HCL® Digital Experience

A Step-By-Step Guide
to Configuring an HCL® Digital Experience v9.5 Cluster

HCL® Digital Experience Support

This guide describes a comprehensive procedure for installing, configuring, and building an HCL® Digital Experience (HCL® Portal) v9.5 cluster using:

- Red Hat® Enterprise Linux v7.7
- IBM® WebSphere Application Server (WAS) v9.0.5 – 64 bit
- IBM® DB2 v11.1 – Database Server
- IBM® Directory Server v6.4 – LDAP Server
- IBM® HTTP Server v9.0.5 – Web Server

Table of Contents

Introduction

Higher Versions of HCL® Digital Experience and IBM® WebSphere Application Server
This guide is specifically written for 64-bit HCL® Digital Experience v9.5 cumulative fix 17 or a later CF and IBM® WebSphere Application Server v9.0.5. However, the same steps may apply on newer versions of HCL® Digital Experience v9.5 cumulative fixes and newer IBM® WebSphere Application Server v9.0.x fixpacks.

Windows/Unix Differences
This guide was written using Linux as the base operating system, however the steps/concepts listed in this guide are independent of operating system.

The only significant difference is that for Windows, you must use the batch file commands instead of the UNIX shell commands listed in this guide. For example:

UNIX: ./startServer.sh WebSphere_Portal

Windows: startServer.bat WebSphere_Portal

or

UNIX: ./ConfigEngine.sh cluster-node-config-cluster-setup

Windows: ConfigEngine.bat cluster-node-config-cluster-setup

Migration Considerations
This guide is targeted towards new installations of HCL® Digital Experience v9.5. Many of the steps in this guide are not required if you are migrating from a previous version of IBM® WebSphere Portal or an older HCL® Digital Experience version. An Appendix is provided an outline of migration considerations. If you are migrating from a previous version of IBM® WebSphere Portal this guide strongly recommends contacting HCL® Support to discuss migration options prior to executing the steps in this guide.

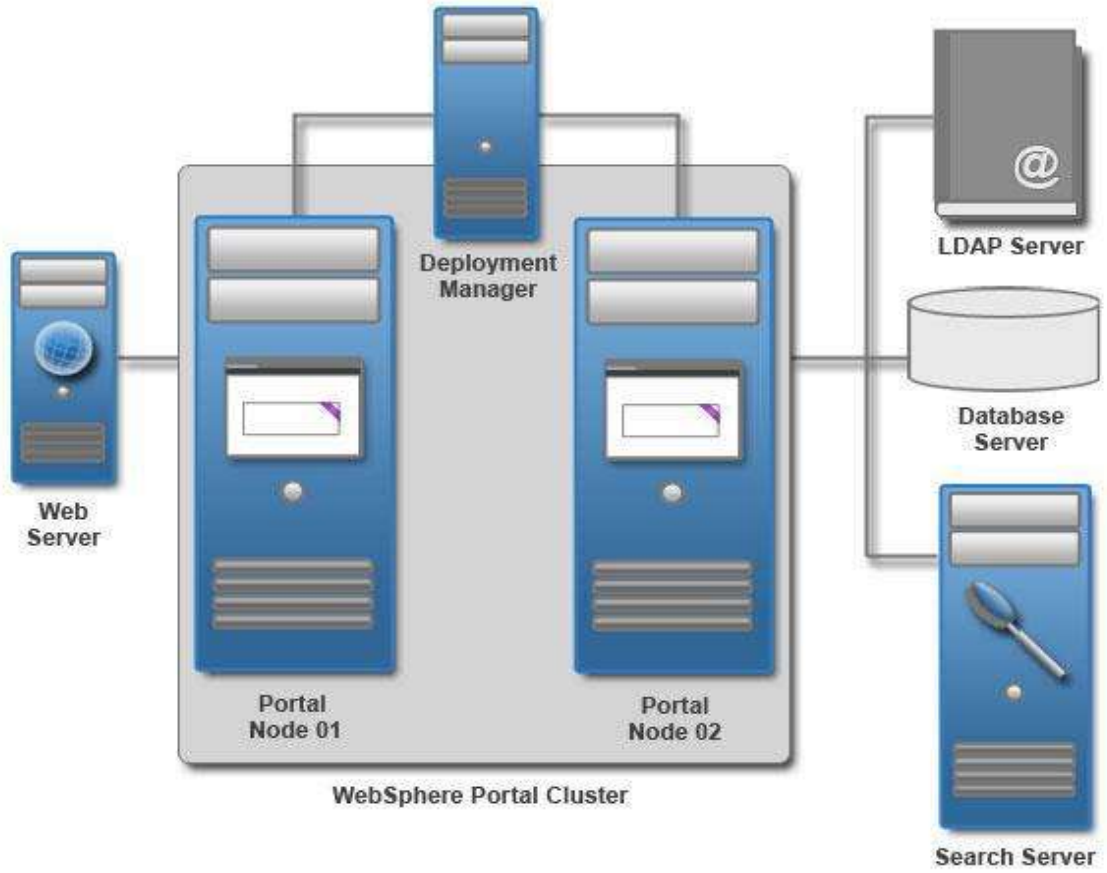
Cluster Concepts

Server – A Java Virtual Machine (JVM) that manages user applications (such as Digital Experience / Portal and Web Content Management).

Node – A logical grouping of one or more application servers. A node does not necessarily mean a single physical server.

Cell – A logical grouping of one more nodes.

Cluster – A logical grouping of one or more servers across one or more nodes. The servers are managed together and participate in workload management. Servers in a cluster share resources, such as applications. Multiple clusters can exist in a single cell, but a single cluster cannot exist across multiple cells.



An HCL® Digital Experience cluster (WebSphere Portal Cluster) with two horizontal nodes, each with two cluster members.

NOTE: There is a Remote Search Server in this illustration. This is a separate WebSphere Application server from the Portal Server.

Using this Guide

While there are numerous different ways to build a HCL® Digital Experience cluster, this guide describes the method widely considered the easiest: building a cluster with horizontal nodes and a remote Deployment Manager.

This can be achieved by following the steps in these chapters:

1. Installing HCL® Digital Experience v9.5 on the Primary Node
2. Configuring the Primary Node for a Remote Database
3. Installing and Configuring the Deployment Manager
4. Federating and Clustering the Primary Node
5. Configure the HCL® Digital Experience cluster for Federated LDAP Security
6. Installing HCL® Digital Experience cluster on an additional horizontal Node
7. Federating and Clustering an Additional Horizontal Node
8. Configuring the Cluster with an External Web Server

Appendices are provided to guide you through additional concepts not covered in the main portion of the guide. The appendices contain tasks, features, and configuration options the authors of this guide have found useful for many administrators but not required in all environments. The main portion of this guide is recommended for all HCL® Digital Experience environments.

Before You Begin

This guide does **NOT** cover the following:

- Installing IBM® DB2
- Creating multiple clusters in a single cell
- Advanced Security configuration
- Installing and Configuring IBM® Directory Server

For more information on these and other topics, visit the HCL® Digital Experience v9.5 Product Documentation:

https://help.hcltechsw.com/digital-experience/9.5/welcome/wp95_welcome.html?

To perform the tasks described in this document, you need basic HCL® Digital Experience and IBM® WebSphere Application Server knowledge and administration skills. Some steps might require the assistance of another system administrator, such as the database administrator or LDAP administrator.

Hostnames Used in This Guide
To avoid confusion, each instance of the hostnames has been replaced with a sample value that corresponds to the server it belongs to, so it is easier to understand to which server the guide is referring.

Sample Values:

Primary Portal Node - myprimaryportal.hcl.com
Secondary Portal Node – mysecondaryportal.hcl.com
Deployment Manager – mydmgr.hcl.com
Database Server – mydbserver.hcl.com
LDAP Server – myldapserver.hcl.com
IBM® HTTP Server – mywebserver.hcl.com

The following references to HCL® Digital Experience and IBM® WebSphere Application Server file paths will be used throughout the guide:

AppServerRoot - The root path of the AppServer directory, for example:

/opt/HCL/WebSphere/AppServer

PortalServer root - The root path of the PortalServer directory, for example:

/opt/HCL/WebSphere/PortalServer

wp_profile - The root path of the wp_profile directory, for example:

/opt/HCL/WebSphere/wp_profile

dmgr_profile - The root path of the dmgr profile directory, for example:

/opt/HCL/WebSphere/AppServer/profiles/dmgr01

httpRoot – The root path of the IBM® HTTP Server, for example:

/opt/HCL/HTTPServer

pluginRoot - The root path of the WebSphere Plugin directory, for example:

/opt/HCL/WebSphere/Plugins

The following references to relevant usernames and passwords will be used throughout the guide:

PortalAdminID - The Portal administrator user ID, set during HCL® Digital Experience installation.

PortalAdminPswd - The Portal administrator password, set during HCL® Digital Experience installation.

ConfigWizardID – The Configuration Wizard administrator ID, set during HCL® Digital Experience installation.

ConfigWizardPswd – The Configuration Wizard administrator password, set during HCL® Digital Experience installation.

dmgrAdminID – The Deployment Manager administrator ID, set by HCL® Digital Experience scripting

dmgrAdminPswd – The Deployment Manager administrator password, set by HCL® Digital Experience scripting

WASAdminInLDAP – The WAS administrator ID stored in the LDAP. This is set during the configuration of the Cluster for federated LDAP security.

WASPswdInLDAP – The WAS administrator password stored in the LDAP. This is set during the configuration of the Cluster for federated LDAP security.

NOTE: If you plan to configure an LDAP to your cluster, ensure the user names you choose for the *PortalAdminId* and *dmgrAdminID* values do NOT match any names in the LDAP.

Configuration Wizard Server Information

server1 – This is the name of the Configuration Wizard server. It should not be federated or added to the cluster. If the Configuration Wizard is stopped (after initial Portal installation), it can be re-started by navigating to:

AppServerRoot/profiles/cw_profile/bin

and running:

./startServer.sh server1

Chapter 1 – Installing HCL® Digital Experience v9.5 on the Primary Node

Chapter Overview

This chapter will demonstrate how to install HCL® Digital Experience v9.5 on the primary node. In this guide, the installation was completed with a graphical user interface (GUI) using the root user with installation images on a local hard drive.

This chapter contains multiple sections each performing a specific action within the IBM® Installation Manager (IIM) tool. Ensure you complete each section as outlined before proceeding to the section.

Section 1 – Installing IBM® Installation Manager

Section 2 – Installing HCL® Portal (WebSphere Portal) v8.5 Binaries only

Section 3 – Upgrading HCL® Portal (WebSphere Portal) v8.5 to Cumulative Fix (CF) 17 or a later CF

Section 4 – Upgrading HCL® Portal (WebSphere Portal) v8.5 CF17 or a later CF to HCL® Portal v9.5

Before installing HCL® Portal, ensure you review the planning documentation:
https://help.hcltechsw.com/digital-experience/9.5/plan/plan_installation.html

Section 1 - Installing IBM® Installation Manager

The IBM® Installation Manager (IIM) is a tool that you can use to install and maintain your IBM® software packages. Wizards guide you through the steps that you must take to install, modify, update, roll back, or uninstall your IBM® and/or HCL® products.

1. Open a terminal window and run: ping

   myprimaryportal.ibm.com

   where *myprimaryportal.ibm.com* is your fully qualified hostname.

2. In the same terminal window,

   run: ping localhost

   to verify that the localhost settings are properly configured on your server.

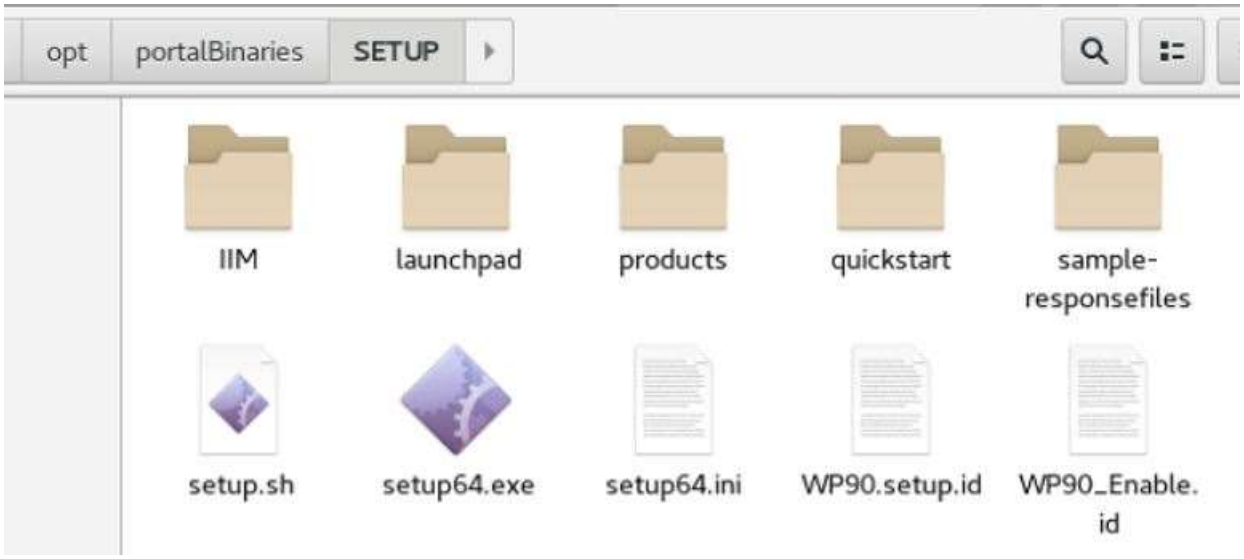
3. **Linux/UNIX environments only:** Ensure ulimit is set to 10240 or higher by running:

   ulimit -n 10240

   in the command line.

4. Unzip all .zip files provided with your HCL® Digital Experience media into a single folder. This folder will be referred to as the *installationMediaRoot* folder.

For this guide the following directory is used for the *installationMediaRoot* folder: /opt/portalBinaries/SETUP/products



5. From the HCL® Digital Experience v9.5 SETUP directory, navigate to:

   SETUP/IIM/*yourEnvironment*

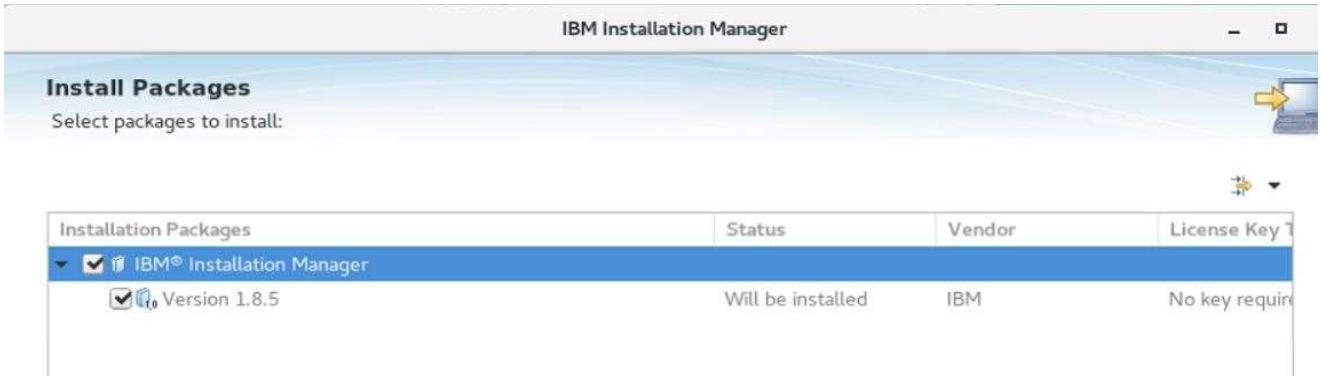
   and run

   ./install

   where *yourEnvironment* is the folder that best describes the operating system of the environment in which you are installing HCL® Digital Experience. For this guide the following is used:

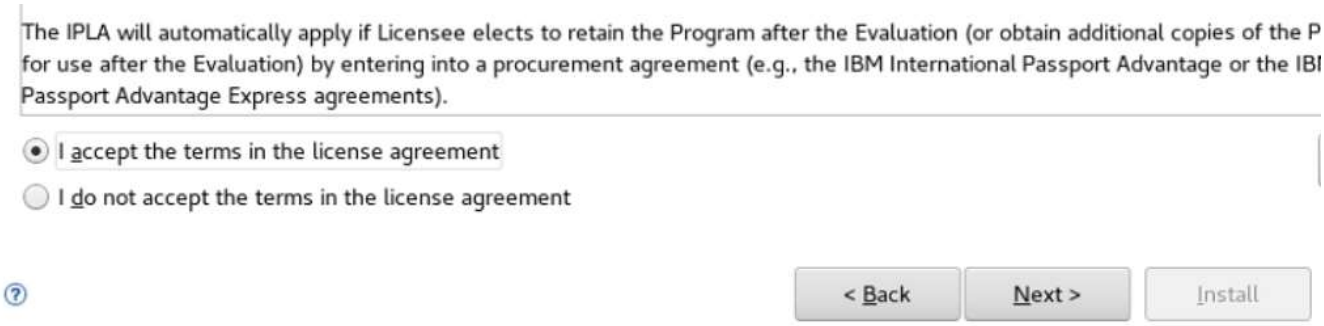
   installationMediaRoot/SETUP/IIM/linux_x86_64

The following window will appear:



6. Click **Next**.

7. Accept the license agreement and click **Next**.



8. Choose a directory in which to install IIM. This guide uses:
   /opt/HCL/InstallationManager/eclipse

   for Windows this guide recommends:
   c:\HCL\InstallationManager\eclipse

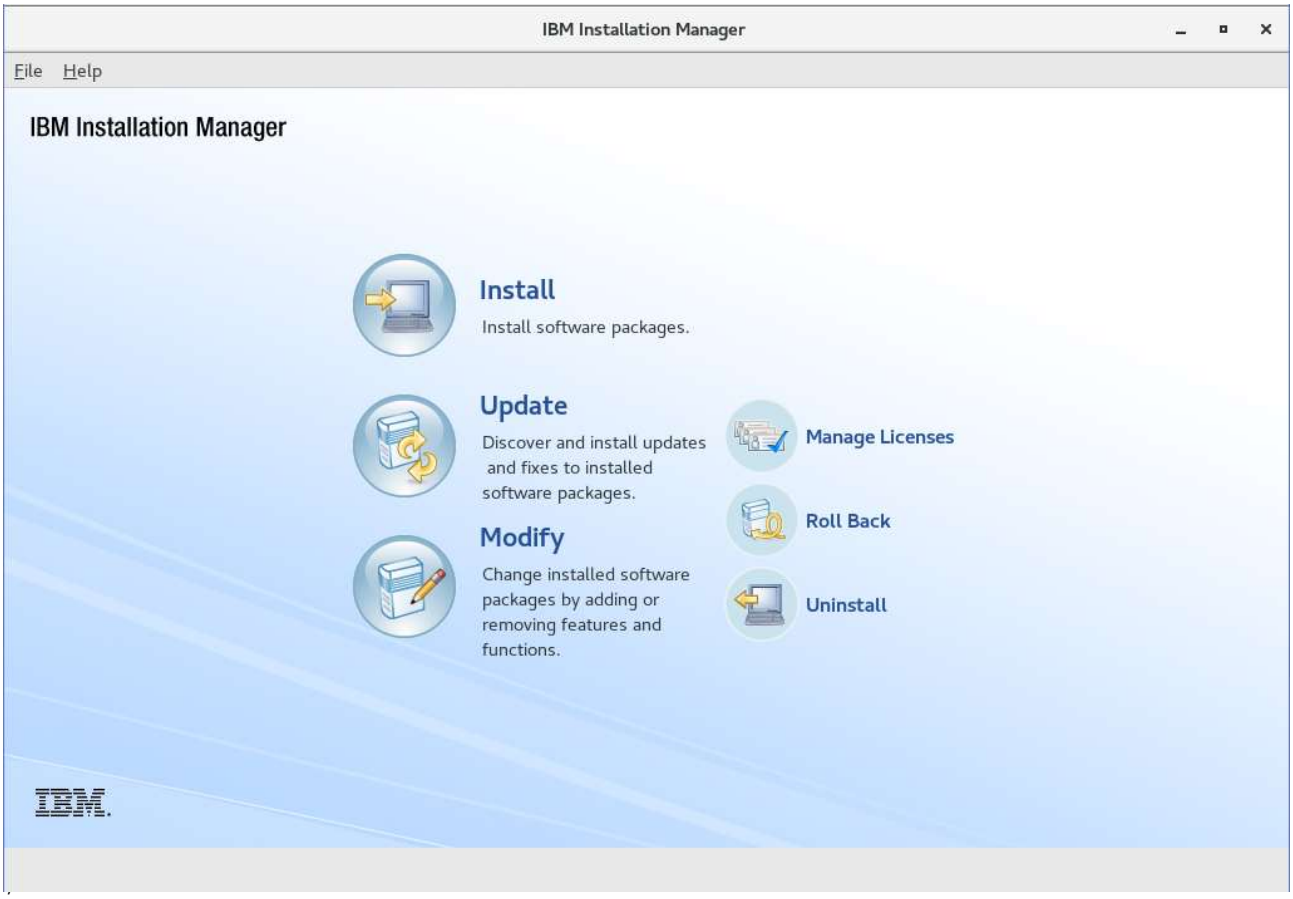
NOTE: In Windows environments, the default location will be C:\Program Files\HCL\InstallationManager. Spaces in the file path can cause problems later in the installation/configuration of HCL® Portal. This guide recommends creating a folder named "HCL" at C:\HCL or a similar location into which IIM and HCL® Portal can be installed.

9. Click **Next.**

10. On the Summary screen, click **Install** to begin the installation.

11. When the installation is complete, click **Restart Installation Manager**.

12. The following screen will appear:



At the end of this section, you have successfully installed IBM® Installation Manager 1.8.5.

Section 2 - Installing HCL® Portal (WebSphere Portal) 8.5 Binaries only

This section will cover the installation of HCL® Portal 8.5. HCL® Portal 8.5 must be installed and thereafter upgraded to HCL® Portal 9.5. It is not possible to install HCL® Portal 9.5 directly.

