IBM Cognos 8, simply create a copy of your configuration directory. You should also backup your Content Store by exporting an archive, if you have data you wish to protect.

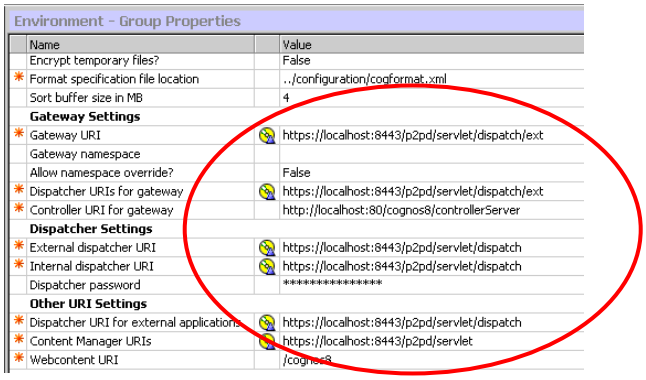
8.1.1 Configure SSL for IBM Cognos 8

Consult the IBM Cognos 8 user documentation for more information regarding SSL configuration.

1. Start IBM Cognos Configuration.
2. In the Explorer window, click Environment.
3. In the Properties window, type the appropriate values for the Internal Dispatcher URI and External Dispatcher URI values:

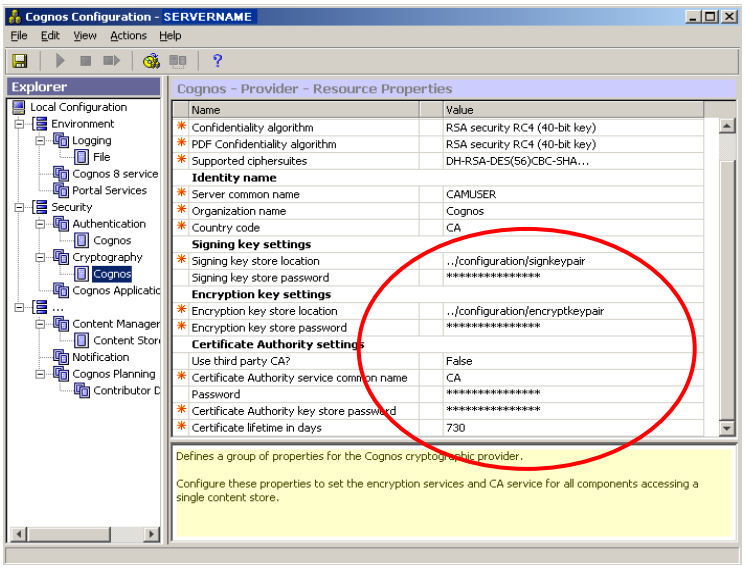
   - To configure SSL for internal connections only, for the Internal Dispatcher URI property, type https and a port for SSL communication. For the External Dispatcher URI property, type http and use the default or another available port. The ports in the Internal and External Dispatcher URIs must be different.
   - To configure SSL for external connections only, for the External Dispatcher URI property, type https and a secure port. For the Internal Dispatcher URI property, type http and use the default or another available port. The ports in the Internal and External Dispatcher URIs must be different.
   - To configure SSL for all connections, type the same URI for both the Internal Dispatcher URI and External Dispatcher URI properties. Type https and a secure port, such as 8443. In this case, the ports would be the same for the Internal and External Dispatcher URI's.

     Note: You do not have to use port 8443, the default SSL port for JBoss. You can choose any available port.



4. Configure the SSL protocol for the other environment URIs, including the Content Manager URIs, the Dispatcher URI for external applications, the Dispatcher URI for gateway and Gateway URI.

5. To use SSL, you must specify passwords for the IBM Cognos 8 encryption key stores. The passwords are found under Security -> Cryptography -> Cognos. If you are setting up multiple servers, the passwords must be the same on each server included in the configuration.



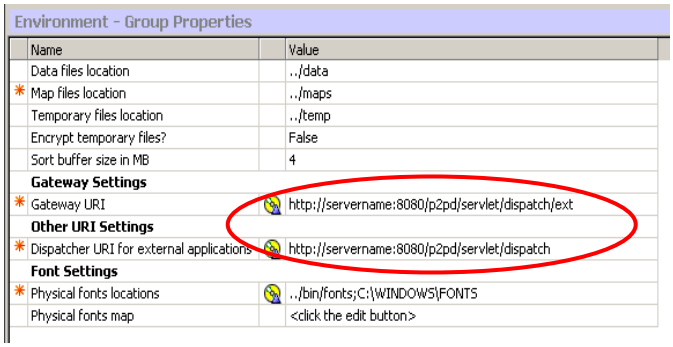
6. From the File menu, click Save.