1. In IIM, click **File > Preferences > Repositories**

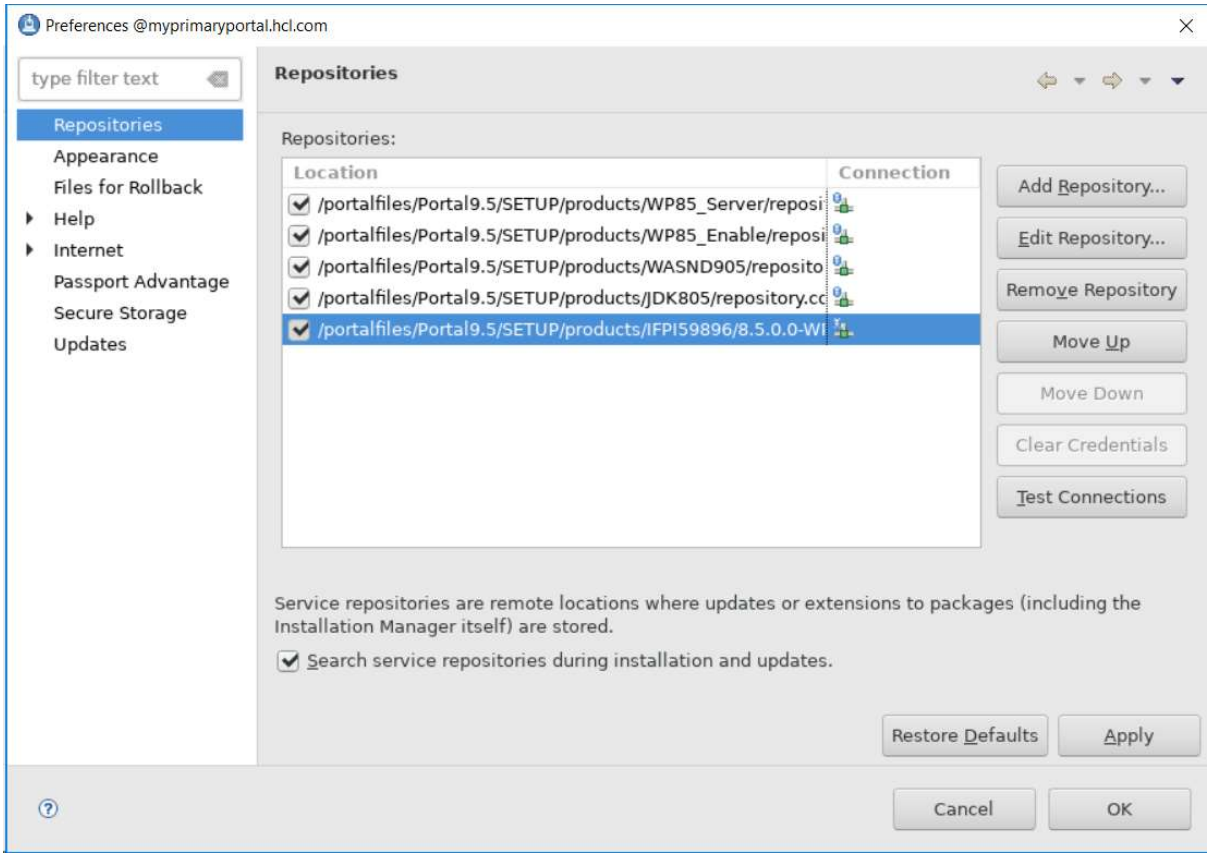
2. Click **Add Repository**, navigate to

   installationMediaRoot/WP85_Enable/repository.config

   and click **OK**.

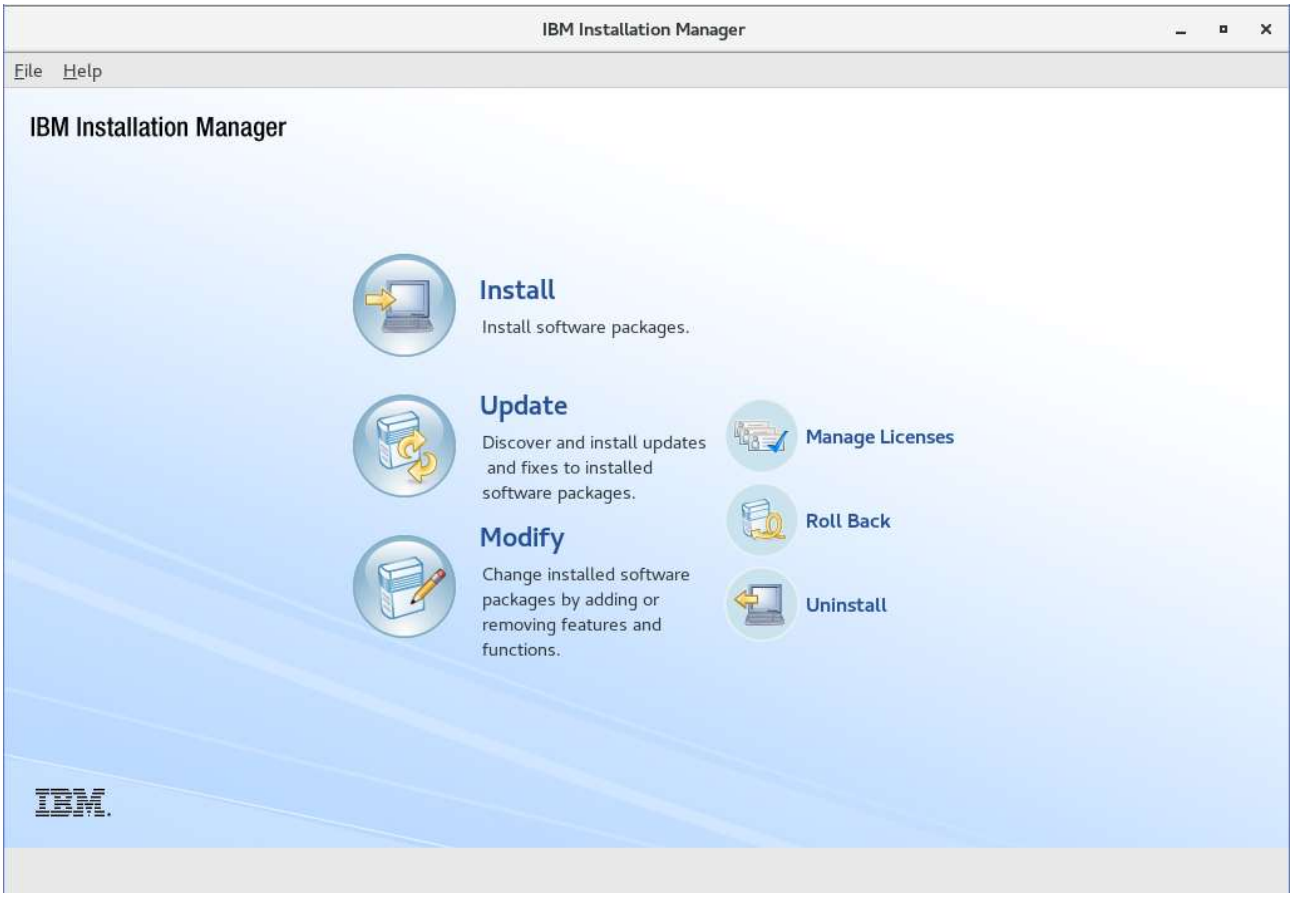
3. Repeat step 2 for the following repositories:

   installationMediaRoot/WP85_Server/repository.config
   installationMediaRoot/WASND90/repository.config
   installationMediaRoot/JDK803/repository.config
   installationMediaRoot/IFPI59896/8.5.0.0-WP-Server-PI59896.zip

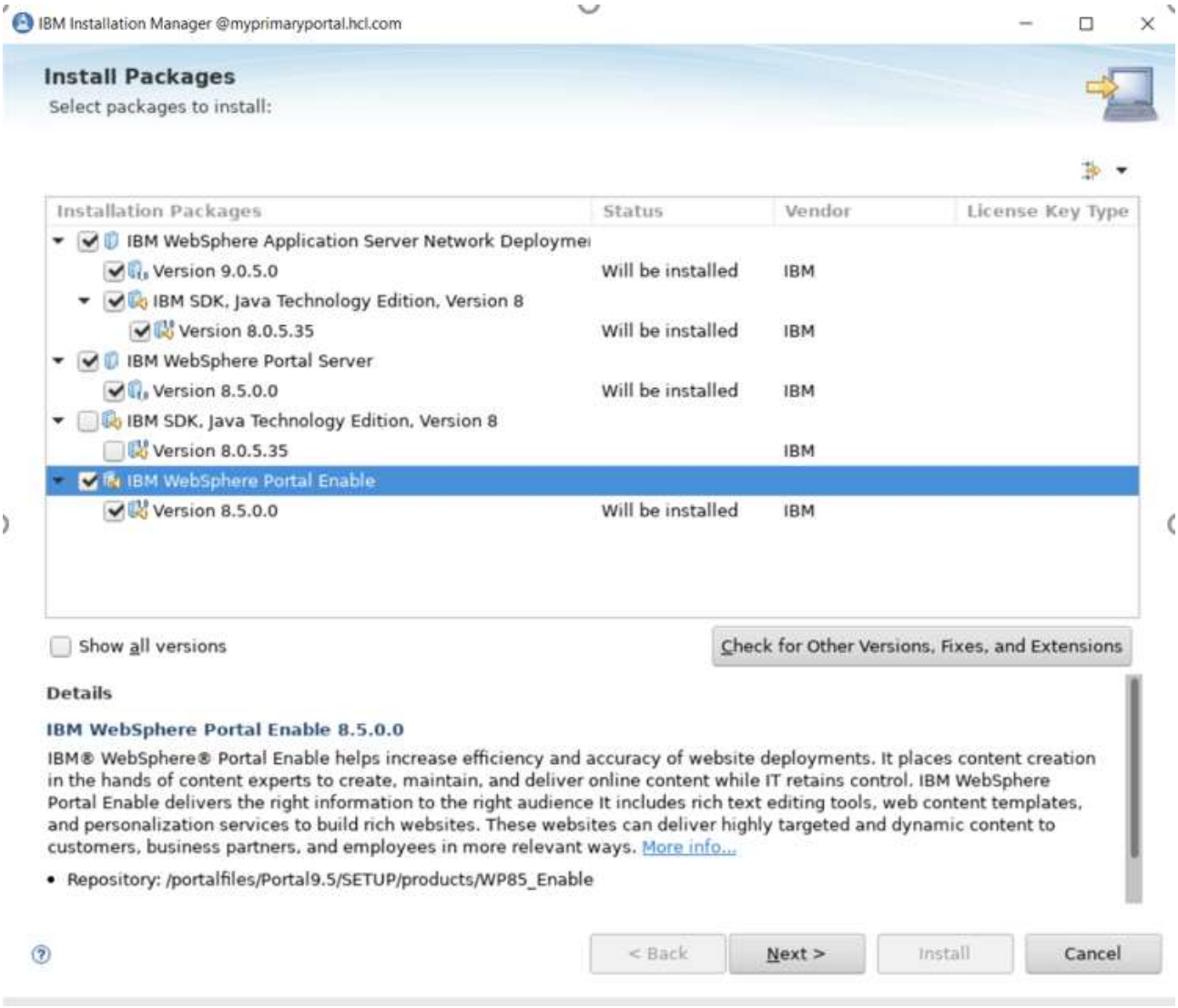


4. Ensure that all the repositories you just added are selected (i.e. there is a check mark in the box next to them) and click **Apply** then **OK**.

5. Back on the IIM Home Screen, click **Install**.

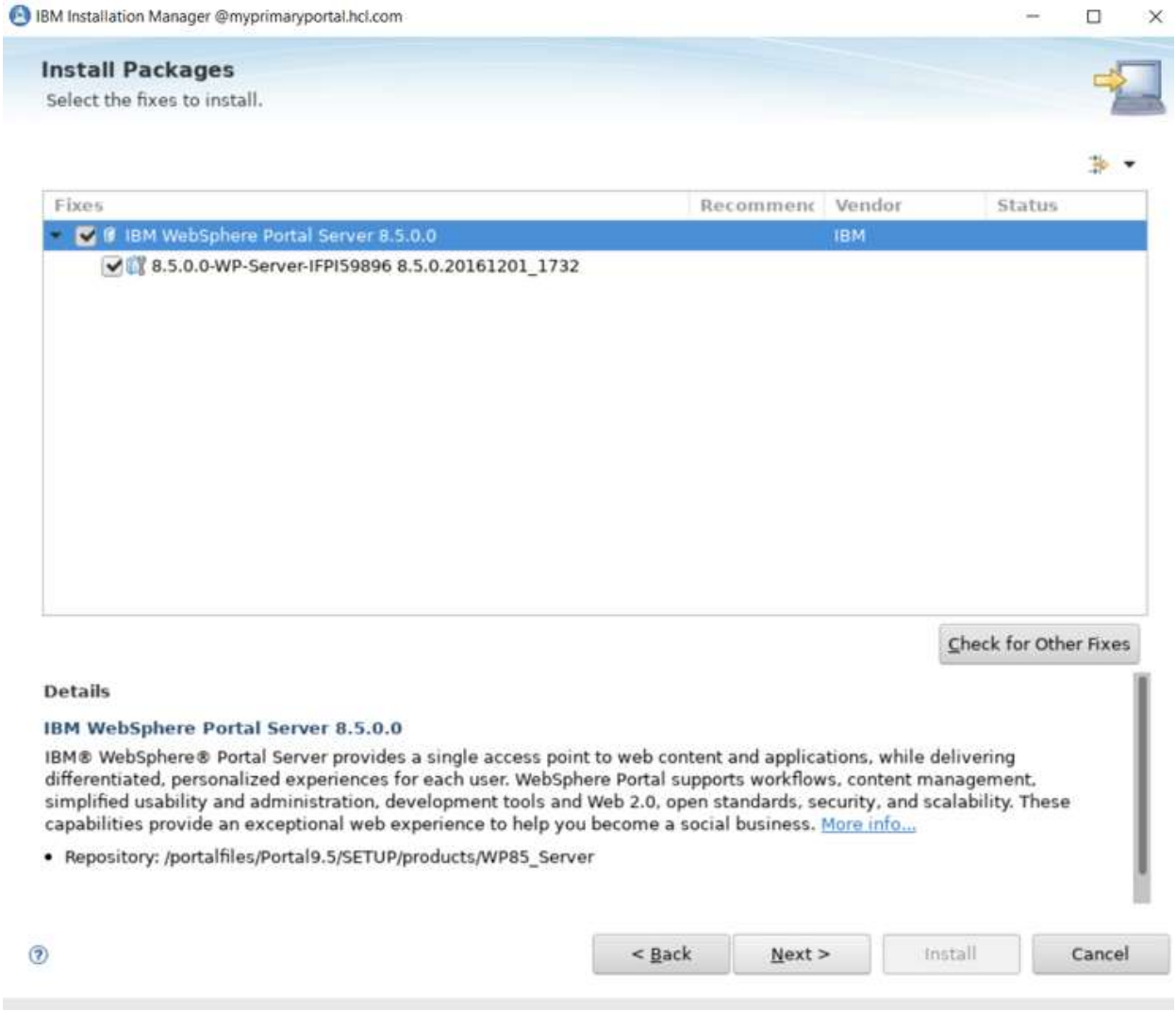


6. Check the boxes to install IBM WebSphere Application Server Network Deployment, IBM WebSphere Portal Server, and IBM WebSphere Portal Enable (or the offering you are installing, e.g. Extend, Express, etc.). IBM SDK, Java Technology Edition, Version 8 package should not be selected as it is will be automatically installed with the IBM WebSphere Application Server Network Deployment package.

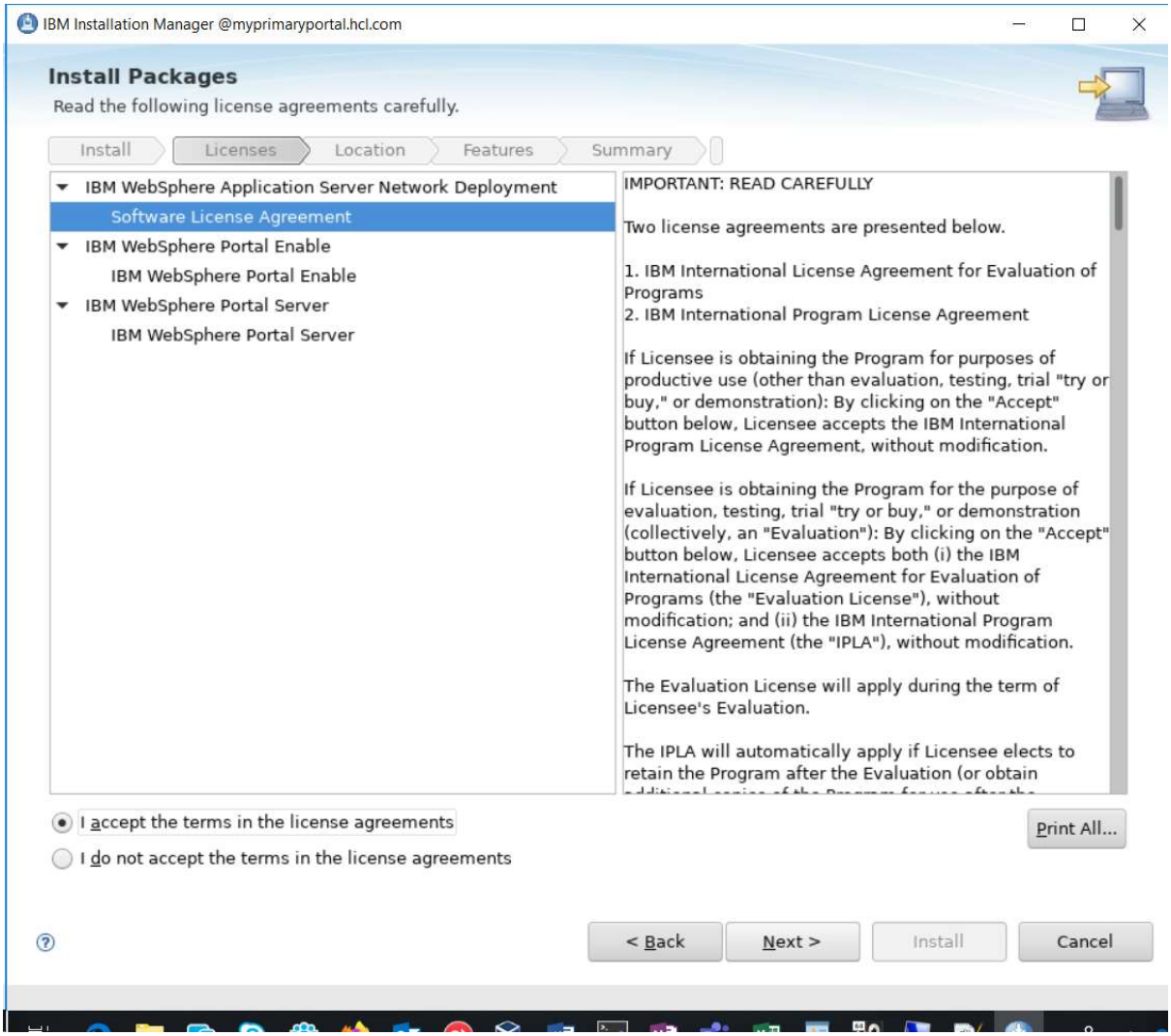


Click **Next**.

7. **Select** the iFix IFPI59896 and click **Next**

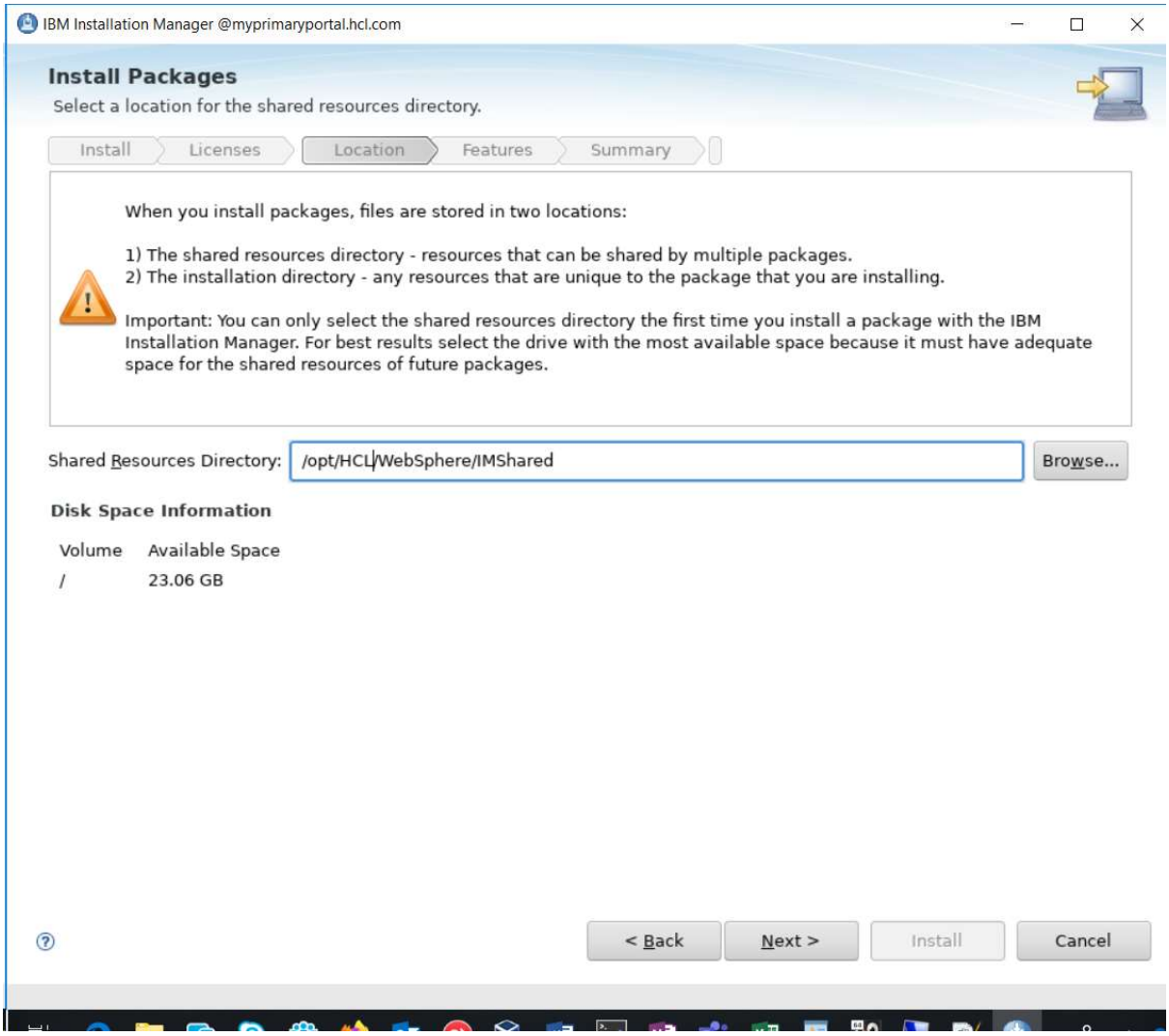


8. **Accept** license agreement and click **Next**



9. Select a location for the IIM Shared Resources Directory. This guide uses:
   /opt/HCL/WebSphere/IMShared

   for Windows this guide recommends:
   c:\HCL\WebSphere\IMShared



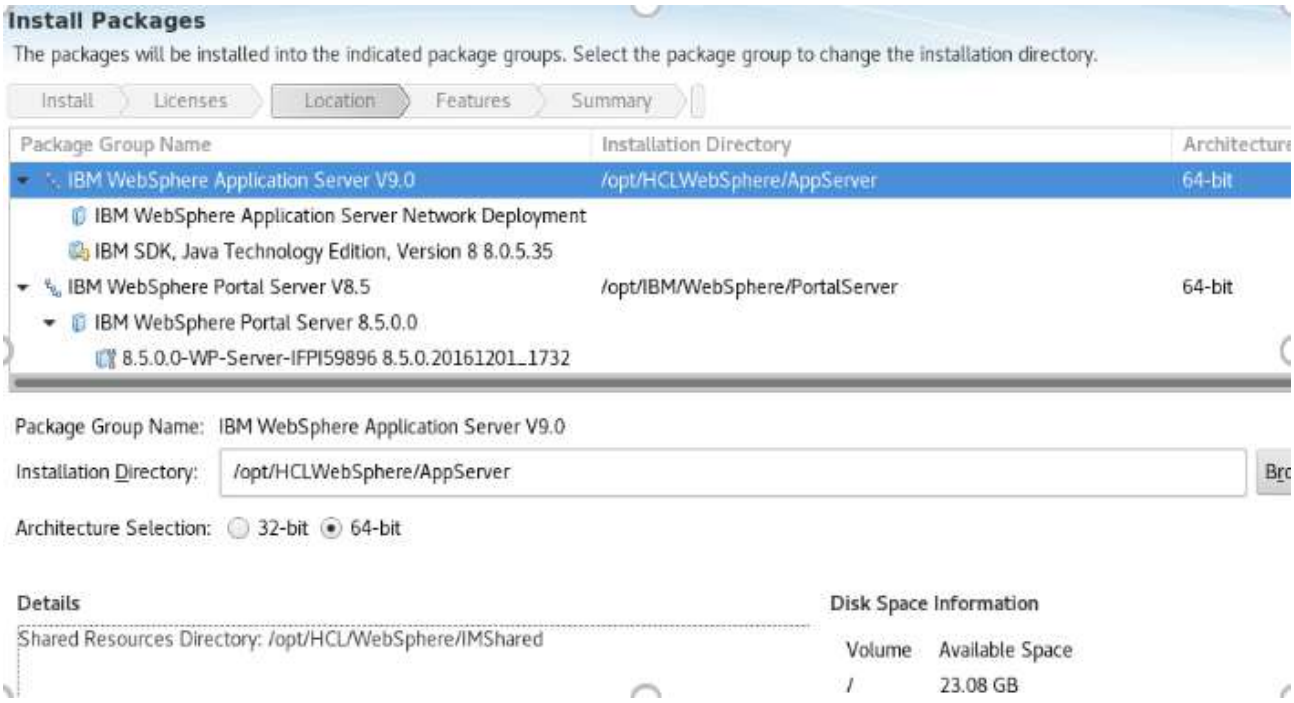
Click **Next.**

10. Click **IBM WebSphere Application Server** to set the WAS installation location. This guide uses:

    /opt/HCL/WebSphere/AppServer

    for Windows this guide recommends:

    C:\HCL\WebSphere\AppServer



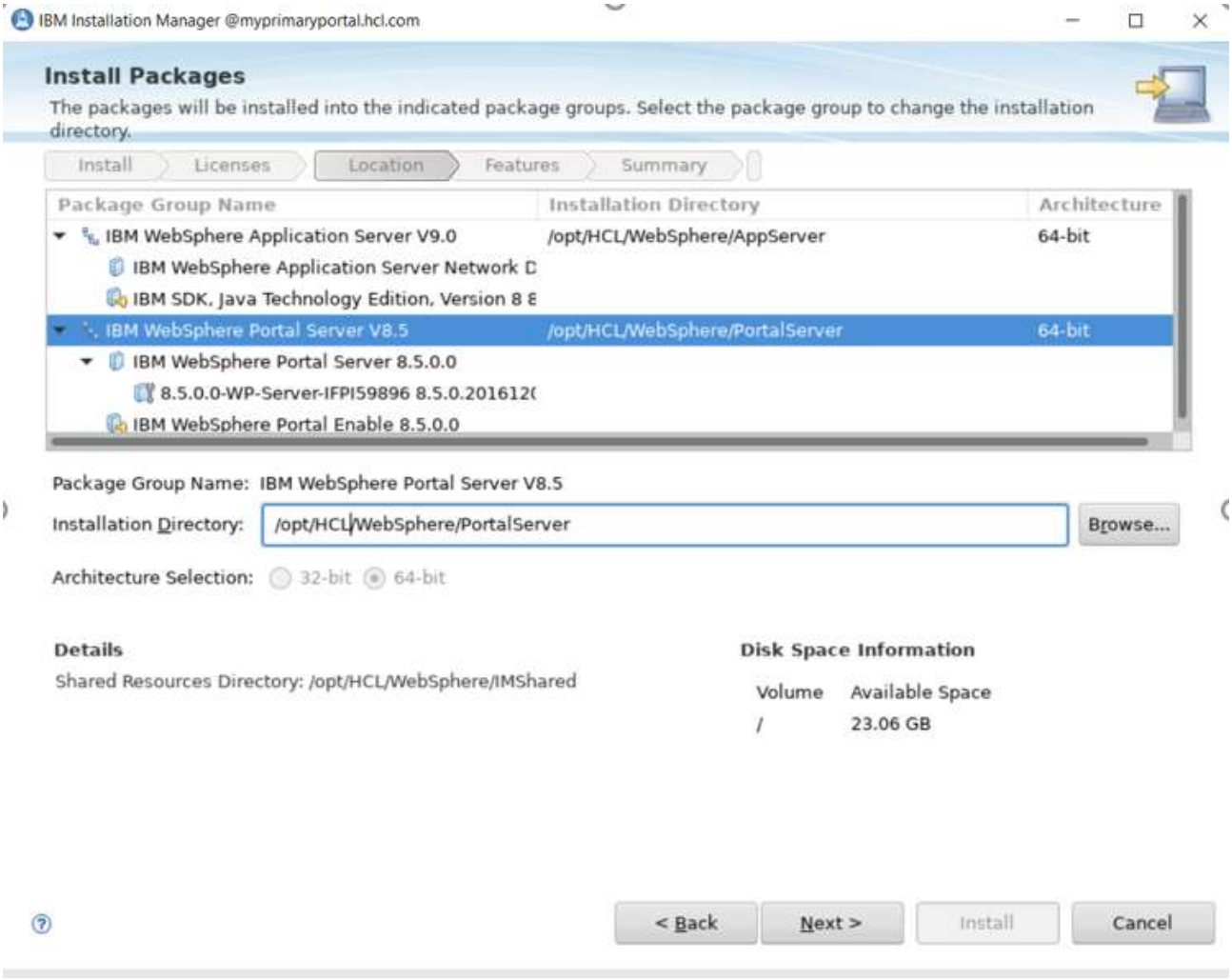
Click **Next.**

11. Click **IBM WebSphere Portal Server V8.5** to set the Portal Server installation directory:

    /opt/HCL/WebSphere/PortalServer

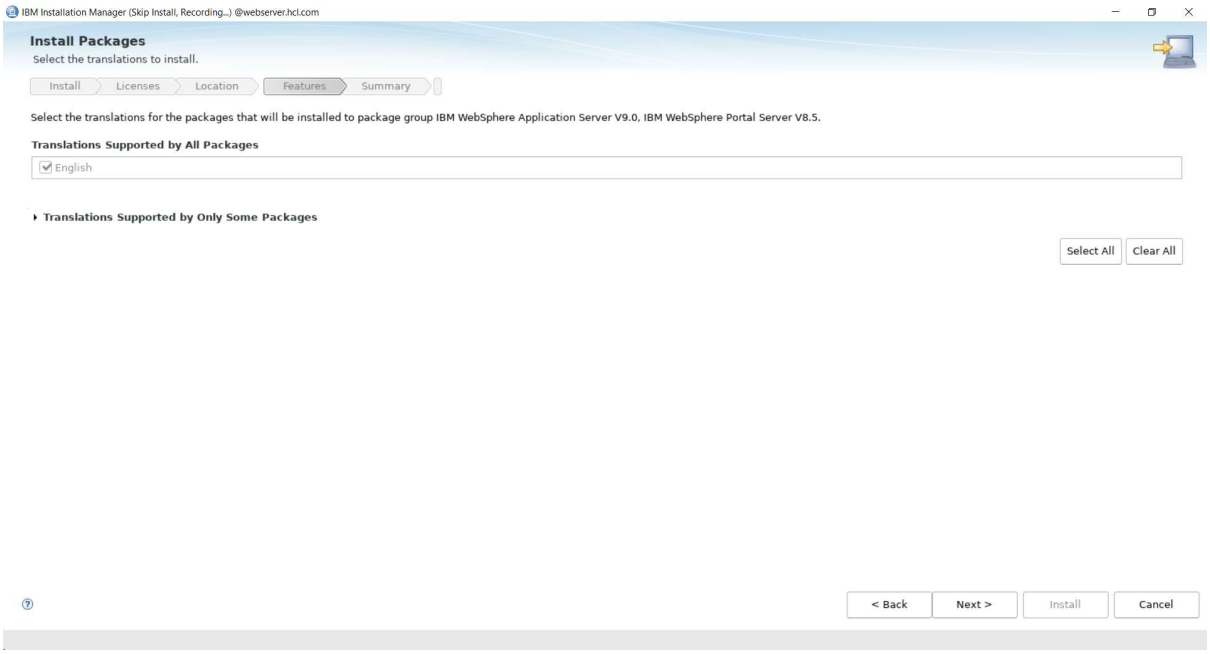
    for Windows this guide recommends:

    C:\HCL\WebSphere\PortalServer



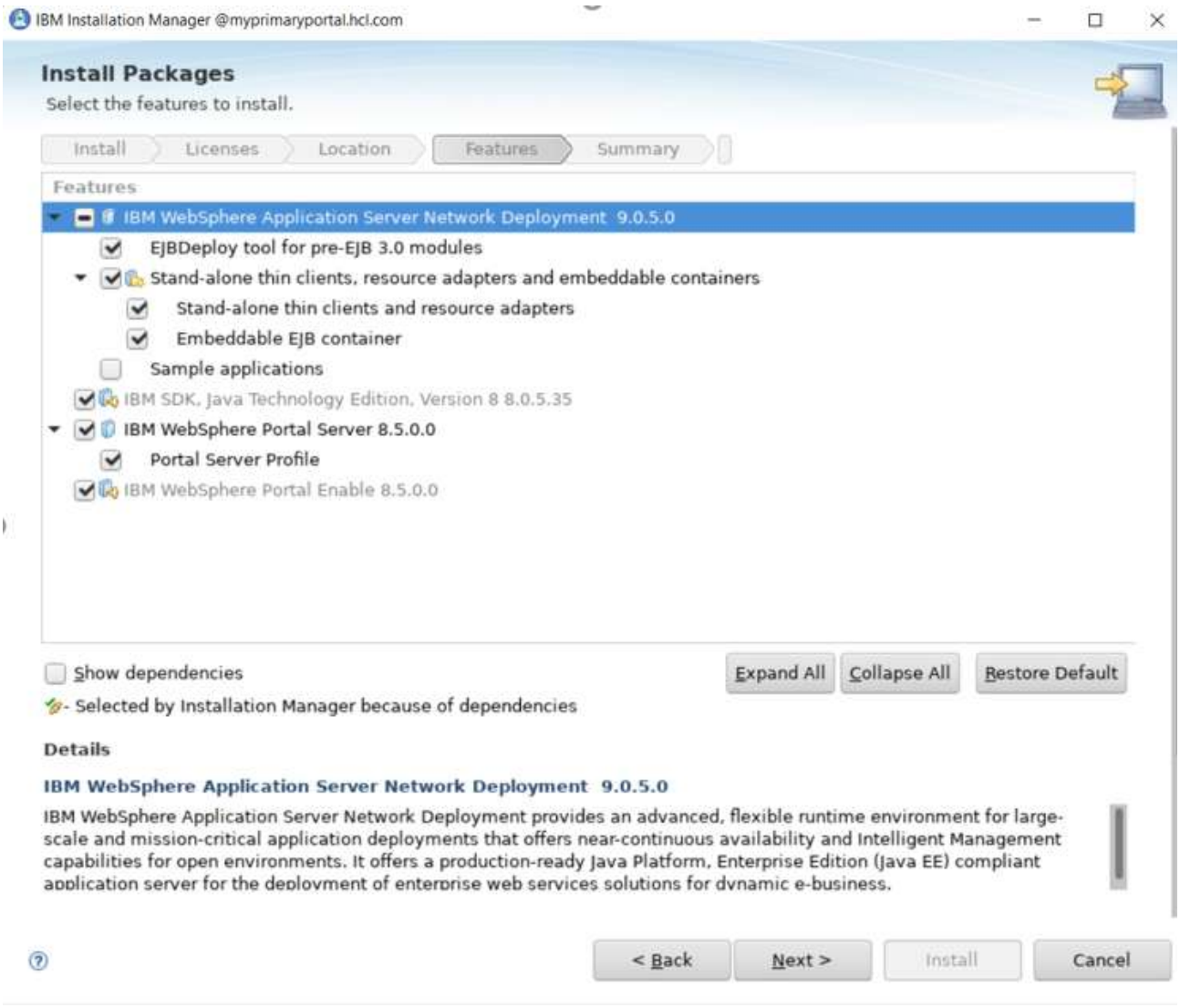
Click **Next**.

12. Select any additional language translations your environment requires. Only English was selected for this guide. Click **Next**.



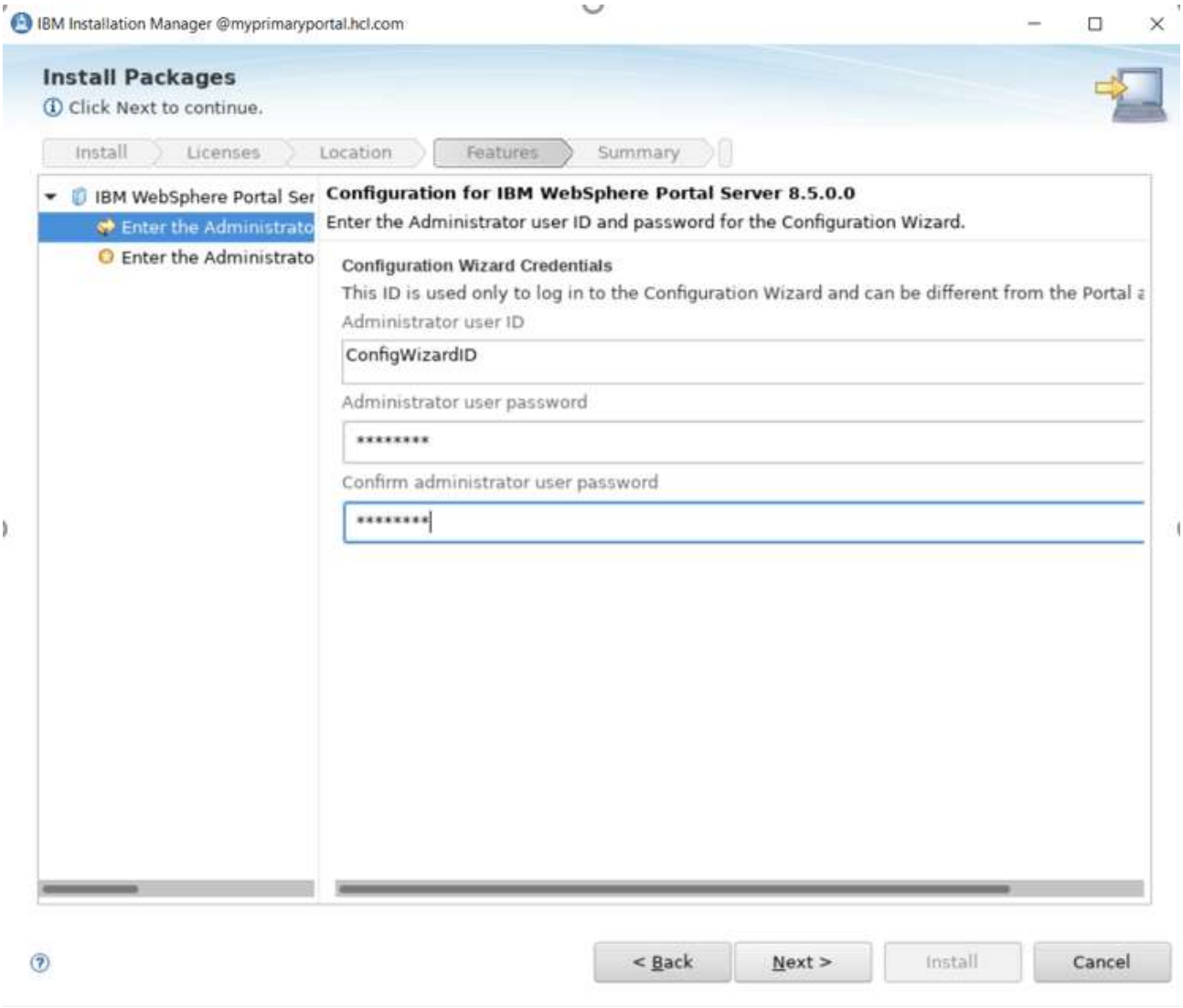
13. View the features to install for both WebSphere Application Server and WebSphere Portal. For this guide, the defaults were used.

NOTE: Do not de-select any WebSphere Application Server features.
Ensure you install a WebSphere Portal profile (selected by default).



Click **Next**.

14. Set the Configuration Wizard (Config Wizard) username and password. You can set these to any values you want to use for the Config Wizard credentials. “ConfigWizardID” is used for this guide.



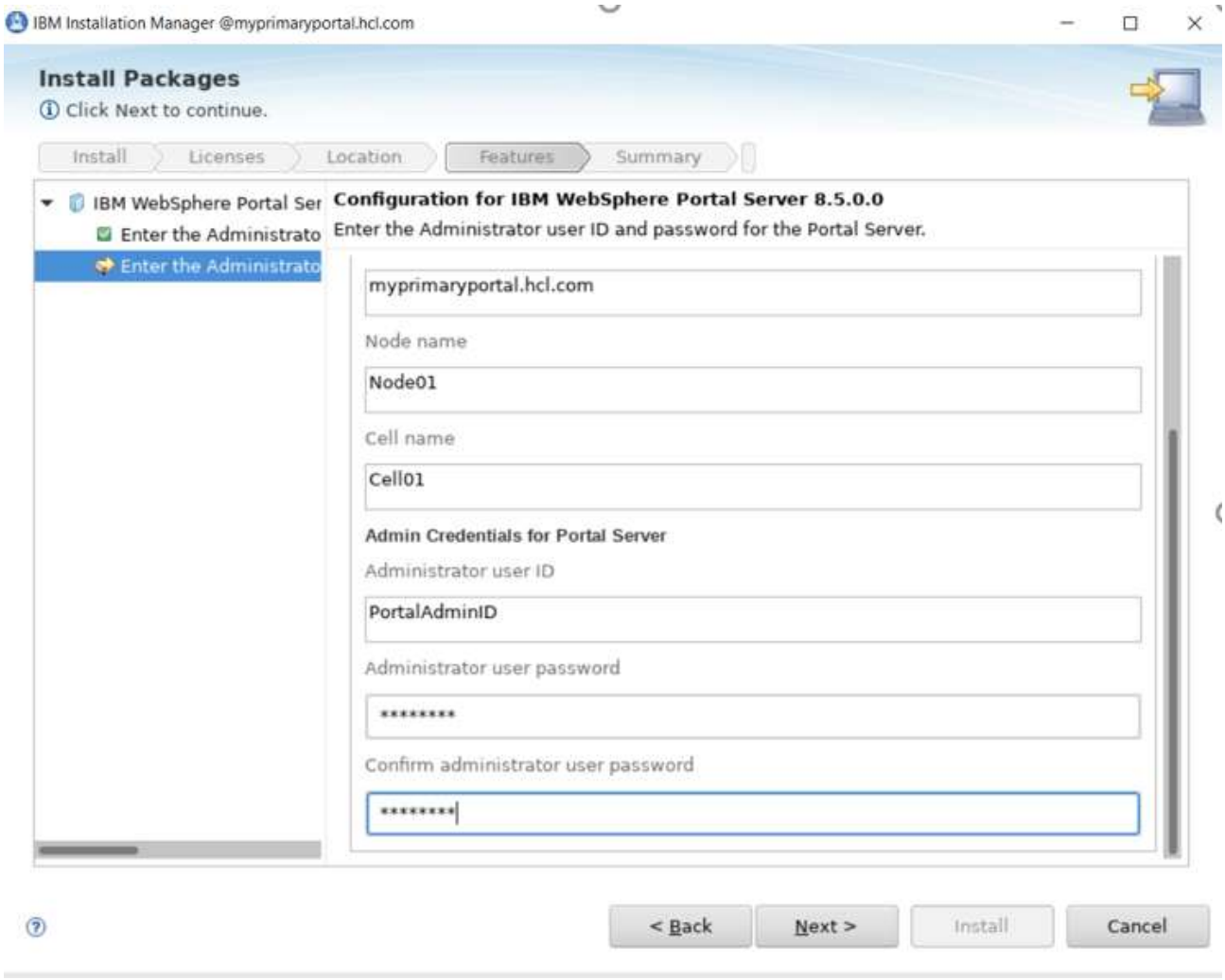
Click **Next.**

15. Select Standard configuration mode. Set the hostname to match the fully qualified hostname of your system. Set the node and cell names.

    NOTE: If you have an existing Deployment Manager, choose a node name and cell name different from the Deployment Manager node name and cell name.

16. Scroll down and set the Administrator user ID and password.

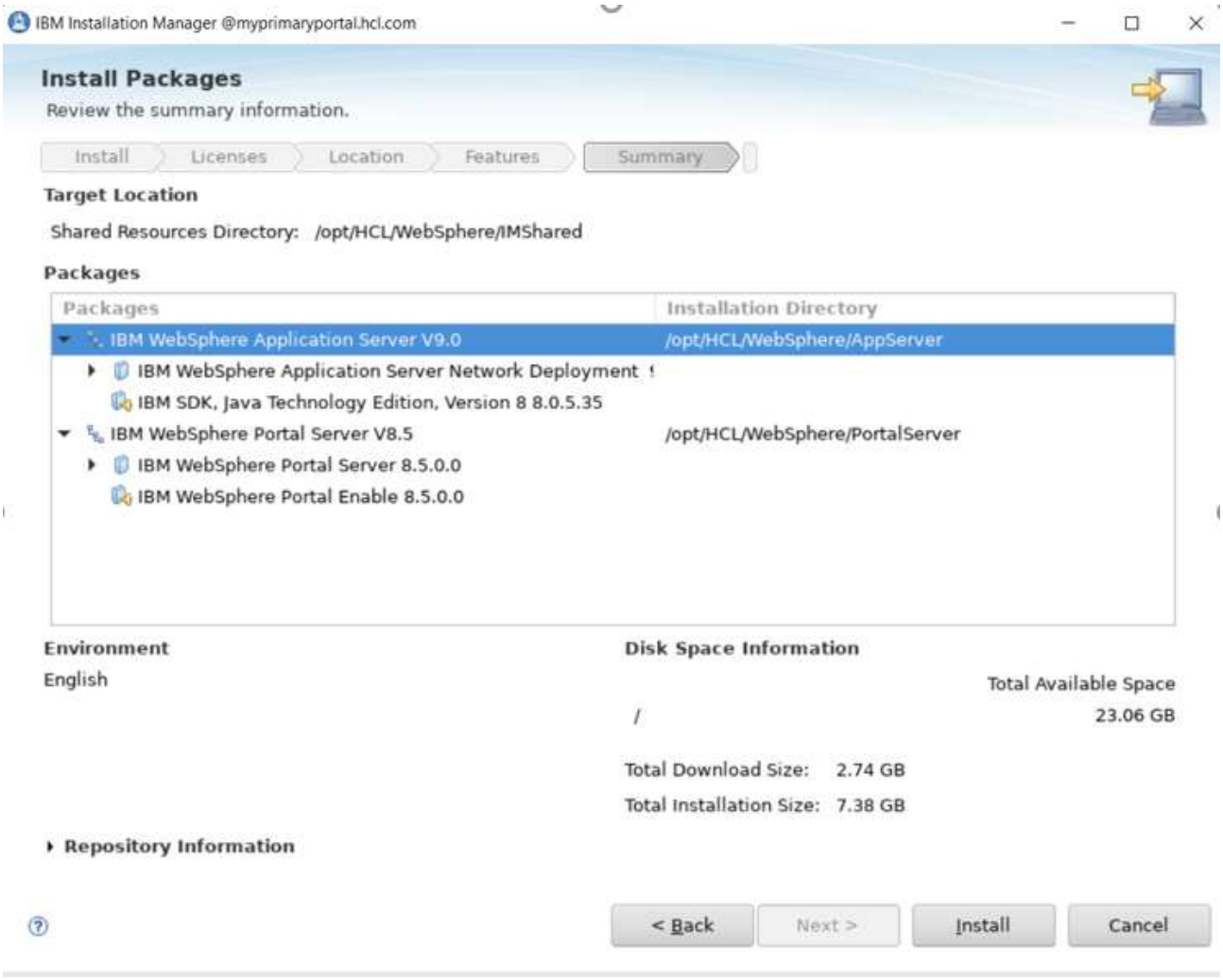
    NOTE: These credentials will be stored in an internal repository and must be unique from any existing user names in your LDAP. Otherwise, LDAP configuration in Chapter6 will fail.



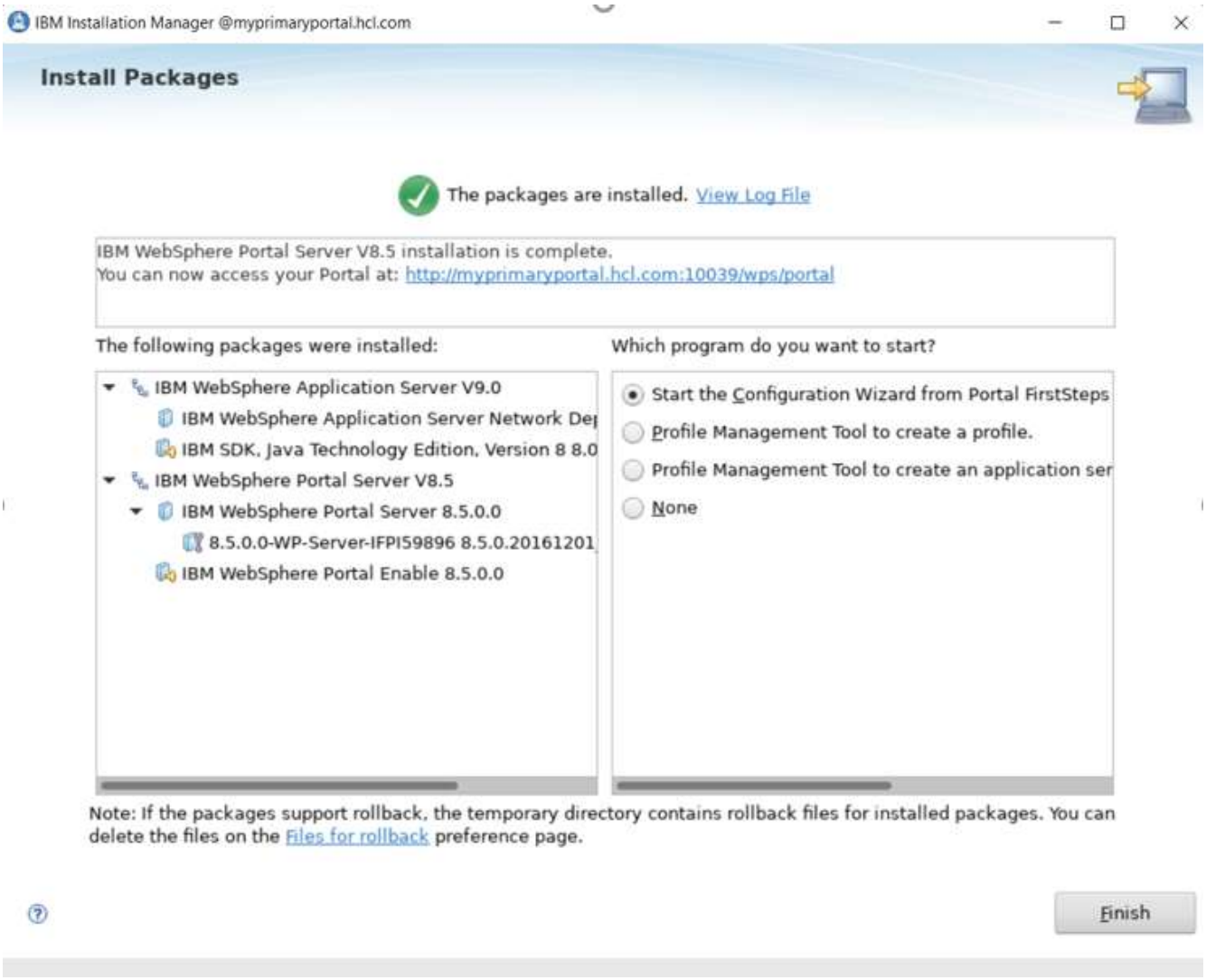
Click **Next**.

17. Review your installation selections and click **Install**.

    NOTE: The installation will take 30-60 minutes; don't be concerned if the Installation Manager seems to be stuck on one task for several minutes.



18. When the installation is finished, select the **None** option for “Which program do you want to start?” and click **Finish**.



19. Verify that you can access your Portal in an internet browser by navigating to: http://myprimaryportal.hcl.com:10039/wps/portal

At the end of this section, you have successfully installed HCL® Portal v8.5 with IBM® WebSphere Application Server v9.0.5

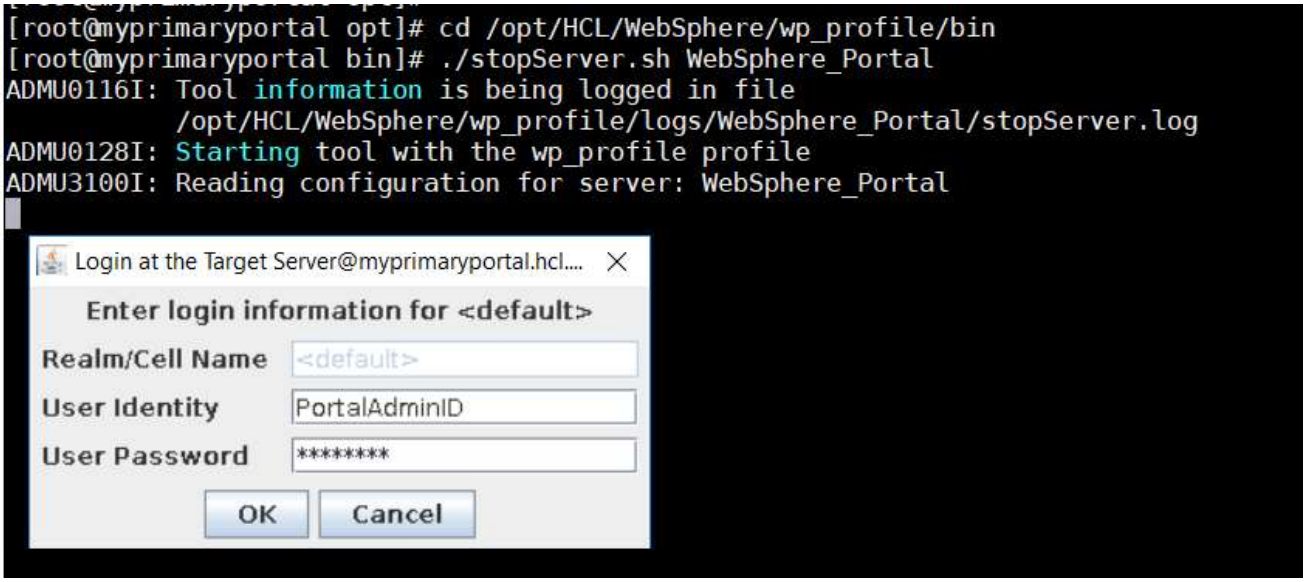
Section 3 – Upgrading HCL® Portal (WebSphere Portal) v8.5 to Cumulative Fix (CF) 17

HCL® Portal 8.5 now needs to be upgraded to Cumulative Fix 17 or a later CF to support the installation of HCL® Portal 9.5. You will need to stop the Portal Server and Configuration Wizard to proceed with the upgrade.

1. Open a terminal window and navigate to *wp_profile*/bin

2. Execute the following command:
   ./stopServer.sh WebSphere_Portal -user *PortalAdminID* -password *PortalAdminPswd*

3. You will be prompted for a userID and password.
   Enter your *PortalAdminID* for the userID and *PortalAdminPswd* for the password.

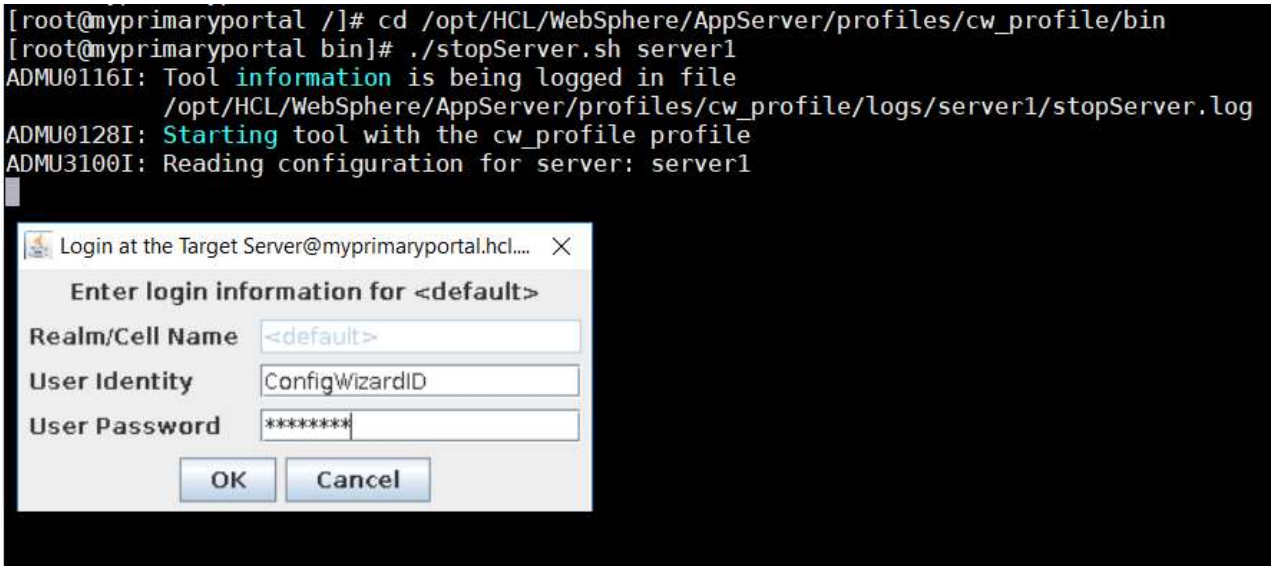


4. Navigate to the *AppServerRoot* folder. Continue in the directory structure to the /profiles/cw_profile/bin subdirectory. This guide uses the following directory for the full path:

   /opt/HCL/WebSphere/AppServer/cw_profile/bin

5. Execute the following command:
   ./stopServer.sh server1 -user *ConfigWizardID* -password *ConfigWizardPswd*

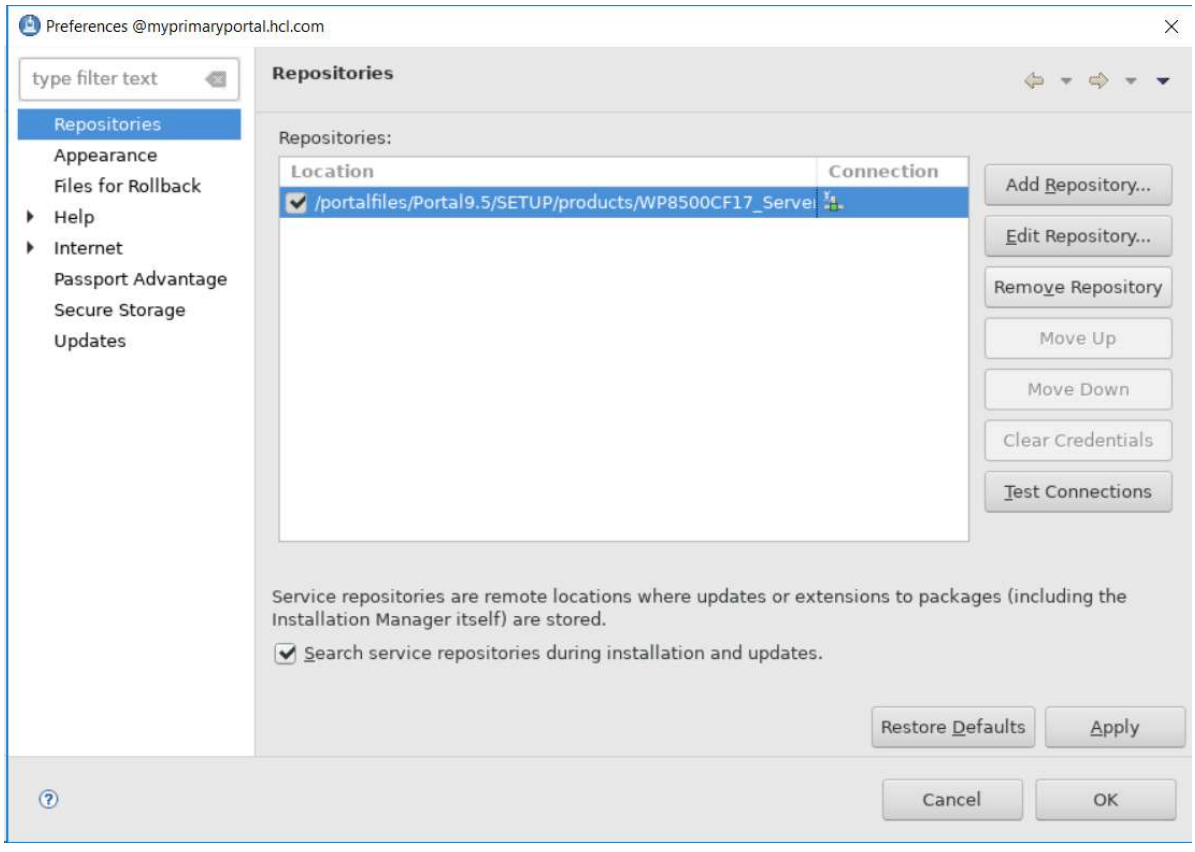
6. You will be prompted for a userID and password. Enter your *ConfigWizardID* for the userID and *ConfigWizardPswd* for the password.



7. Return to IBM Installation Manager. Click **File > Preferences > Repositories.**

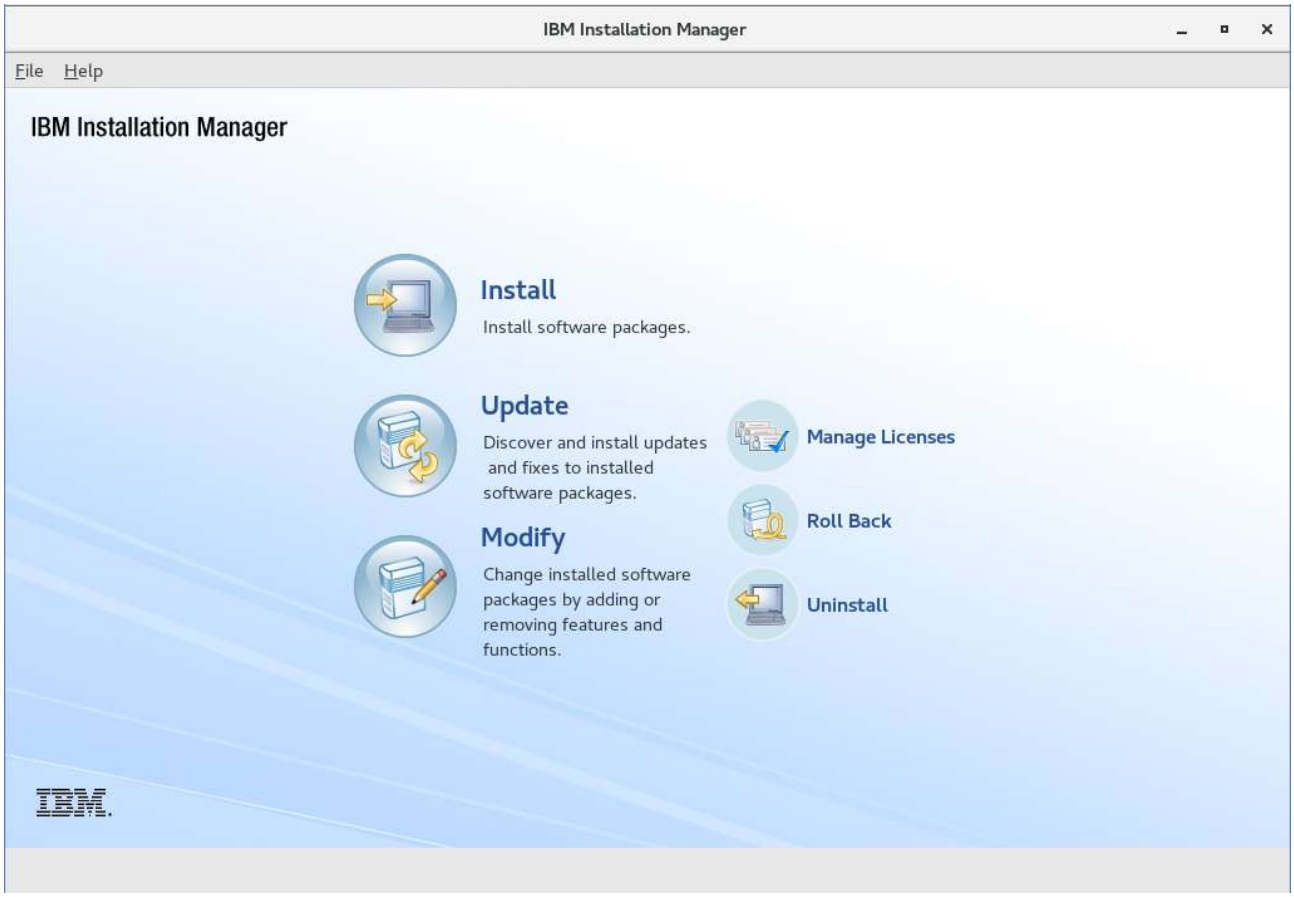
8. Select each of the existing Repositories and Click **Remove Repository.**

9. Click **Add Repository**, navigate to:
installationMediaRoot/SETUP/products/WP8500CF17_Server/repository.config

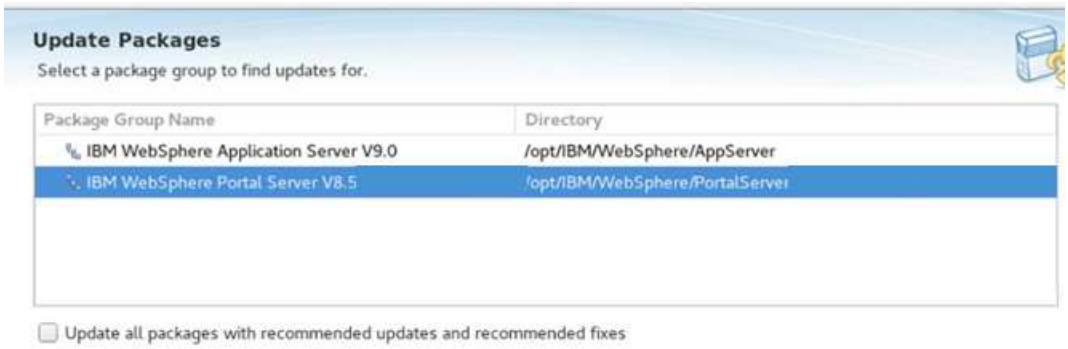


Click **OK** twice.

10. In IBM Installation Manager, click the Update icon:



11. Select the IBM WebSphere Portal Server 8.5 package.



12. Click **Next** to proceed with the Version 8.5.0.0 CF17 package.

13. Click **Next** to proceed beyond the Validation Results.

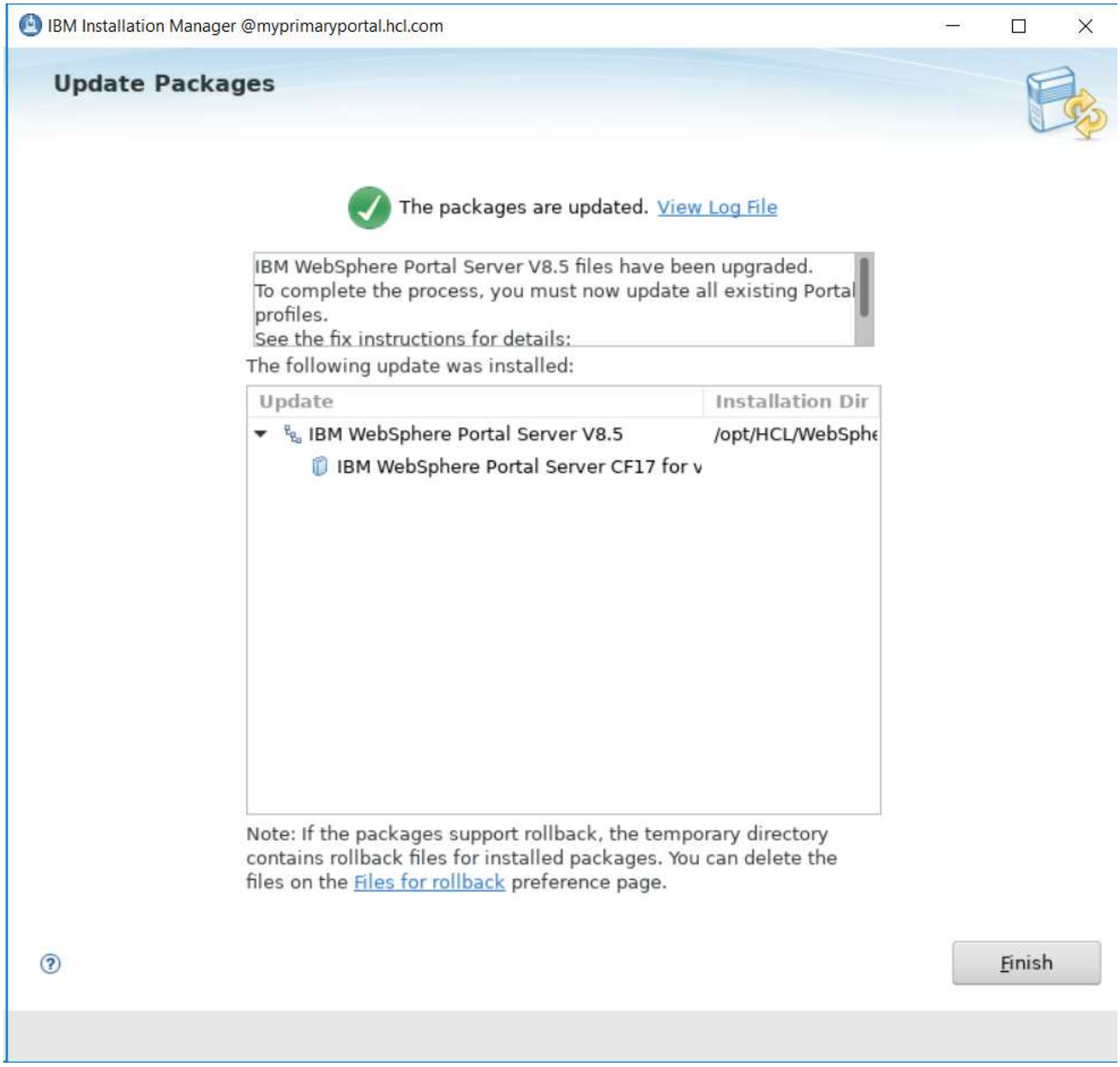
NOTE: HCL® highly recommends that you backup of your entire Portal architecture when installing a cumulative fix on an established Portal system. As the system in this guide represents a brand new system, a backup is not required at this time.