8.1.1.1 Setup Framework Manager and SSL

If you have IBM Cognos 8 running with SSL on a server and want to configure another component, you must disable SSL before configuring the new component. This applies when you have the new component installed on a separate server. For your UNIX installs, you will have Framework Manager installed on your Windows machine. The following steps are specific to Framework Manager.

1. You must disable SSL on the IBM Cognos 8 machine when configuring a new component. Once the keys have been generated, then SSL can be enabled, and the configuration can be saved with SSL.

2. Open IBM Cognos Configuration for your Framework Manager install. Modify the Gateway URI and Dispatcher URI for external applications to the appropriate values. For example, if you're using the Dispatcher as the Gateway, set both the Gateway URI and Dispatcher URI for external applications to the Dispatcher using the HTTP port.



3. Modify the Crypto settings by entering the password you used when configuring your IBM Cognos 8 server. Save your changes. You will now have security keys.
4. Copy the exported certificates from your JBoss keystore. Refer to Steps to Set Up Shared Trust Between JBoss and IBM Cognos 8 later in this document for the steps to export certificates. Import the certificates to your local keystore (<Cognos8_location>\configuration\signkeypair\jCAKeystore).
5. Stop JBoss Application Server and change the IBM Cognos 8 configuration back to HTTPS. Save your changes in IBM Cognos Configuration. Make sure you follow the steps to enable SSL for JBoss and restart JBoss Application Server.
6. Open IBM Cognos Configuration for your Framework Manager install. Change the Gateway URI and Dispatcher URI for external applications to use HTTPS and the SSL port. Save your changes. You should now be able to communicate with your IBM Cognos 8 server using SSL from Framework Manager.
7. Close IBM Cognos Configuration.

8.1.2 Setting up SSL for JBoss

JBoss does not come with a sample keystore installed. You can use an existing keystore used by your organization, or you can create a new one. JBoss provides documentation regarding the creation of new keystores.

> **Important:** When running JBoss with SSL enabled, you may encounter a slowdown in performance response times. You should increase the memory settings in the JAVA_OPTS variable in the run.bat or run.sh scripts. Refer to your JVM documentation for more information. Also, you can refer to the JBoss Wiki for more information on tuning and slimming down JBoss. http://wiki.jboss.org/wiki/Wiki.jsp?page=JBossASTuningSliming

The following sections describe the steps to configure SSL in JBoss and Shared Trust between JBoss and IBM Cognos 8.

The steps are:

1. Create a Keystore using keytool
2. Generate a Certificate Signing Request (CSR)
3. Signing your CSR
4. Obtain CA Certificate
5. Import the CA Certificate to your keystore
6. Import the signed certificate to your keystore
7. Enable SSL in JBoss
8. Set Up Shared Trust Between JBoss and IBM Cognos 8

8.1.2.1 Create a Keystore using keytool

The keytool utility is a key and certificate management utility provided with the Java Development Kit (JDK). Users can create and administer their own public/private key pairs and certificates for use in self-authentication or data integrity and authentication services, using digital signatures.

Refer to the following link for details re. keytool.

http://java.sun.com/j2se/1.5.0/docs/tooldocs/windows/keytool.html or
http://java.sun.com/j2se/1.4.2/docs/tooldocs/solaris/keytool.html

To create a new keystore, use the –genkey option as demonstrated in the following syntax. The default key algorithm used by keytool is DSA. You must set the key algorithm to RSA using the following syntax.

```
keytool -genkey -keystore keystore_file -alias alias_name -keyalg rsa –
storepass password
```

You will then be prompted for the relevant information to include in the alias, such as your name, organizational unit, organization, city, state or province and country code. You also have the option to include this information at the command line using -dname. Refer to the example below.

Creating a keystore - Example for Windows:

```
C:\jdk1.5.0_05\bin>keytool -genkey -keystore C:\jboss-
4.0.4.GA\server\cognos\conf\mykeystore.jks -alias c8test -keyalg rsa
Enter keystore password:  password
What is your first and last name?
  [Unknown]:  Cognos user
What is the name of your organizational unit?
  [Unknown]:  Cognos
What is the name of your organization?
  [Unknown]:  cognos.com
What is the name of your City or Locality?
  [Unknown]:  Ottawa
What is the name of your State or Province?
  [Unknown]:  Ontario
What is the two-letter country code for this unit?
  [Unknown]:  CA
Is CN=Cognos user, OU=Cognos, O=cognos.com, L=Ottawa, ST=Ontario, C=CA correct?
  [no]:  yes
Enter key password for <c8test>
        (RETURN if same as keystore password):
```