14. Click the radio icon for "I accept the terms in the license agreement". Click **Next.**

15. Click **Next** to Accept the terms of the licensing agreement.

16. Click **Next** to Install the IBM WebSphere Portal CF17 feature.

17. Click **Update.** This step will take approximately 20-30 minutes to execute.



18. Click **Finish.**

19. Open a terminal window and navigate to *wp_profile*/PortalServer/bin

    Execute the following command:
    ./applyCF.sh -DWasPassword= *PortalAdminPswd* -DPortalAdminPwd=*PortalAdminPswd*

```
[root@myprimaryportal bin]# pwd
/opt/HCL/WebSphere/wp_profile/PortalServer/bin
[root@myprimaryportal bin]# ls
applyCF.bat           genVersionReport.bat  rollbackCF.bat     slcheckertool.bat  WPHistoryInfo.bat  WPVersionInfo.bat
applyCF.sh            genVersionReport.sh   rollbackCF.sh      slcheckertool.sh   WPHistoryInfo.sh   WPVersionInfo.sh
genHistoryReport.bat  releasebuilder.bat    setupCmdLine.bat   wpcollector.bat    wpscript.bat       xmlaccess.bat
genHistoryReport.sh   releasebuilder.sh     setupCmdLine.sh    wpcollector.sh     wpscript.sh        xmlaccess.sh
[root@myprimaryportal bin]# ./applyCF.sh -DWasPassword=PortalAdminPwd -DPortalAdminPwd=PortalAdminPwd
```

20. Verify that you can access your Portal in an internet browser by navigating to:
    http://myprimaryportal.hcl.com:10039/wps/portal

At the end of this section, you have successfully installed Cumulative Fix 17 for HCL® Portal v8.5 on IBM® WebSphere Application Server v9.0.5.

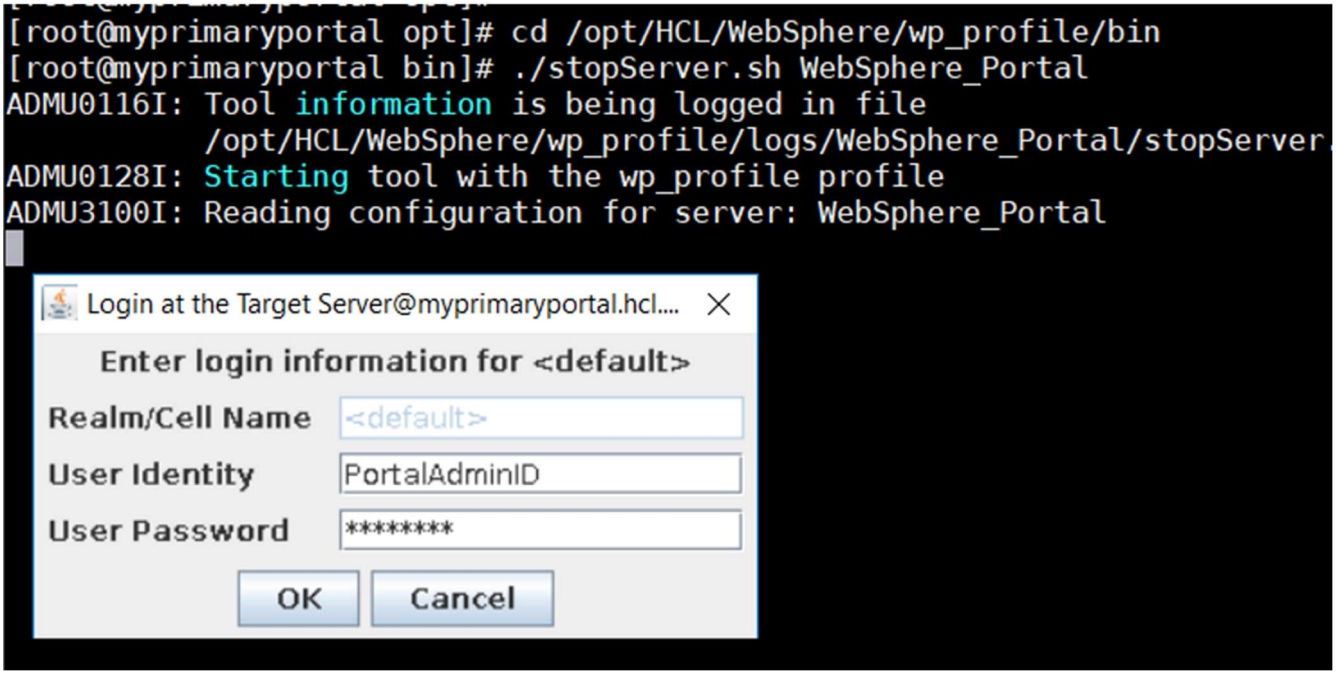
```
cleanup-config:
     [echo] executing post-configuration tasks
BUILD SUCCESSFUL
isIseries currently set to: null

update-registry-sync-property:
     [echo] updated RegistrySynchronized in file wkplc.properties w

print-final-message:
Return code = 0
deleting temporary files

SUCCESS: Update to Cumulative Fix CF17 completed successfully.
[root@myprimaryportal bin]#
```

Section 4 – Upgrading HCL® Portal (WebSphere Portal) v8.5 CF17 or a later CF to HCL® Portal v9.5

In this final section HCL® Portal 8.5 CF17 will be upgraded to HCL® Portal Cumulative Fix 17. You will need to stop the Portal Server and Configuration Wizard to proceed with the upgrade.

1. Open a terminal window and navigate to *wp_profile*/bin
2. Execute the following command:
   ./stopServer.sh WebSphere_Portal

3. You will be prompted for a userID and password. Enter your *PortalAdminID* for the userID and *PortalAdminPswd* for the password.

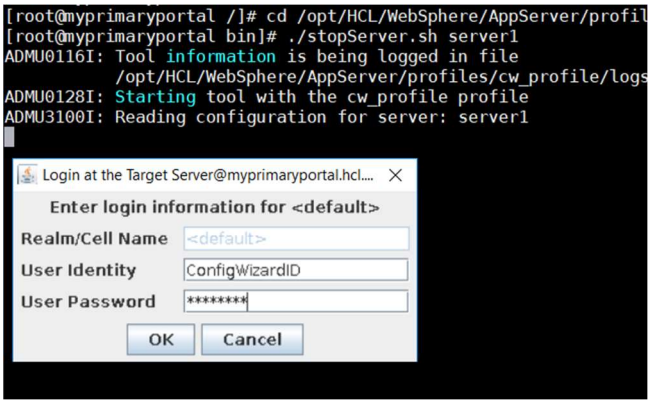


4. Navigate to the location you installed IBM® WebSphere Application Server. Continue in the directory structure to the /profiles/cw_profile/bin subdirectory. This guide uses the following directory for the full path:

   /opt/HCL/WebSphere/AppServer/cw_profile/bin

5. Execute the following command:
   ./stopServer.sh server1

6. You will be prompted for a userID and password. Enter your *ConfigWizardID* for the userID and *ConfigWizardPswd* for the password.



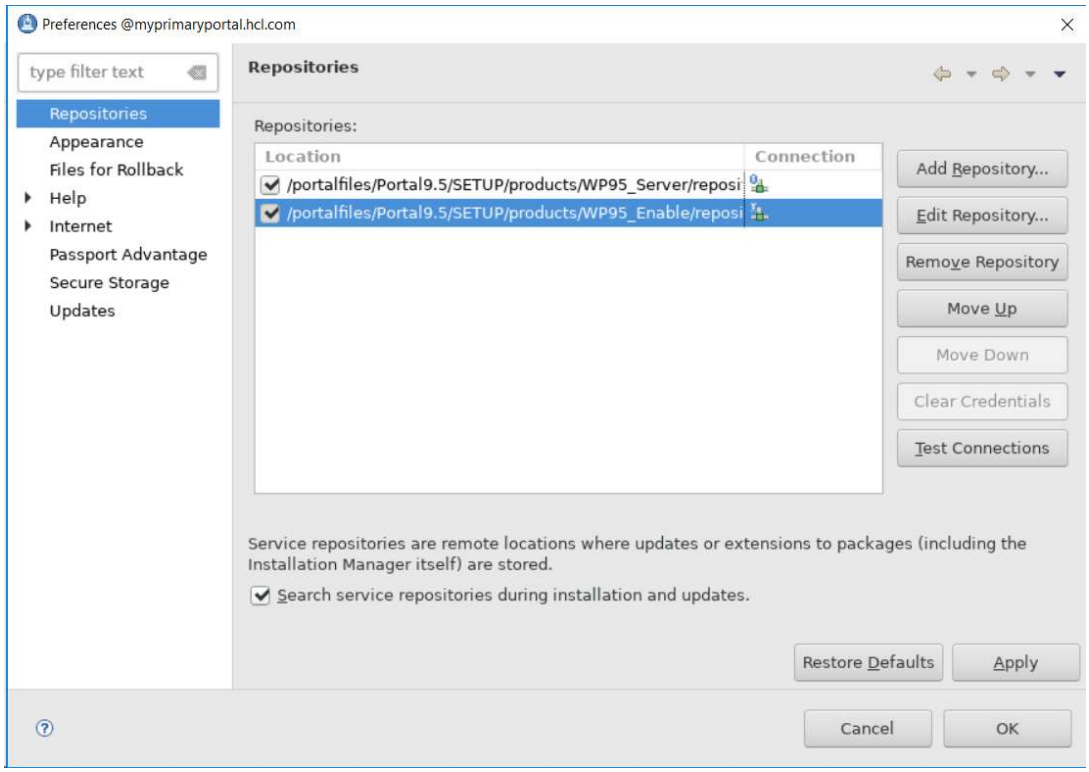
7. Return to IBM® Installation Manager. Click **File > Preferences > Repositories.**

8. Select each of the existing Repositories and Click **Remove Repository.**

9. Click **Add Repository**, navigate to:
installationMediaRoot/SETUP/products/WP95_Portal/repository.config

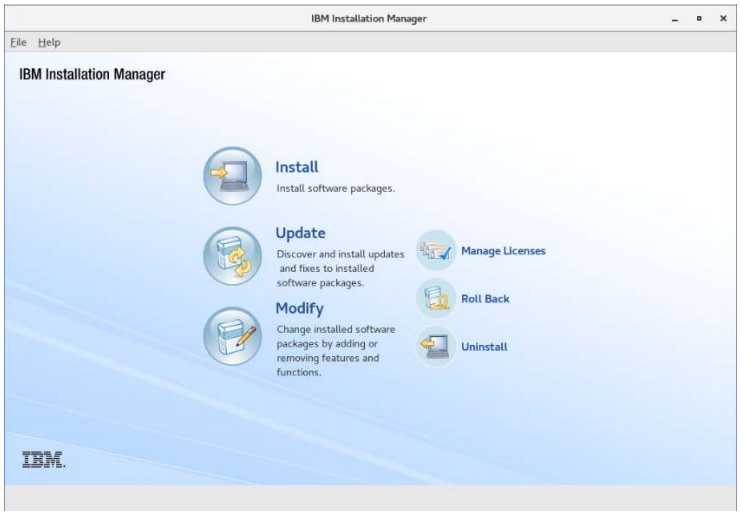
   Click **OK.**

10. Click **Add Repository**, navigate to:
installationMediaRoot/SETUP/products/WP95_Enable/repository.config

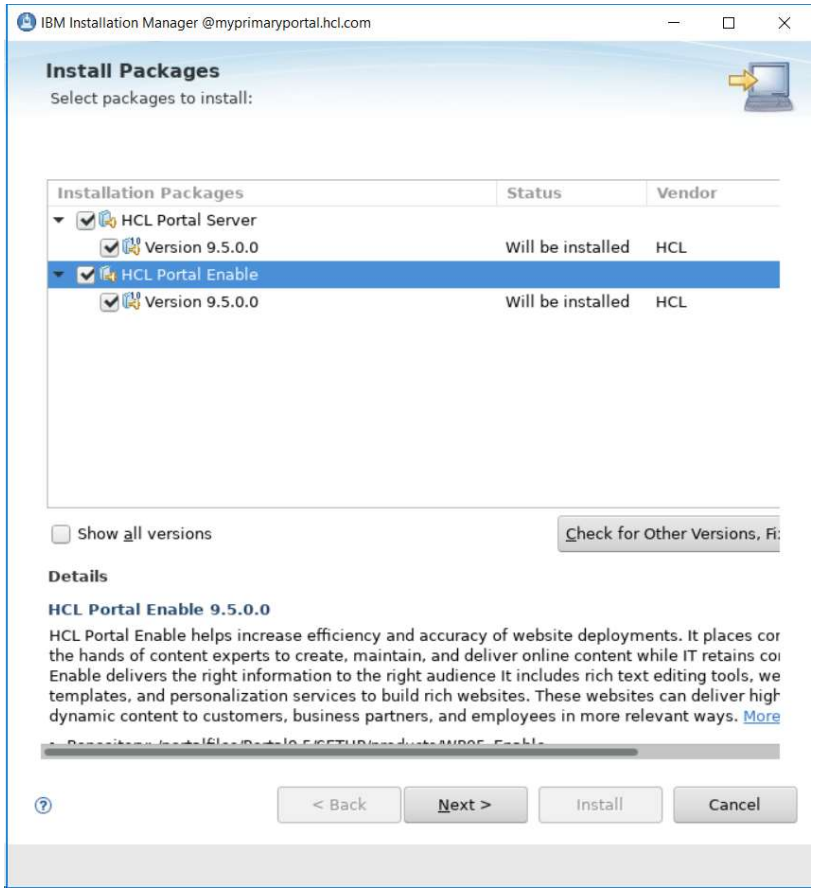


Click **OK** twice.

11. In IBM® Installation Manager, click the Install icon:



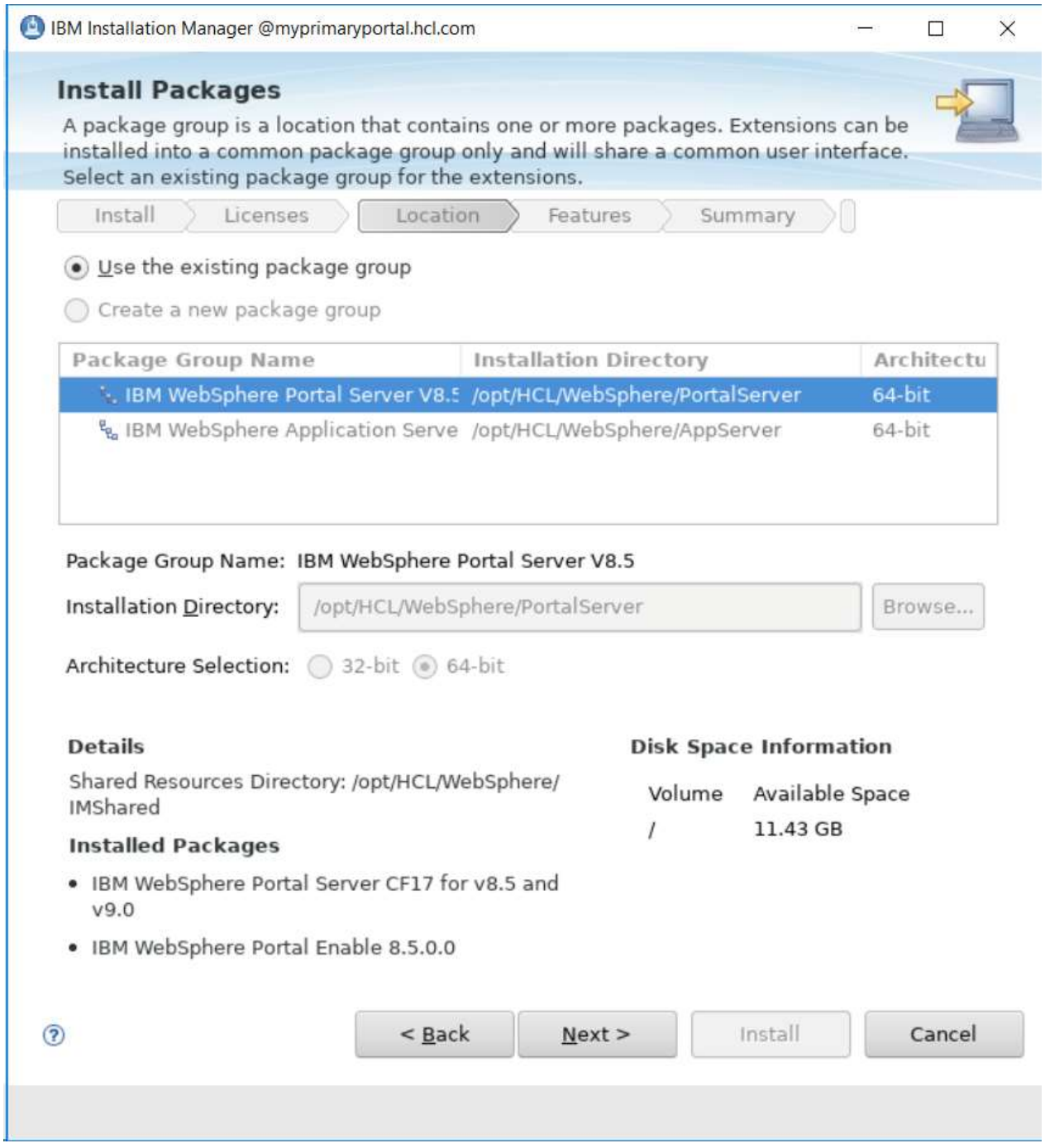
12. Check the boxes to install the HCL Portal Server and HCL Portal Enable (or the offering you are installing, e.g. Extend, Express, etc.) packages.



Click **Next**

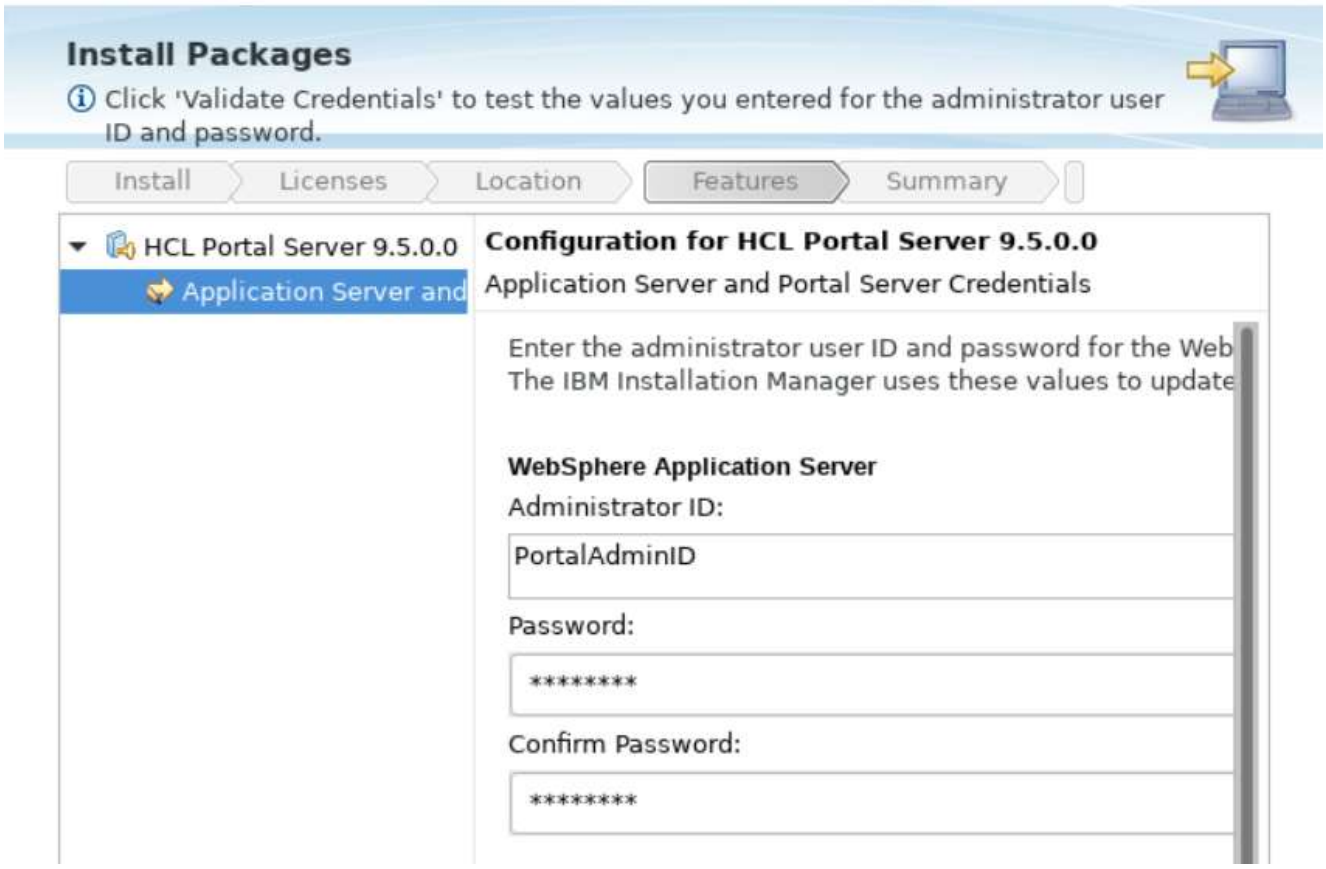
13. Accept terms of licensing agreement. Click **Next.**

14. Select the option **Use the existing package group** and click on **IBM WebSphere Portal v8.5.**

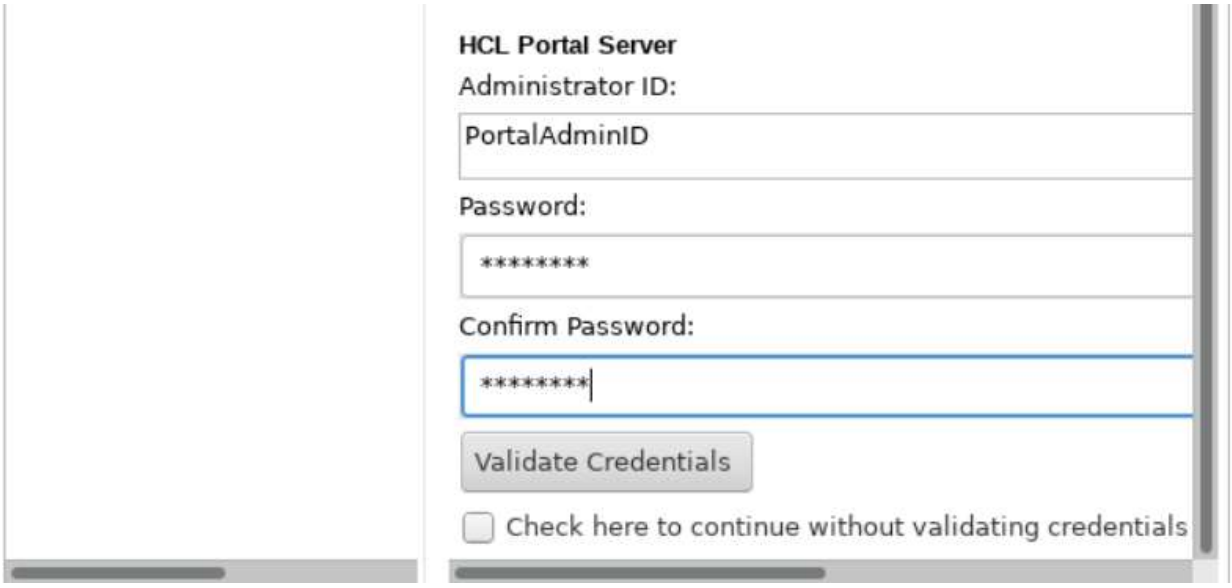


Click **Next**

15. Enter your *PortalAdminID* and *PortalAdminPswd* for the Websphere Application Server credentials. Scroll down. Enter your *PortalAdminID* and *PortalAdminPswd* for the Portal Server credentials.