8.1.2.2 Generate a Certificate Request

You will need to generate a certificate request to send to your Certificate Authority to get a signed certificate. This is part of the required steps to form a certificate chain. Use the following syntax:

```
keytool -certreq -alias alias_name -file cert_req_file_name –keystore
keystore_file -storepass password
```

For example:

```
C:\jdk1.5.0_05\bin>keytool -certreq -alias c8test -file certreqjb.cer -keystore
C:\jboss-4.0.4.GA\server\cognos\conf\mykeystore.jks -storepass password -v
Certification request stored in file <certreqjb.cer>
Submit this to your CA
```

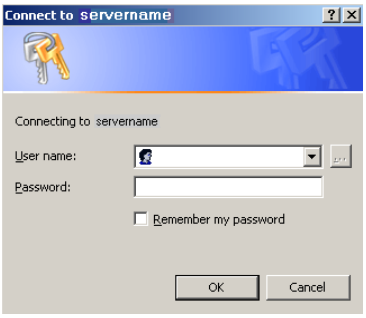
8.1.2.3 Signing Your Certificate

At this point, you must send your certificate request to a CA to have it digitally signed. It is important that you follow your CA's instructions for submitting certificate requests, and wait for them to return a signed certificate to you. As different CA authorities have different instructions for the process of applying for a signed certificate, please consult with your CA for details.

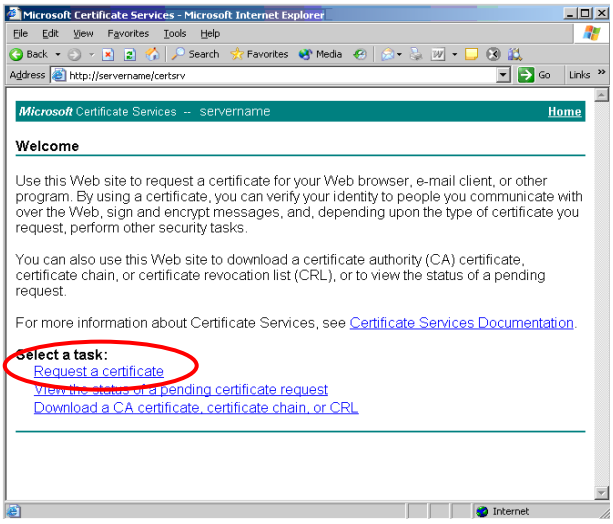
Note: For internal IBM Cognos users, the Access Manager team has setup Certificate Authorities for development and test use. **These are not available to customers or others outside of IBM.** The IP addresses, URLs and logins for these machines should **NOT** be distributed outside of IBM.

In this example, we apply for a signed certificate from the CA provided by the Access Manager team. Contact a member of the Access Manager team for the URL.

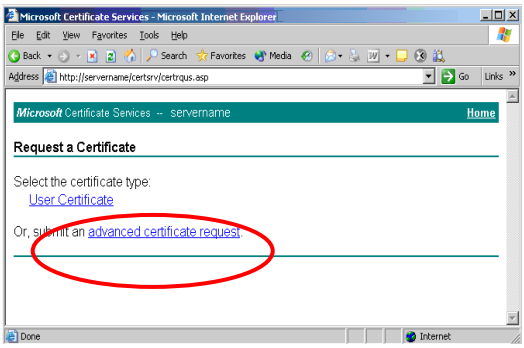
1. Login to Certificate Services.



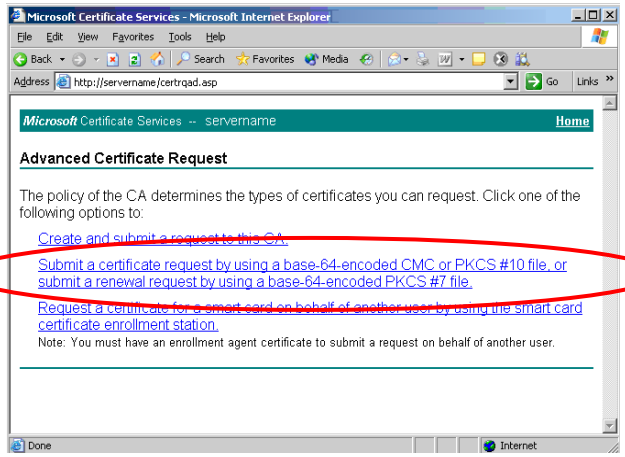
2. Select the Request a certificate link.



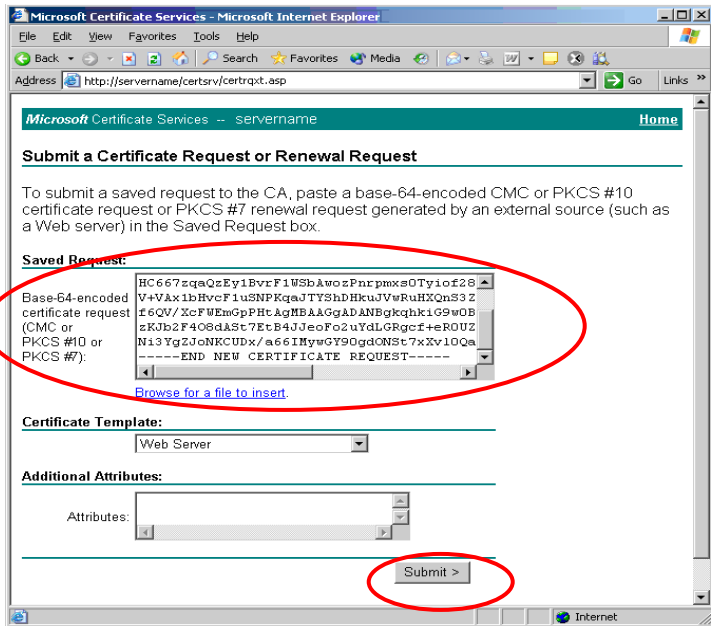
3. Under Request a Certificate, Select the Advanced certificate request link.



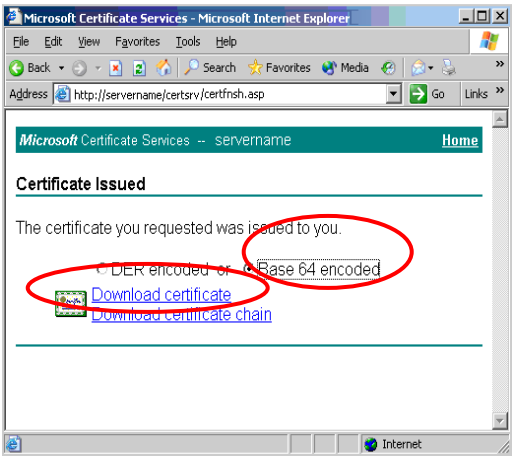
4. Under Advanced Certificate Request, Select the Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64-encoded PKCS #7 file link.



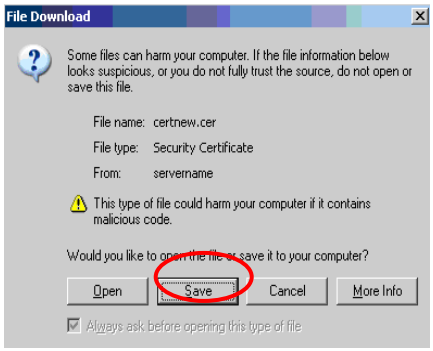
5. In the Submit Certificate Request or Renewal Request page, paste the content of your certificate request file in the Saved Request box, and Select Web Server as the Certificate Template in the dropdown list. Click the Submit button.



6. In the Certificate Issued page, select the Base 64 encoded option button, then click the Download certificate link.



Click the Save button.



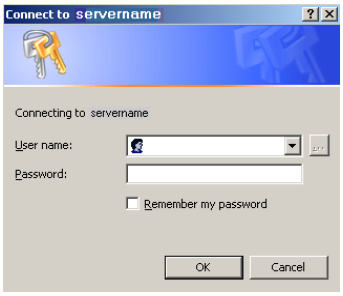
Save the file in the <*jboss-4.0.4.GA_home*>\server\cognos\conf folder.

This is your signed certificate from a third party CA. It must be added to your JBoss keystore.

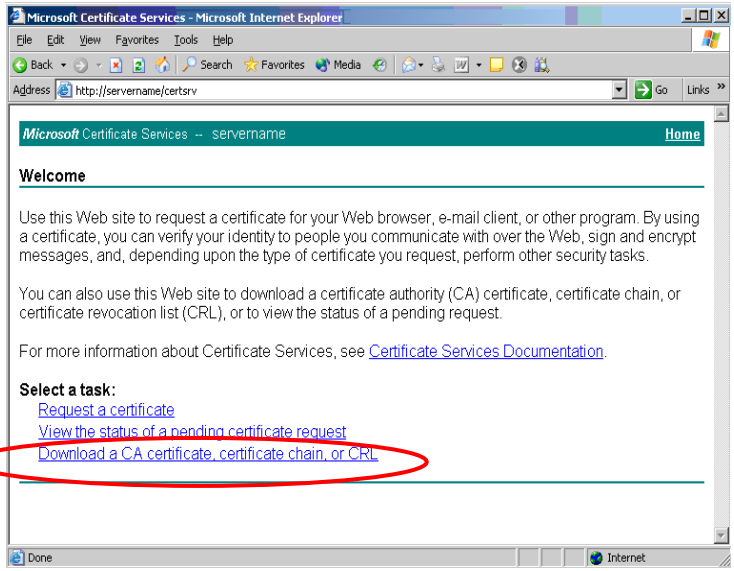
8.1.2.4 Obtain a CA Certificate

For internal IBM Cognos users, the Access Manager team has setup Certificate Authorities for development and test use. **These are not available to customers or others outside of IBM.** Contact the Access Manager team for the URL.