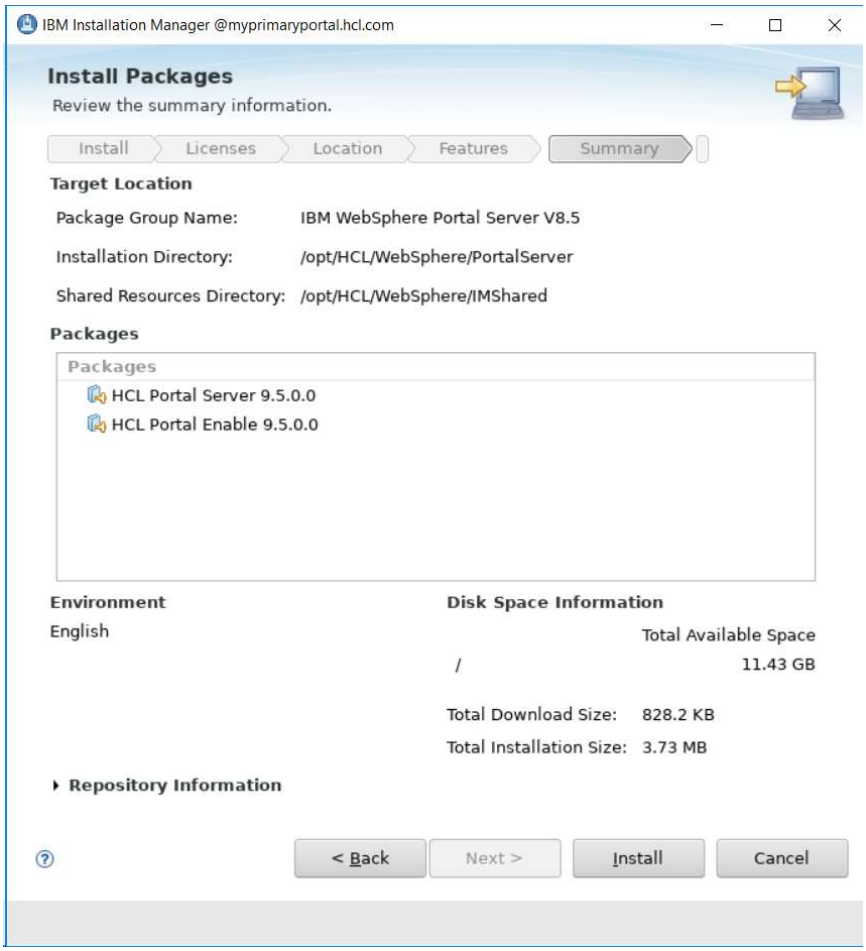


16. Click **Validate Credentials**

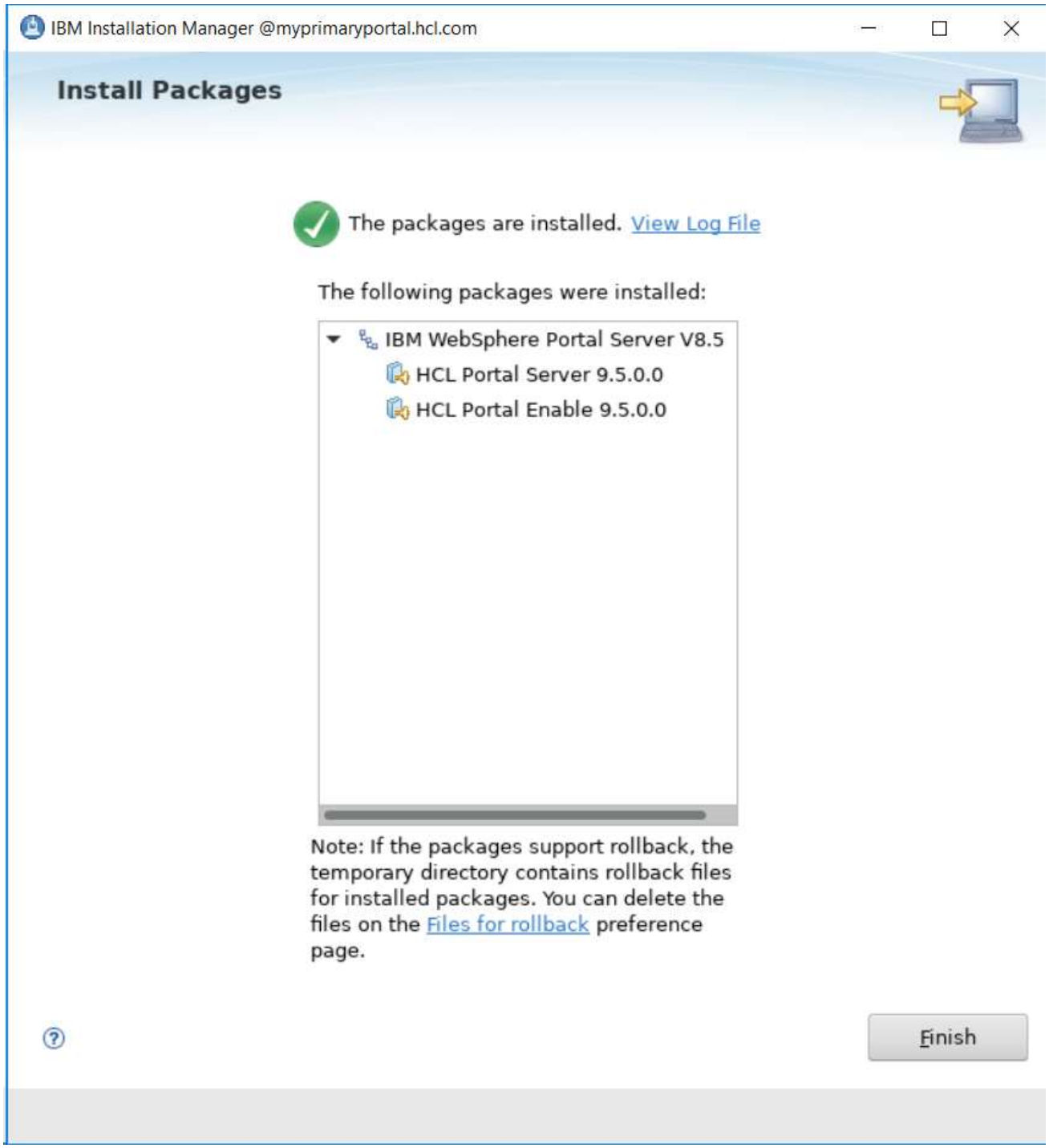


Wait a few minutes for validation to complete. Click **Next**.

17. Review Summary. Select **Install.**



18. When the installation is finished, you should see:



NOTE: On a successful upgrade, you will be presented with a link to fully integrate HCL ® Portal 9.5 with Watson Content Hub. Watson Content Hub integration is not required to build a WebSphere Portal 9.5 cluster

19. Verify that you can access your Portal in an internet browser by navigating to: http://myprimaryportal.hcl.com:10039/wps/portal

Chapter 2 – Configuring the Primary Node for a Remote Database

In this section, you will configure HCL® Portal to use an external database. For this guide, IBM® DB2 is used as the external database with Type 4 drivers installed and run on a different host than HCL® Portal. More information about other databases that can be used with HCL® Portal is available by referencing the HCL® Digital Experience v9.5 Product Documentation at the following link:

https://help.hcltechsw.com/digital-experience/9.5/welcome/wp95_welcome.html?query=9.5

To complete the task of configuring the Primary node for a remote database, execute the following steps:

1. On the Portal Server, create a directory called "dbdrivers" at the following location:

   wp_profile/PortalServer/dbdrivers

   for this guide:

   /opt/IBM/WebSphere/wp_profile/PortalServer/dbdrivers

2. On the DB2 environment, navigate to *DB2InstallationRoot*/*YourDB2Version*/java, for example:

   /opt/ibm/db2/V11.1/java

   and locate these two files:

   db2jcc4.jar
   db2jcc_license_cu.jar

```
[root@myprimaryportal java]# pwd
/opt/ibm/db2/V11.1/java
[root@myprimaryportal java]# ls -la | grep -i 'db2jcc4.jar\|db2jcc_license_cu.jar'
-r--r--r--  1 bin  bin  3894263 Jun  9  2016 db2jcc4.jar
-r--r--r--  1 bin  bin     1534 Jun  9  2016 db2jcc_license_cu.jar
[root@myprimaryportal java]#
```

3. Copy the two files from the DB2 server to the Primary Portal server and save them in the newly created /opt/HCL/WebSphere/wp_profile/PortalServer/dbdrivers folder.

NOTE: The next several steps will use a web-based tool called the Configuration Wizard. The Config Wizard helps you create custom scripts with instructions called workflows. Workflows are used to configure different aspects of HCL® Digital Experience. For more information see the following page in the IBM® Knowledge Center:

https://help.hcltechsw.com/digital-experience/9.5/welcome/wp95_welcome.html?query=9.5

4. On the Portal Server, navigate to the *AppServerRoot/*profiles/cw_profile/bin directory. Execute the following command to start the Configuration Wizard:
   ./startServer.sh server1

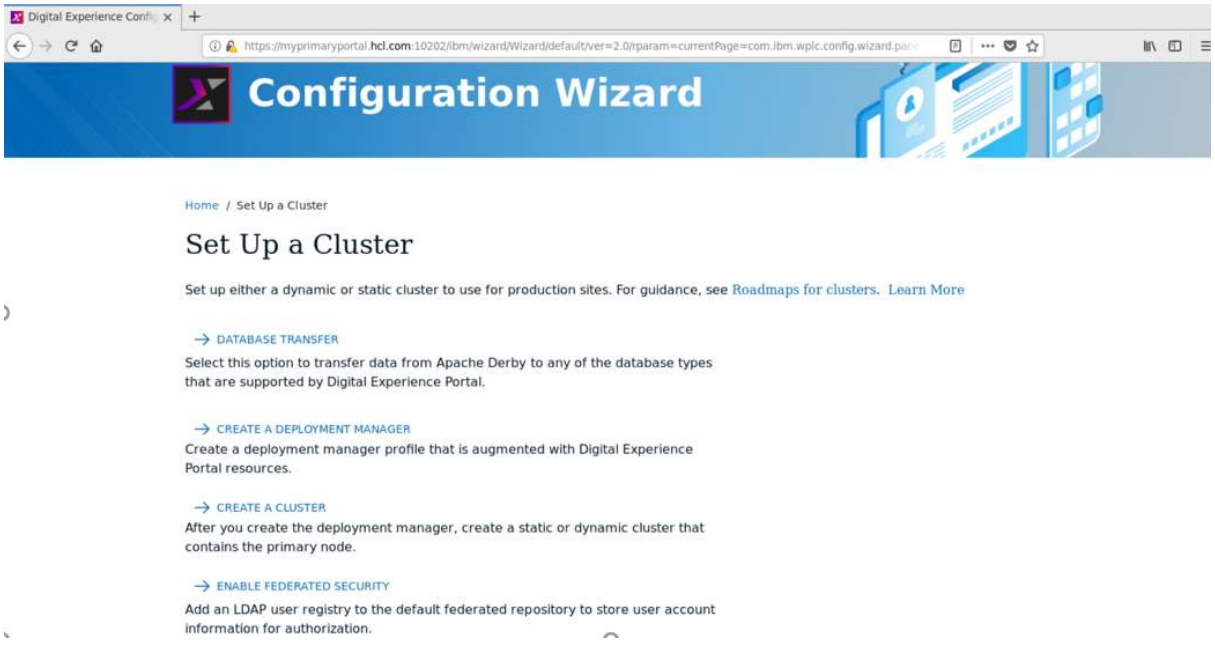
5. Open a web browser and navigate to the Configuration Wizard:

   http://myprimaryportal.hcl.com:10200/hcl/wizard

   and log in with the *ConfigWizardID* and *ConfigWizardPswd* user credentials you created during Portal installation.

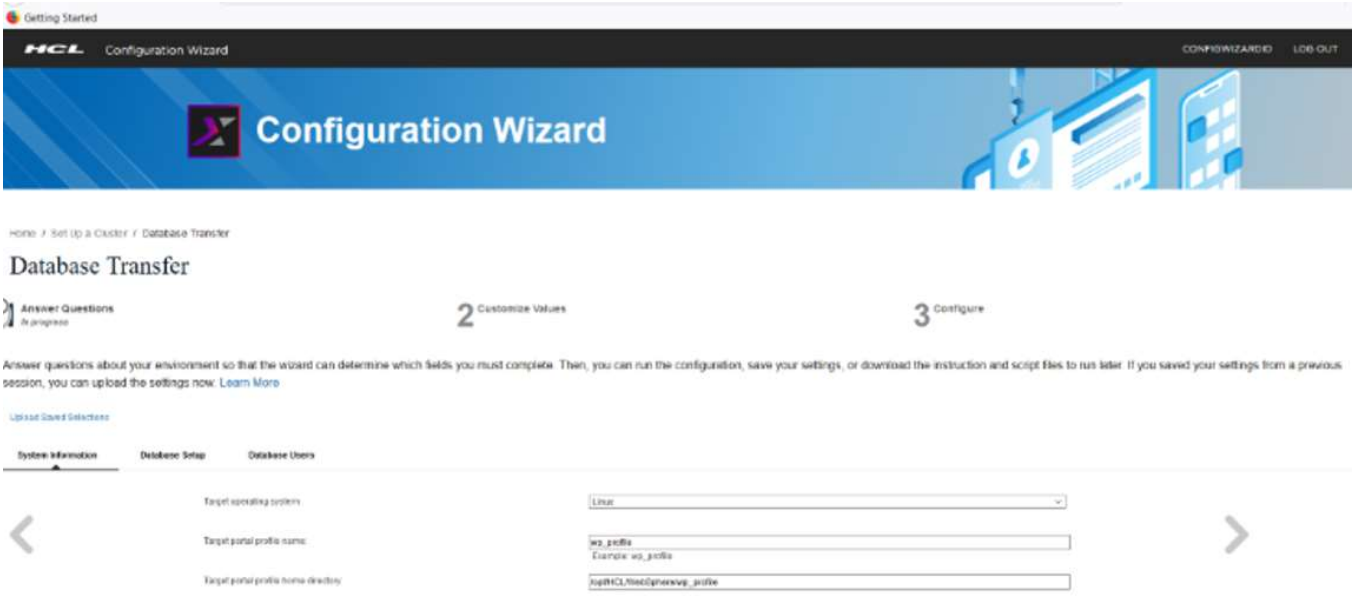
CONFIG WIZARD CUMULATIVE FIX NOTE: The following screenshots are taken from a Portal system with cumulative fix 17 installed from Chapter 1 of this guide. If your installation has a different cumulative fix level, your Config Wizard options and screens could differ slightly from those shown in this guide.

6. From the Configuration Wizard home screen, select **Set Up a Cluster**>**Database Transfer**.



7. Choose your target operating system, name of your Portal profile, and Portal profile's location

   NOTE: The profile name and profile location fields are pre-populated with the defaults.



   Click the right arrow.

8. Provide answers for the following database setup items (examples shown; you can customize these values according to your environment or preferences):

   Database management software: **DB2**

   Do you want to transfer one database or multiple databases: **Multiple Databases**

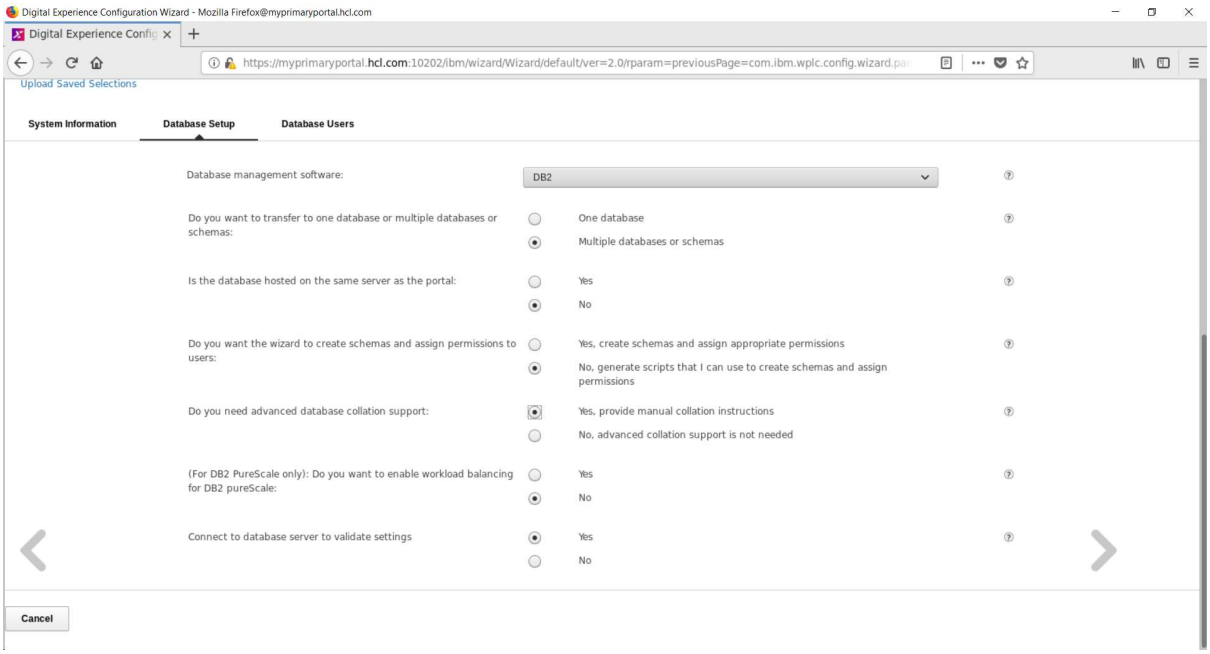
   Is the database hosted on the same server as the portal: **No**

   Do you want the wizard to create users and assign them permission: **No, generate scripts**

   Do you need advanced database collation support: **Yes**

   Do you want to enable workload balancing for DB2 pureScale: **No**

   Connect to database server to validate settings: **Yes**



Click the right arrow.

9. HCL® Portal leverages two different database users - a configuration user and a runtime user. The configuration user is used during a limited number of database operations and requires additional privileges on the database server. The runtime user is used to connect the Portal to the database during normal, day-to-day operations and requires fewer privileges.

   Review the following link for more details on the required permissions for the configuration and runtime user for each of the Portal databases:

   https://help.hcltechsw.com/digital-experience/9.5/config/unix_db2i_priv_dbusers_common.html?query=portal%20databases

   This guide will use **db2inst1** for both the configuration user and runtime user for all databases in subsequent steps. For this step you must manually setup database configuration users and database runtime users on the database server to meet your company's enterprise database requirements. Record the IDs and passwords for each of the database users you created as they will be needed in subsequent steps.

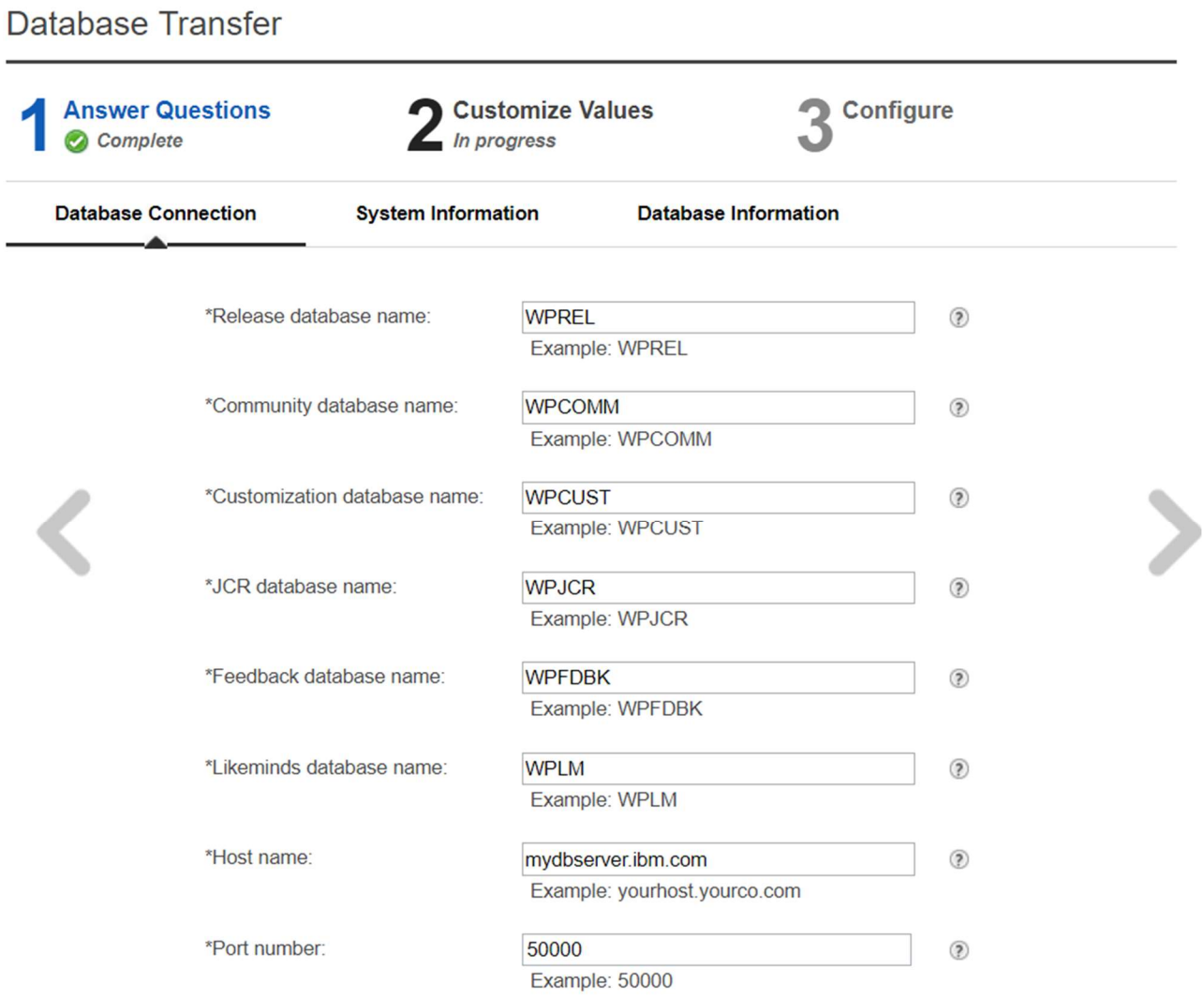
10. Answer the database users questions (examples provided):

Do portal database domains use the same user ID and passwords: Yes

Do you need runtime database user ID for day-to-day operations: Yes

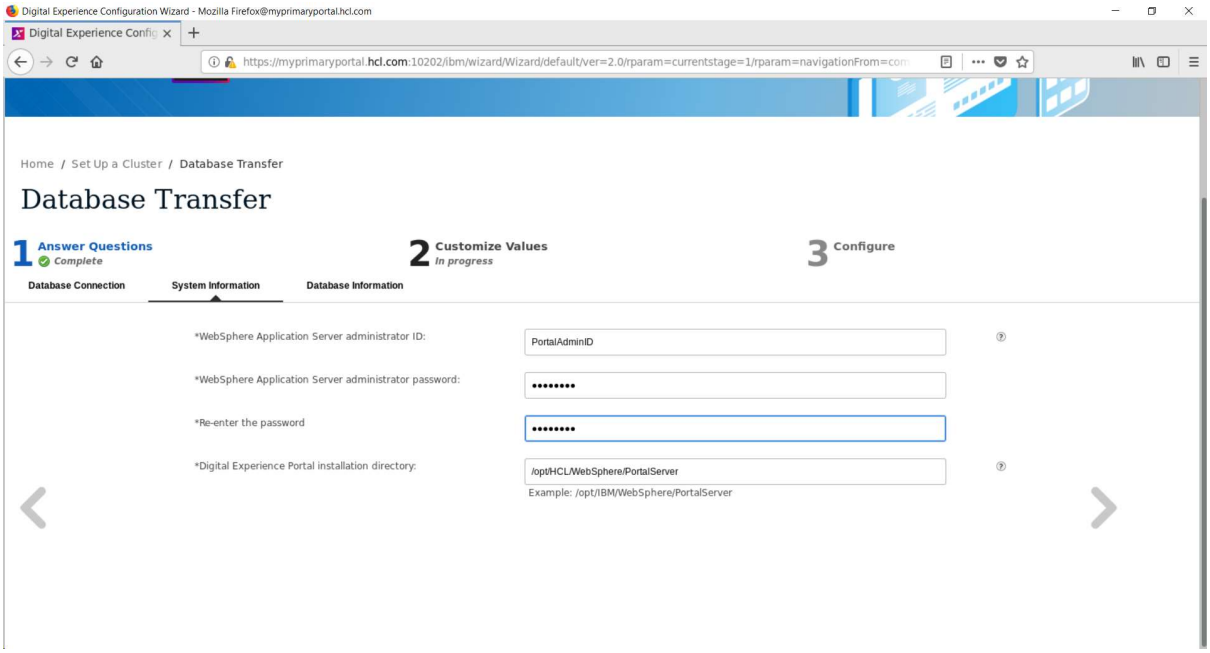
Click the right arrow.