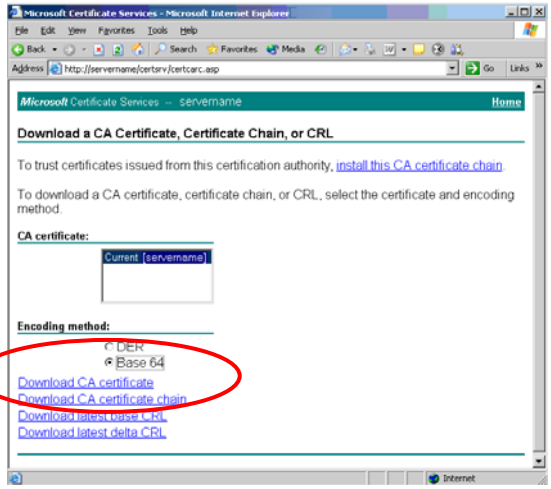
1. Connect to the certificate authority and login when prompted.



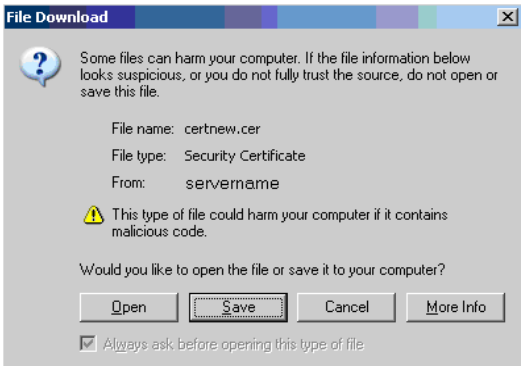
2. Click the “Download a CA certificate, certificate chain or CRL” link.



3. Select the “Base 64” option button and click the “Download CA certificate” link.



Save the file as cacert.cer in the <*jboss-4.0.4.GA_home*>\server\cognos\conf folder.



You should now have a CA root certificate which is stored as cacert.cer.

To view the contents of a certificate file, you can use –printcert, as in:

```
keytool –printcert –file keystore_file
```

For example:

```
D:\jdk1.5.0_05\bin>keytool –printcert –file D:\jboss-
4.0.4.GA\server\cognos\conf\ca.cer –v

Owner: CN=CA, O=Cognos, C=CA

Issuer: CN=CA, O=Cognos, C=CA

Serial number: 1

Valid from: Sun Aug 27 13:02:31 EDT 2006 until: Sat Aug 28 13:02:31 EDT
2010

Certificate fingerprints:

        MD5:  92:28:81:98:E4:EF:CB:75:E6:31:72:E9:96:1D:9A:15

        SHA1: 72:7A:51:F9:71:88:1F:E8:40:D5:A8:72:7B:8E:CD:AD:A1:61:34:62
```

8.1.2.5 Import a CA Certificate to your Keystore

Once you have obtained a CA certificate from your Certificate Authority, you must import it into your JBoss keystore.

Use the following syntax.

```
keytool -import -file CA_certificate_file -alias alias_name -keystore
keystore_file -storepass password -v
```

For example:

```
C:\jdk1.5.0_05\bin>keytool -import -file cacert.cer -alias ca -keystore
C:\jboss-4.0.4.GA\server\cognos\conf\mykeystore.jks -storepass password -
v

Owner: CN=common_name, DC=domain, DC=com, DC=cognos, DC=cog

Issuer: CN= common_name, DC=domain, DC=com, DC=cognos, DC=cog

Serial number: 1714e292e33551ba40f988f15547c360

Valid from: Wed Oct 26 15:03:15 EDT 2005 until: Tue Oct 26 15:10:12 EDT
2010

Certificate fingerprints:

        MD5:  0B:E1:03:82:C7:43:A1:22:88:D6:4A:09:46:86:01:1C

        SHA1: 57:A2:41:F7:5E:02:DC:DA:A3:4B:BF:03:26:DA:58:C5:C6:E6:F3:37

Trust this certificate? [no]:  yes

Certificate was added to keystore

[Storing C:\jboss-4.0.4.GA\server\cognos\conf\mykeystore.jks]
```

8.1.2.6 Add a Signed Certificate

Once you have received the response from your Certificate Authority, you will need to import the signed certificate into your keystore. You should use the same alias name used when creating the keystore. The signed certificate will replace the original self-signed certificate. Use the following syntax:

```
keytool -import -file signed_cert_file -alias alias_name -keystore
keystore_file -storepass password
```

For example:

```
C:\jdk1.5.0_05\bin>keytool -import -file certnewsign.cer –alias c8test -
keystore C:\jboss-4.0.4.GA\server\cognos\conf\mykeystore.jks -storepass
password -v

Certificate was added to keystore

[Storing C:\jboss-4.0.4.GA\server\cognos\conf\mykeystore.jks]
```

8.1.2.7 Enable SSL in JBoss

In jboss-4.0.4, the tomcat-5.5 container has its configuration in the jbossweb-tomcat55.sar/server.xml descriptor. Edit server.xml and uncomment the following section.

```
<!-- SSL/TLS Connector configuration using the admin devl guide keystore

<Connector port="8443" address="${jboss.bind.address}"
      maxThreads="100" strategy="ms" maxHttpHeaderSize="8192"
      emptySessionPath="true"
      scheme="https" secure="true" clientAuth="false"
      keystoreFile="${jboss.server.home.dir}/conf/chap8.keystore"
      keystorePass="rmi+ssl" sslProtocol = "TLS" />

-->
```

You need to replace the value for keystoreFile and keystorePass with the keystore and password you intend to use. You can also specify a new port number, if desired. For example:

```
<!-- SSL/TLS Connector configuration using the admin devl guide keystore
-->

<Connector port="8443" address="${jboss.bind.address}"
      maxThreads="100" strategy="ms" maxHttpHeaderSize="8192"
      emptySessionPath="true"
      scheme="https" secure="true" clientAuth="false"
      keystoreFile="${jboss.server.home.dir}/conf/mykeystore.jks"
      keystorePass="password" sslProtocol = "TLS" />
```

Restart the JBoss server and connect to the console using http://localhost:8443 to test the SSL connection. Your browser should complain about not trusting the signer. You should be prompted with a Security Alert dialog.

You can view the certificate to verify its contents, and that it's using the correct certificate. Click Yes to use the certificate for that browser session.

More details regarding JBoss security can be found in chapter 8 of the JBoss Admin Guide. More information can also be found in the JBoss Wiki.

8.1.2.7.1 Special note for JBoss SSL on AIX

An extra parameter is required in the server.xml file when enabling JBoss SSL on AIX.

In addition to replacing the value for keystoreFile and keystorePass, you'll also need to add an algorithm parameter: **algorithm="IbmX509"**.

For example:

```
<!-- SSL/TLS Connector configuration using the admin devl guide keystore
-->

<Connector port="8443" address="${jboss.bind.address}"
      maxThreads="100" strategy="ms" maxHttpHeaderSize="8192"
      emptySessionPath="true"
      scheme="https" secure="true" clientAuth="false"
      keystoreFile="${jboss.server.home.dir}/conf/mykeystore.jks"
      keystorePass="password" algorithm="IbmX509" sslProtocol =
      "TLS" />
```

If you don't include the algorithm parameter in server.xml configuration file, JBoss will not initialize properly and error messages will appear in the JBoss console and server.log.

8.1.2.8 Set Up Shared Trust Between JBoss and IBM Cognos 8

1. You can export keys and certificates using the keytool utility included with your JVM.

   ```
   $JAVA_HOME/bin/keytool -export -alias alias_name -file cert_file -
   rfc -keystore keystore_file –storepass keystore_password
   ```

   You should see the following message in your command prompt.