11. Fill in the name for each Portal Domain as well as the Database server hostname and port

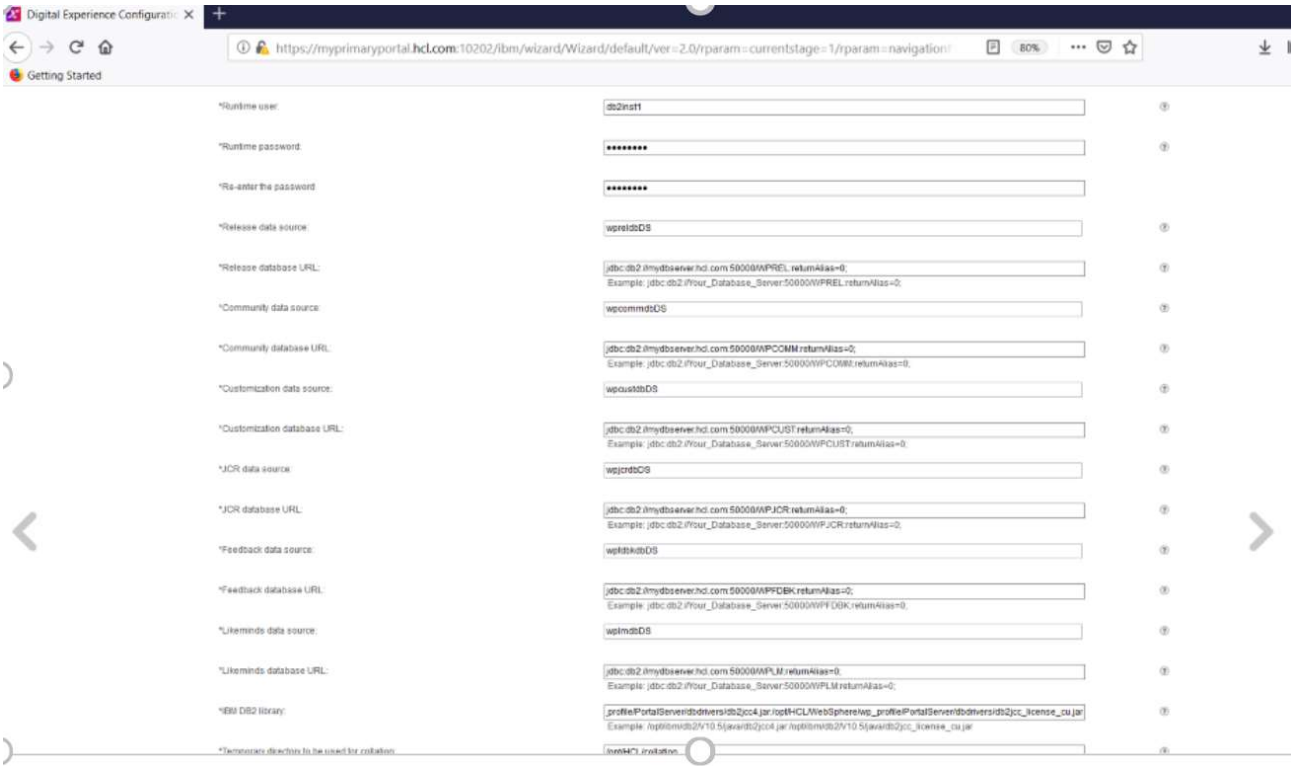


Click the right arrow.

12. Fill in the values for your *PortalAdminID* and *PortalAdminPswd* specified during installation in Chapter 1.



13. Fill in your Configuration, Database administrator, and Runtime user ID's and corresponding passwords. All are **db2inst1** for this guide.



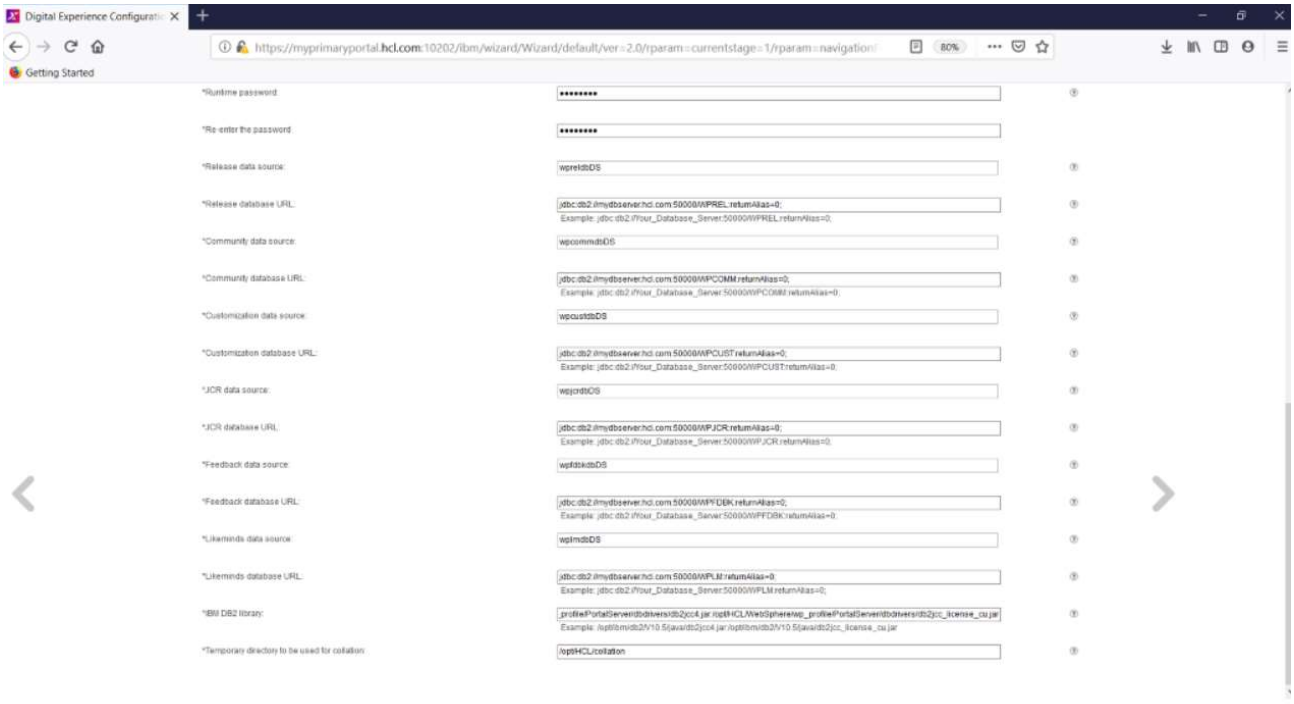
Step 13 is continued on the next page.

Scroll down and fill in the following values for each database:

- Database Name: this guide uses the pre-populated defaults
- Data Source: this guide uses the pre-populated defaults
- Database URL: use the example provided below the text box and add your database server hostname in place of mydbserver.ibm.com

  NOTE: DO NOT put "@" symbols around the database urls. Be sure to end each URL with a semicolon. Example:

  jdbc:db2://mydbserver.ibm.com:50000/<databaseName>:returnAlias=0;



14. Scroll down and fill in the last two values:

- IBM® DB2 Library: the full paths to both type 4 DB2 drivers that you copied onto the primary Portal server, separated by a colon. This guide used:

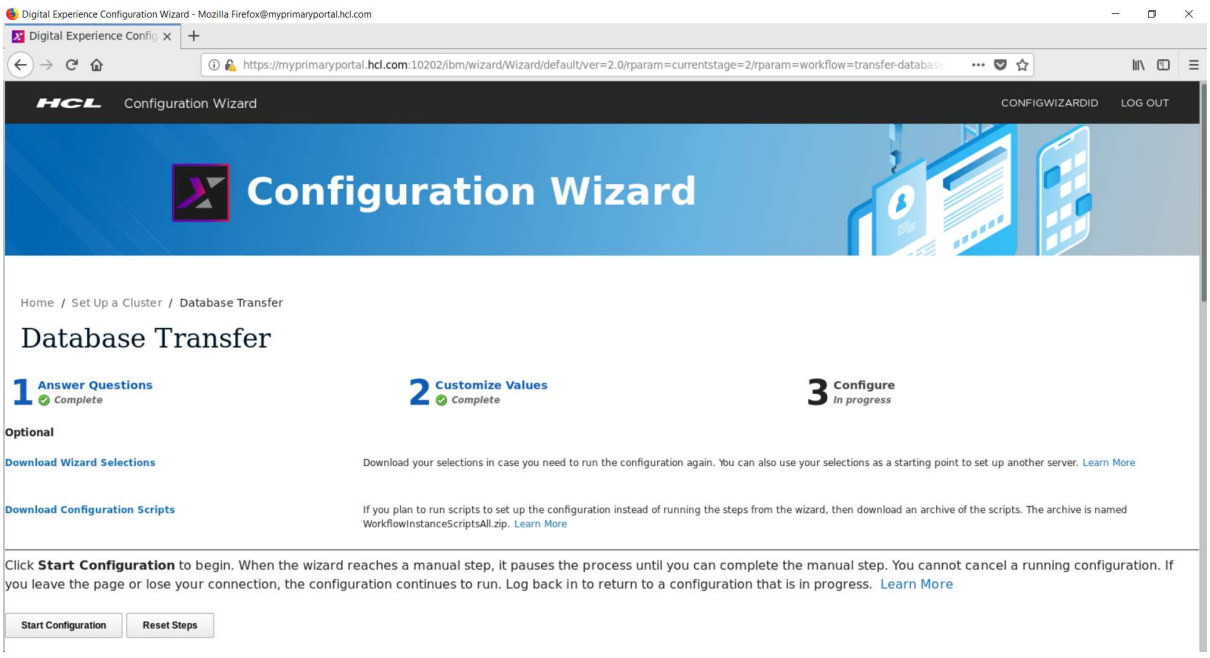
  /opt/HCL/WebSphere/wp_profile/PortalServer/dbdrivers/db2jcc4.jar:
  /opt/HCL/WebSphere/wp_profile/PortalServer/dbdrivers/db2jcc_license_cu.jar

NOTE: For Windows environments, use a semi-colon between the two paths rather than a colon, which is used for Linux environments.

- Temporary directory to be used for collation: choose a name and location for your temporary directory. This guide uses:
  /tmp/tmpdb

Click the right arrow.

15. On the next screen, click **Download Configuration Scripts** and save the downloaded file.



Do not close this window. Minimize it during the next step as you will need it again.

NOTE: Many of the following steps will be specific to DB2; see the instructions from the Config Wizard for steps specific to your database.

16. Move the downloaded .zip file to a convenient location on your database server as the database instance user. This guide uses /home/user/Desktop/CWScripts and db2inst1. Unzip the file by changing directories to the location of the scripts and running:

    unzip WorkflowInstanceScriptsAll.zip

    The CWScripts directory now contains the scripts you will run to create and setup your databases.

17. Go up one directory:

    cd ..

    and run the following from /home/user/Desktop, or your equivalent location, to change the permissions on the scripts.:

    chmod -R 777 CWScripts

The resulting permissions in the Scripts/ folder should look like this:

18. Navigate to the scripts subdirectory.
    Change the name of “CreateDB2Database” to “CreateDB2Database.sh”.

19. As the db2inst1 user execute the CreateDB2Database.sh script
    (ensure that DB2 is started before running this script):

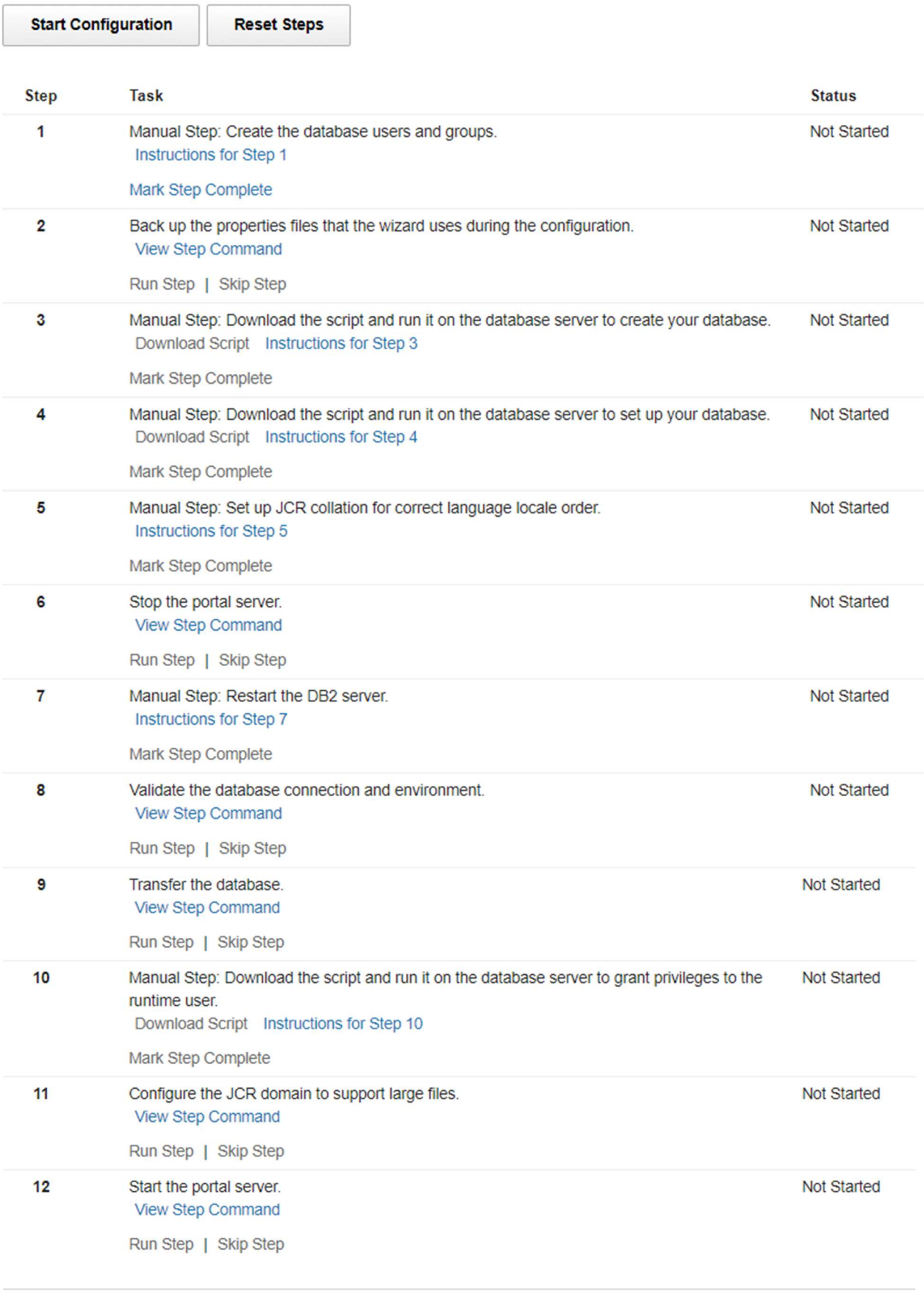
    su db2inst1

    ./CreateDB2Database.sh

20. After that command completes successfully, execute the following command:

    db2 -tvf SetupDB2Database.sql

21. Go back to the Config Wizard window. You should see a screen like the following:

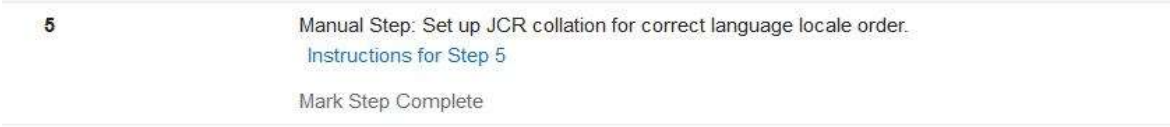


22. Click **Mark Step Complete** for Step 1

23. Click **Run Step** for Step 2,

24. Click **Mark Step Complete** for Step 3 and Step 4.

25. Click **Instructions for Step 5** and review the details provided.



26. Copy the following files from the WebSphere Portal server to /tmp/tmpdb directory (the temporary folder you specified on the previous Config Wizard page) on the DB2 server:

/opt/HCL/WebSphere/PortalServer/jcr/wp.content.repository.install/lib/wp.content.repository.install.jar
/opt/HCL/WebSphere/wp_profile/PortalServer/jcr/config/registerCollationUDFTemplate.sql

27. Set up collation on the database where the JCR domain is located. Change to this directory:

db2_instance_owner_home/sqllib/function

28. Execute the following command:

db2home/sqllib/java/jdk/bin/jar -xvf /tmp/tmpdb/ wp.content.repository.install.jar icm/CollationUDF.class

29. Change to the temporary directory where you copied the files in a previous step. For example, you can use this temporary directory on the DB2 server:
/tmp/tmpdb

30. Open the file “registerCollationUDFTemplate.sql” and change all SCHEMA references to the JCR schema; for example, JCR. For this guide, the default schema name, JCR, was used and the final result looked like the following:

```
[db2inst1@myprimaryportal tmpdb]$ more registerCollationUDFTemplate.sql
CREATE FUNCTION JCR.SORTKEYJ
(
    VALUE        VARCHAR(32672),
    LOCALEID     VARCHAR(50)
)
RETURNS VARCHAR(5000) FOR BIT DATA
FENCED THREADSAFE
DETERMINISTIC
NO SQL
NO EXTERNAL ACTION
LANGUAGE JAVA
PARAMETER STYLE JAVA
EXTERNAL NAME 'icm.CollationUDF!generateKey'
ALLOW PARALLEL
RETURNS NULL ON NULL INPUT;

GRANT EXECUTE ON FUNCTION JCR.SORTKEYJ TO PUBLIC;

UPDATE DBM CFG USING JAVA_HEAP_SZ 4096;
[db2inst1@myprimaryportal tmpdb]$
```

31. Connect to the JCR database:
    db2 connect to WPJCR user *DBUser* using *DBPasword*

32. Enter this command to run the script:

    db2 -tvf /tmp/tmpdb/registerCollationUDFTemplate.sql

```
[db2inst1@myprimaryportal tmpdb]$ pwd
/tmp/tmpdb
[db2inst1@myprimaryportal tmpdb]$ db2 connect to WPJCR user db2inst1 using passw0rd

   Database Connection Information

 Database server        = DB2/LINUXX8664 11.1.0
 SQL authorization ID   = DB2INST1
 Local database alias   = WPJCR
```

33. Disconnect from the JCR database:
    db2 disconnect all

34. Restart the DB2 instance.
    db2stop
    db2start

35. Connect to the JCR database. Validate the UDF template was registered

    db2 connect to WPJCR user *DBUser* using *DBPasword* values jcr.sortkey('abc','en')

    This guide observed the following message after running the final command:

```
  1 record(s) selected.

db2 =>
```

36. Disconnect from the DB2 terminal window

    quit
    db2 disconnect all
    db2 terminate

37. Switch back to the Portal server. Open a terminal window and navigate to <wp_profile>/bin.

38. Execute the following command:
    ./startServer WebSphere_Portal

39. Open a web browser and navigate to the following URL:
    https://myprimarportal.ibm.com:10041/ibm/console

    Login with your *PortalAdminID* and *PortalAdminPswd* specified during installation.

40. Navigate to to **Resources** > **Resource Environment** > **Resource Environment Providers** > **JCR ConfigService PortalContent** > **Custom properties**.

41. Click **New**. Create a new property for each of the following. Click **OK** after specifying each property and **Save** to save the Changes.

    Name: jcr.query.collation.db2.enabled
    Value: true
    Type: java.lang.String

    Name: jcr.query.collation.en
    Value: en
    Type: java.lang.String

    Name: jcr.query.collation.sv
    Value: sv
    Type: java.lang.String

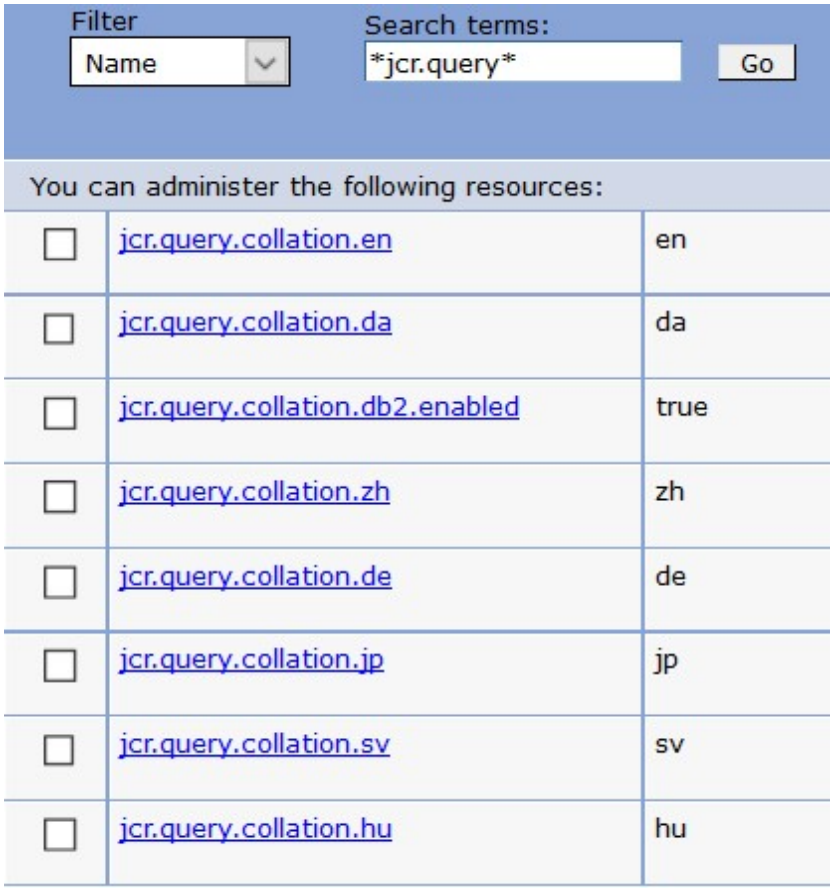
    Name: jcr.query.collation.zh
    Value: zh
    Type: java.lang.String

    Name: jcr.query.collation.de
    Value: de
    Type: java.lang.String

    Name: jcr.query.collation.da
    Value: da
    Type: java.lang.String

    Name: jcr.query.collation.hu
    Value: hu
    Type: java.lang.String

Name: jcr.query.collation.jp
Value: jp
Type: java.lang.String



42. Click **Mark Step Complete** for Step.5

43. Click **Run Step** for Step 6.

44. Restart the DB2 server. Run the following commands on the DB2 server:
    db2stop
    db2start

45. In the Config Wizard, click **Mark Step Complete** for Step 7.

46. In the Config Wizard, click, **Run Step** for Step 8 - Validate the database connection and environment..

    NOTE: If this step fails, click "View Result" and look for the first ERROR message in the log. Issues with this step are often caused by small typing mistakes in the DB URL and DB2 Library (driver paths) fields. You can click the left arrow to return to the page where those values are defined and ensure that all information and formatting is correct, then click right again, mark steps 1-6 as Complete or Skip Step, then run the validation again.