   ```
   Certificate stored in file <certfile.cer>
   ```

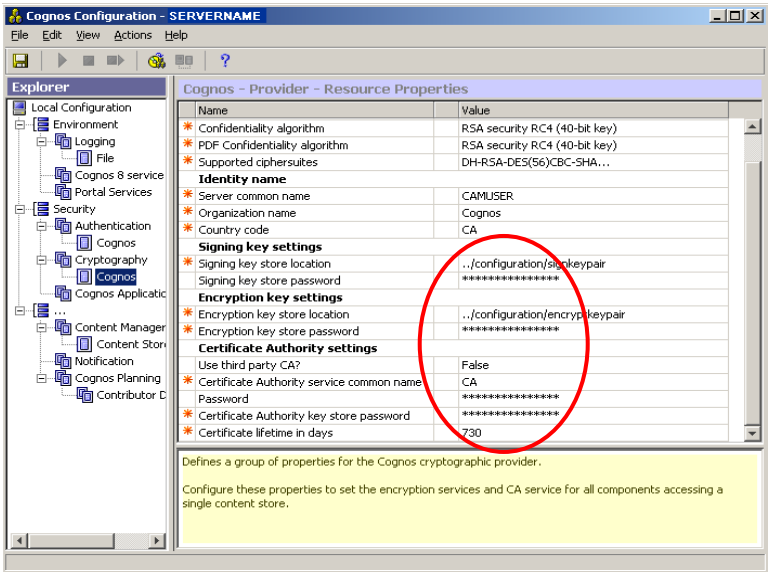
   You should export the CA certificate and the alias you created when creating the keystore. For example:

```
C:\jdk1.5.0_05\bin>keytool -export -alias ca -file ca.cer -rfc -
keystore C:\jboss-4.0.4.GA\server\cognos\conf\mykeystore.jks -
storepass password

Certificate stored in file <ca.cer>


C:\jdk1.5.0_05\bin>keytool -export -alias c8test -file c8test.cer
-rfc -keystore D:\jboss-4.0.4.GA\server\cognos\conf\mykeystore.jks
-storepass password

Certificate stored in file <c8test.cer>
```

You can find more information on the keytool utility from http://java.sun.com/j2se/1.4.2/docs/tooldocs/solaris/keytool.html or http://java.sun.com/j2se/1.5.0/docs/tooldocs/windows/keytool.html.

2. Copy the *.cer files to <cognos8_location>/bin.

3. You can import the keys and certificates using the ThirdPartyCertificateTool utility located in <cognos8_location>/bin. You must set your cryptography passwords in the IBM Cognos Configuration tool, prior to doing this.



For UNIX, use ThirdPartyCertificateTool.sh. On UNIX, you must use $ to refer to environment variables. (eg. $JAVA_HOME) Also, use forward slashes when providing the path to a file.

For Windows, use ThirdPartyCertificateTool.cmd. On Windows, you must use % to refer to environment variables. (eg. %JAVA_HOME%) Also, use backward slashes when providing the path to a file.

```
ThirdPartyCertificateTool.sh -T -i -r cert_file -k
<cognos8_location>/configuration/signkeypair/jCAKeystore -p
your_password
```

You should see a message similar to the following in your command prompt:

```
Using /system_1/java/1.5.0_05/bin/java
```

```
Loaded CA certificate: 'CN=server.cognos.com, OU=FOR TESTING ONLY,
O=MyOrganization, L=MyTown, ST=MyState, C=US'.

Stored CA certificate(s).
```

Import the certificate files that were exported from the JBoss keystore. An example follows. You can ignore the log4j warning.

```
C:\cognos\c8\bin>ThirdPartyCertificateTool.bat -T -i -r cacert.cer
-k C:\cognos\c8\configuration\signkeypair\jCAKeystore -p password

Looking in: C:\jdk1.5.0_05\bin...

Executing:

C:\jdk1.5.0_05\bin\java.exe
com.cognos.accman.jcam.utilities.ThirdPartyCertificateTool -T -i -
r cacert.cer -k C:\cognos\c8\configuration\signkeypair\jCAKeystore
-p password

log4j:WARN No appenders could be found for logger
(Trace.CAM.CRP.jcam).

log4j:WARN Please initialize the log4j system properly.

Loaded CA certificate:
'DC=cog,DC=cognos,DC=your_domain,DC=server,CN=name'.

Stored CA certificate(s).


C:\cognos\c8\bin>ThirdPartyCertificateTool.bat -T -i -r ca.cer -k
C:\cognos\c8\configuration\signkeypair\jCAKeystore -p password

Looking in: C:\jdk1.5.0_05\bin...

Executing:

C:\jdk1.5.0_05\bin\java.exe
com.cognos.accman.jcam.utilities.ThirdPartyCertificateTool -T -i -
r ca.cer -k C:\cognos\c8\configuration\signkeypair\jCAKeystore -p

 password

log4j:WARN No appenders could be found for logger
(Trace.CAM.CRP.jcam).

log4j:WARN Please initialize the log4j system properly.

Loaded CA certificate:
'DC=cog,DC=cognos,DC=your_domain,DC=server,CN=name'.

Stored CA certificate(s).


C:\cognos\c8\bin>ThirdPartyCertificateTool.bat -T -i -r c8test.cer
-k C:\cognos\c8\configuration\signkeypair\jCAKeystore -p password

Looking in: C:\jdk1.5.0_05\bin...

Executing:

C:\jdk1.5.0_05\bin\java.exe
com.cognos.accman.jcam.utilities.ThirdPartyCertificateTool -T -i -
r c8test.cer -k C:\cognos\c8\configuration\signkeypair\jCAKeystore
-p password

log4j:WARN No appenders could be found for logger
(Trace.CAM.CRP.jcam).
```

```
log4j:WARN Please initialize the log4j system properly.

Loaded CA certificate:
'C=CA,ST=Ontario,L=Ottawa,O=cognos.com,OU=Cognos,CN=Cognos user'.

Stored CA certificate(s).
```

8.1.2.9 Set Up Shared Trust Between IBM Cognos 8 and Other Servers

If you want the connection between IBM Cognos 8 and the other server to be mutually authenticated, you must also copy the certificate from your certificate authority to the trust store for IBM Cognos 8.

Steps to Copy the IBM Cognos 8 certificate to another Server

1. Go to the <Cognos8_location>/bin directory.
2. Extract the IBM Cognos 8 certificate using the ThirdPartyCertificateTool found in the IBM Cognos 8 bin directory. Type the appropriate command for the OS you are using.

   UNIX:

   ```
   ThirdPartyCertificateTool.sh -E -T -r destination_file –k
   c8_location/configuration/signkeypair/jCAKeystore -p password
   ```

   Windows:

   ```
   ThirdPartyCertificateTool.bat -E -T -r destination_file –k
   c8_location\configuration\signkeypair\jCAKeystore -p password
   ```

   For example:

   To export the CA certificate from the IBM Cognos 8 keystore, use the following syntax. (You can ignore the log4j warning.)

   ```
   D:\cognos\c8\bin>ThirdPartyCertificateTool.bat -E -T -r ca.cer -k
   D:\cognos\c8\configuration\signkeypair\jCAKeystore -p password

   Looking in: D:\jdk1.5.0_05\bin...

   Executing:

   D:\jdk1.5.0_05\bin\java.exe
   com.cognos.accman.jcam.utilities.ThirdPartyCertificateTool -E -T -
   r ca.cer -k D:\cognos\c8\configuration\signkeypair\jCAKeystore -p
   password

   log4j:WARN No appenders could be found for logger
   (Trace.CAM.CRP.jcam).

   log4j:WARN Please initialize the log4j system properly.

   The CA certificate was successfully exported.
   ```

3. Import the certificate to the trust store on your server. For information on updating the server trust store, see the documentation for your server.

   To import the IBM Cognos 8 CA certificate into the JBoss keystore, use the following syntax.

   ```
   D:\jdk1.5.0_05\bin>keytool -import -alias ca -file D:\jboss-
   4.0.4.GA\server\cognos\conf\ca.cer
   ```

```
Enter keystore password:  password

Owner: CN=CA, O=Cognos, C=CA

Issuer: CN=CA, O=Cognos, C=CA

Serial number: 1

Valid from: Sun Aug 27 13:02:31 EDT 2006 until: Sat Aug 28
13:02:31 EDT 2010

Certificate fingerprints:

       MD5:  92:28:81:98:E4:EF:CB:75:E6:31:72:E9:96:1D:9A:15

       SHA1:
       72:7A:51:F9:71:88:1F:E8:40:D5:A8:72:7B:8E:CD:AD:A1:61:34:62

Trust this certificate? [no]:  yes

Certificate was added to keystore
```

8.2 Web Server plug-ins

Web Server plug-ins are modules that you add to your third-party Web server installation and configure to enable interactions between the Application Server and applications running on Apache HTTP Server.

Refer the JBoss documentation for more information on how to utilize plug-ins with JBoss.

More information on this topic may be added in a future update.

8.3 Clustering

JBoss clustering is not supported in IBM Cognos 8.

9 Application Server References / Resources

9.1 Common commands / Utilities

To enable debug logging in JBoss, add -Djavax.net.debug=all to the JAVA_OPTS variable in the run script.

9.2 Troubleshooting (Application Server Logs)

Log files for server instances can be found in the server directory structure under the JBoss root.

<*jboss_install_directory*>\server\<*server_name*>\log

9.3 Web Sites

http://www.jboss.org
http://www.jboss.com

JBoss Application Server information:
http://labs.jboss.com/portal/jbossas

JBoss Application Server Downloads:
http://labs.jboss.com/portal/jbossas/download

JBoss Wiki:
http://jboss.org/wiki/Wiki.jsp

JBoss Issue Tracker:
http://jira.jboss.com/jira/secure/Dashboard.jspa

JBoss Forums:
http://www.jboss.com/index.html?module=bb

9.4 Documentation

Online documentation can be found at the JBoss website listed below.

http://labs.jboss.com/portal/jbossas/docs

The JBoss Wiki is also useful.

http://jboss.org/wiki/Wiki.jsp