47. In the Config Wizard, click, **Run** Step for Step 9 - Transfer the database.

48. For Step 10 – switch back to your DB2 server as the db2inst1 user and open a terminal window. Navigate to /home/db2inst1/Desktop/CWScripts/scripts directory

49. Execute the following command:

    db2 -tvf GrantDB2RuntimeUserPrivileges.sql

50. On the Config Wizard, click **Mark Step Complete** for Step 10.

51. Click **Run Step** for Step 11 – Configure the JCR domain to support large files.

52. Click **Run Step** for Step 12 – Start the portal server.

53. Click **Finished.**

54. Verify that you can access your Portal on the web after the database transfer by navigating to:

    http://myprimaryportal.ibm.com:10039/wps/portal

    in a browser.

At this point, you have successfully installed HCL® Digital Experience and configured it to use an external database.

Chapter 3 – Installing and Configuring the Deployment Manager

In this section, you will install the Deployment Manager (dmgr) on a separate server. The installation of the dmgr will leverage the IBM® Installation Manager (IIM) tool - like the installation of the HCL® Digital Experience v9.5 server on the primary node in Chapter 1. In this guide, the installation was completed with a graphical user interface (GUI) using the root user with installation images on a local hard drive.

Installing IBM® Installation Manager

The IBM® Installation Manager, (IIM) is a tool that you can use to install and maintain your IBM® software packages. Wizards guide you through the steps that you must take to install, modify, update, roll back, or uninstall your IBM® products.

1. Open a terminal window and run:

   ping *mydmgr.ibm.com*

   where *mydmgr.ibm.com* is your fully qualified hostname.

2. In the same terminal window,

   run: ping localhost

   to verify that the localhost settings are properly configured on your server.

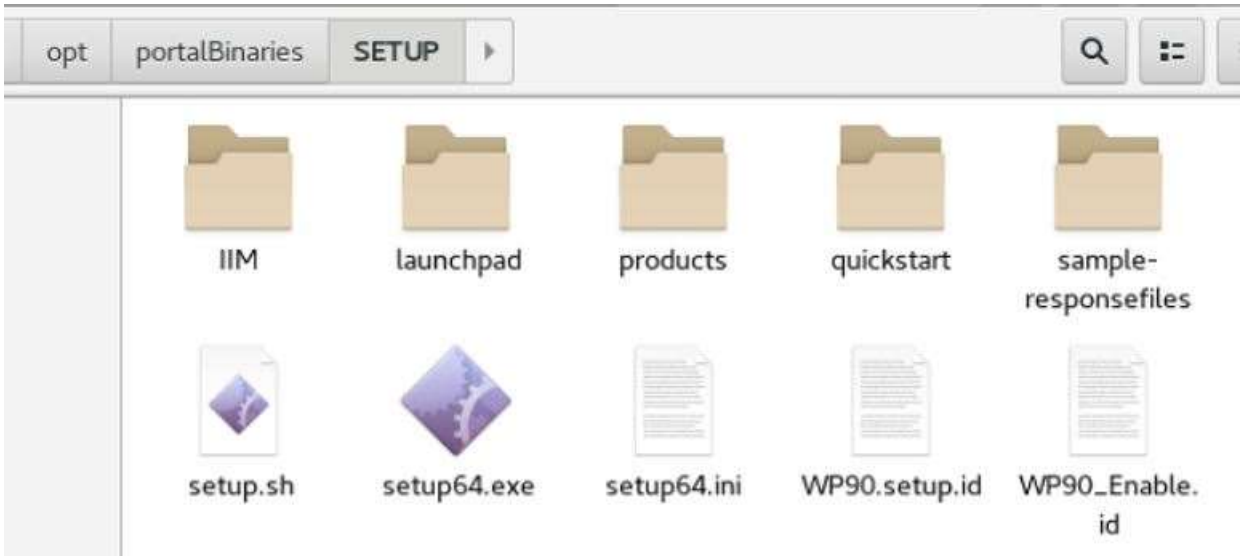
3. **Linux/UNIX environments only:** Ensure ulimit is set to 10240 or higher by running:

   ulimit -n 10240

   in the command line.

4. The installation media for the Deployment Manager is the same as the installation media for the Portal server. Unzip all .zip files provided with your Portal media into a single folder. This folder will be referred to as the installationMediaRoot folder.

   For this guide the following directory is used for the installationMediaRoot folder: /opt/portalBinaries/SETUP/products



5. From the HCL® Portal v9.5 SETUP directory, navigate to:

   SETUP/IIM/*yourEnvironment*

   and run

   ./install

   where *yourEnvironment* is the folder that best describes the operating system of the environment in which you are installing HCL® Portal. For this guide the following is used:

   installationMediaRoot/SETUP/IIM/linux_x86_64

The following window will appear:

6. Click **Next**.
7. Accept the license agreement and click **Next**.
8. Choose a directory in which to install IIM. This guide uses:

   /opt/IBM/InstallationManager/eclipse

   for Windows this guide recommends:

   c:\IBM\InstallationManager\eclpise

NOTE: In Windows environments, the default location will likely be C:\Program Files\IBM\InstallationManager. Spaces in the file path can cause problems later in the installation/configuration of Portal. It is good practice to create a folder called "IBM" at C:\IBM or a similar location into which IIM and HCL® Portal can be installed.

9. Click **Next**.
10. On the Summary screen, click **Install** to begin the installation.
11. When the installation is complete, click **Restart Installation Manager**.
12. In IIM, click **File > Preferences > Repositories.** Click **Add Repository** and add the following repositories:

    installationMediaRoot/WASND90/repository.config
    installationMediaRoot/JDK803/repository.config

    where *installationMediaRoot* is set to /opt/portalv9Binaries/SETUP/products in this guide

13. Click **Apply**>**OK**. Then, back on the home screen click **Install**.

14. Select the check box for **IBM WebSphere Application Server Network Deployment** and click **Next**.

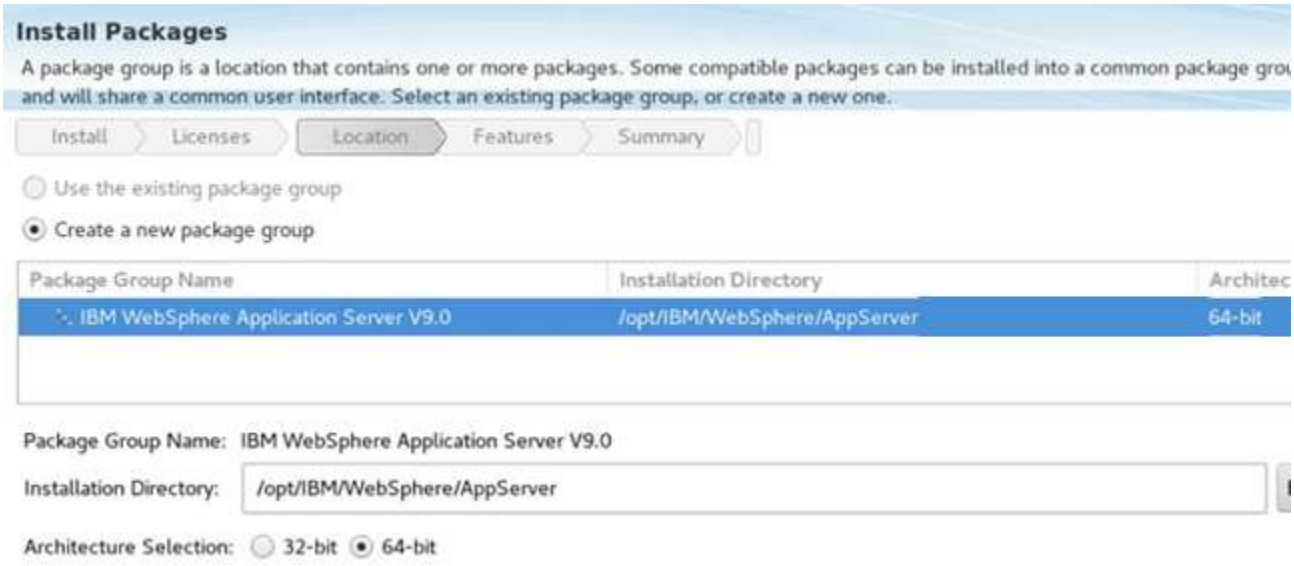
15. Accept the license agreement and click **Next**.

16. Select the location of the Shared Resources directory and click **Next**.

    This guide uses: /opt/IBM/IMShared

17. Select the Installation Location for your Deployment Manager and click **Next**.

    This guide uses: /opt/IBM/WebSphere/AppServer



18. Select any additional languages you want to install and click **Next**. For this guide, no additional languages were selected.

19. Select any additional features you want to install and click **Next**.

    This guide uses the defaults with SDK v8 selected

20. On the summary screen, click **Install**.

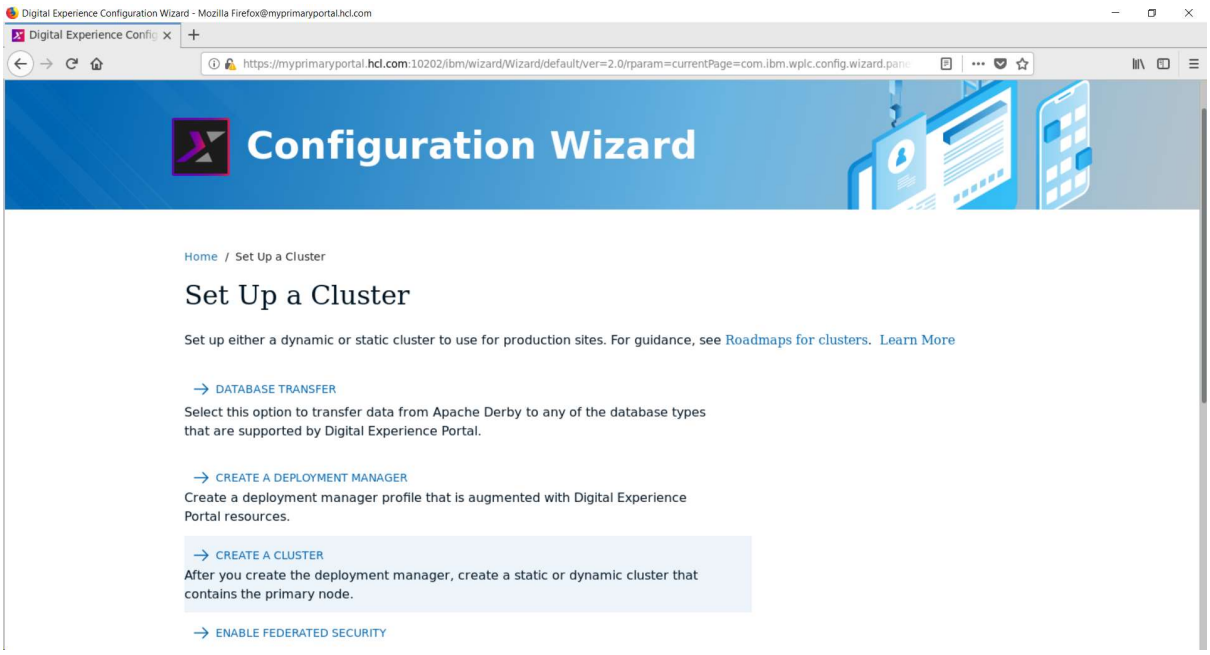
21. When the installation completes, select the radio button **None** for **Which program do you want to start?** and click **Finish**.

22. In this next sequence of steps, you will use the Configuration Wizard to create and configure a profile for the Deployment Manager. Open the Configuration Wizard (Config Wizard) in a web browser by navigating to:

    http://myprimaryportal.ibm.com:10200/hcl/wizard

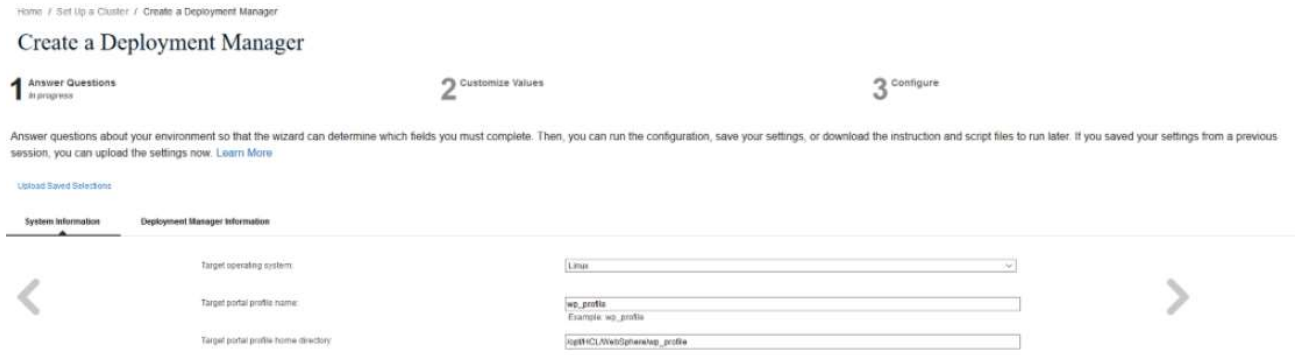
    Log in with your *ConfigWizardID* and *ConfigWizardPswdConfig* credentials.

23. On the Config Wizard Home Screen, click **Set Up a Cluster>Create a Deployment Manager**.



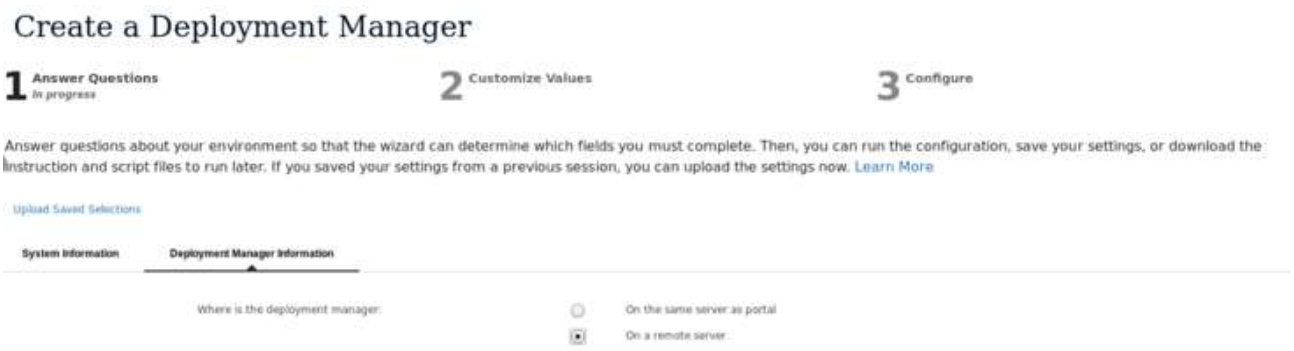
24. Choose your target operating system, name of your Portal profile, and the Portal profile location The profile name and profile location pre-populated values are the defaults.

NOTE: wp_profile is the correct value for the **Target portal profile name** field.



Click the right arrow.

25. Select **On a remote server** for the deployment manager location.



Click the right arrow.

26. Fill in the hostname of your primary Portal server.

Click the right arrow.

27. Fill in the following values (examples given):

Deployment manager host name: **mydmgr.ibm.com**,

New deployment manager profile name: **dmgr01**

Deployment manager profile path:
/opt/HCL/WebSphere/AppServer/profiles/dmgr01

Deployment manager cell name: this guide uses the default, **dmgrCell01**, but you can change it to anything EXCEPT the name of the previously created Portal cell.

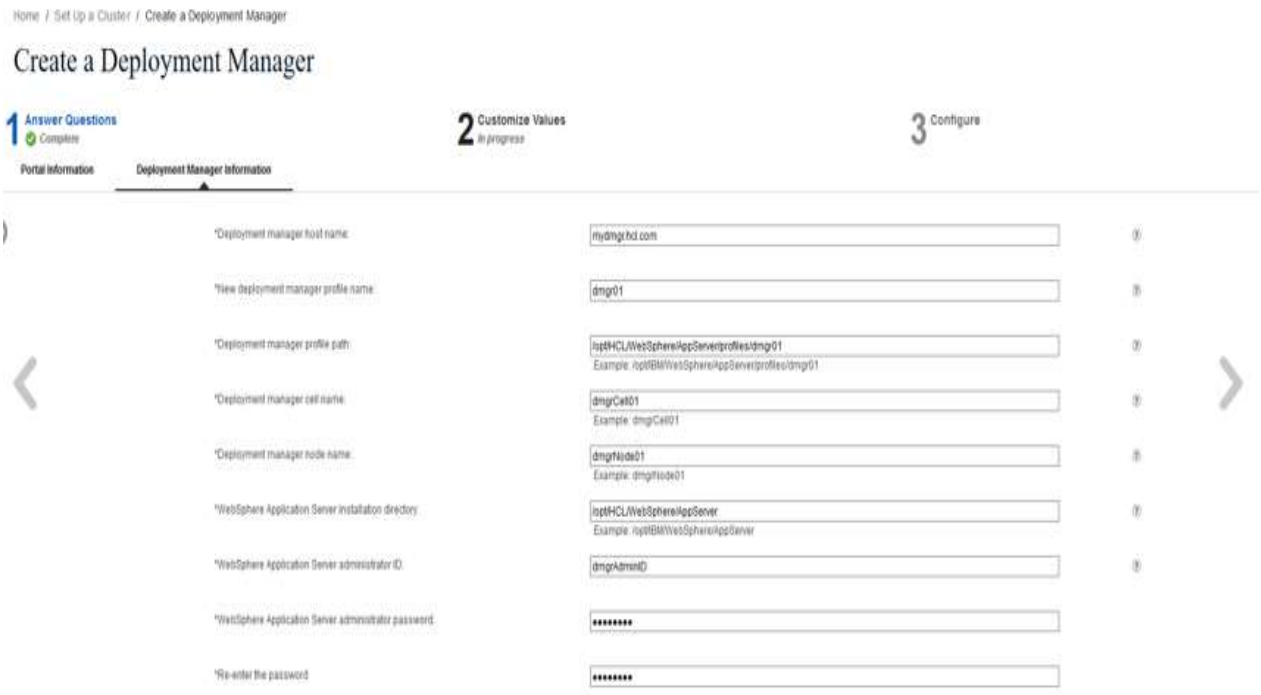
Deployment manager node name: this guide uses the default, **dmgrNode01**, but you can change it to anything EXCEPT the name of the previously created Portal node.

WebSphere Application Server installation directory:
/opt/HCL/WebSphere/AppServer

WebSphere Application Server administrator ID: ***dmgrAdminID***

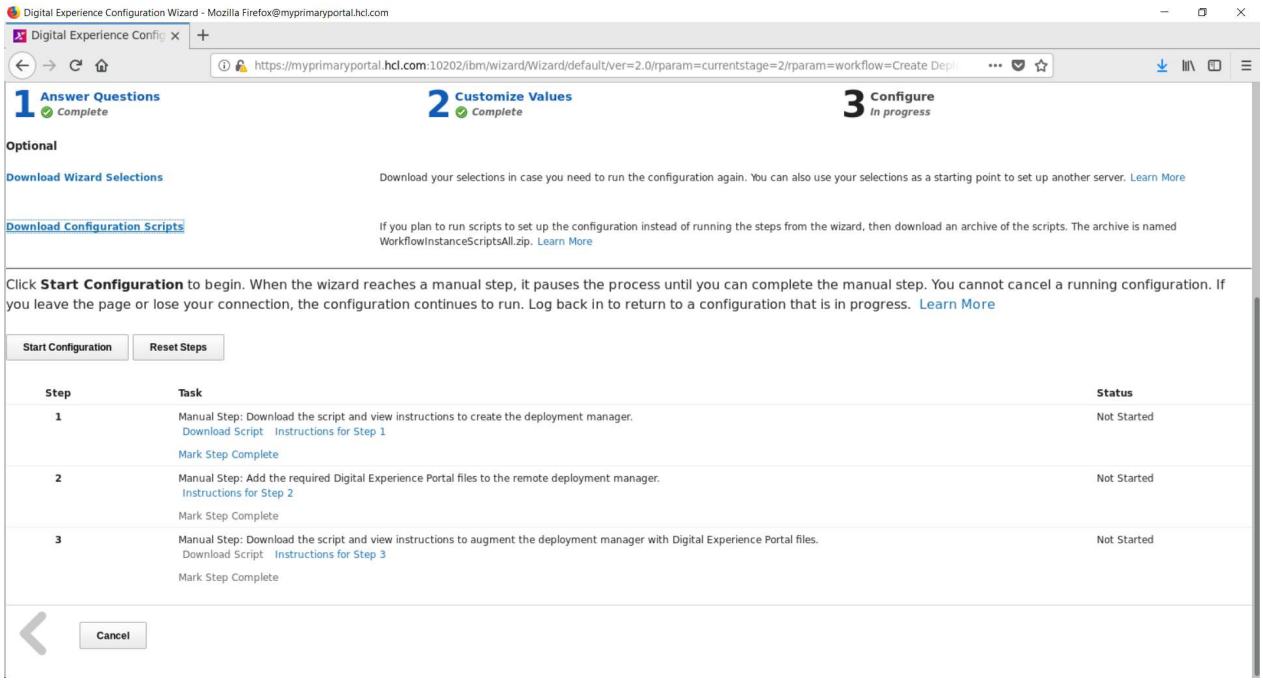
WebSphere Application Server administrator password: ***dmgrAdminPswd***

Re-enter the password: your ***dmgrAdminPswd*** again



Click the right arrow.

28. The following screen will appear:



29. Click **Download Configuration Scripts,** save WorkflowInstanceScriptsAll.zip in an easily accessible location, then unzip it.

30. Copy the following files and save them in a temporary location on the dmgr server: AugmentRemoteDeploymentManagerProfile CreateRemoteDeploymentManagerProfile

For this guide, they were placed in the following location:

/tmp/Scripts

31. Change the permissions on this folder as follows:

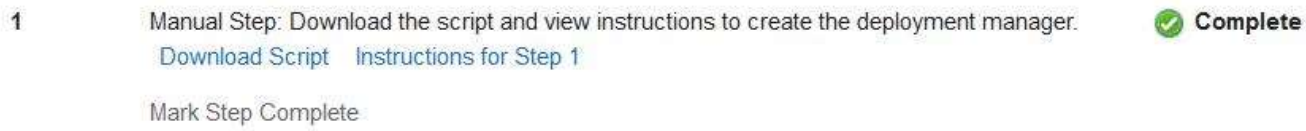
chmod -R 777 /tmp/Scripts

32. Change the name of "CreateRemoteDeploymentManagerProfile" to "CreateRemoteDeploymentManagerProfile.sh"

33. Run CreateRemoteDeploymentManagerProfile.sh:

./CreateRemoteDeploymentManagerProfile.sh

34. Click **Mark Step Complete** for Step 1 – Download the script and view instructions to create the Deployment Manager.

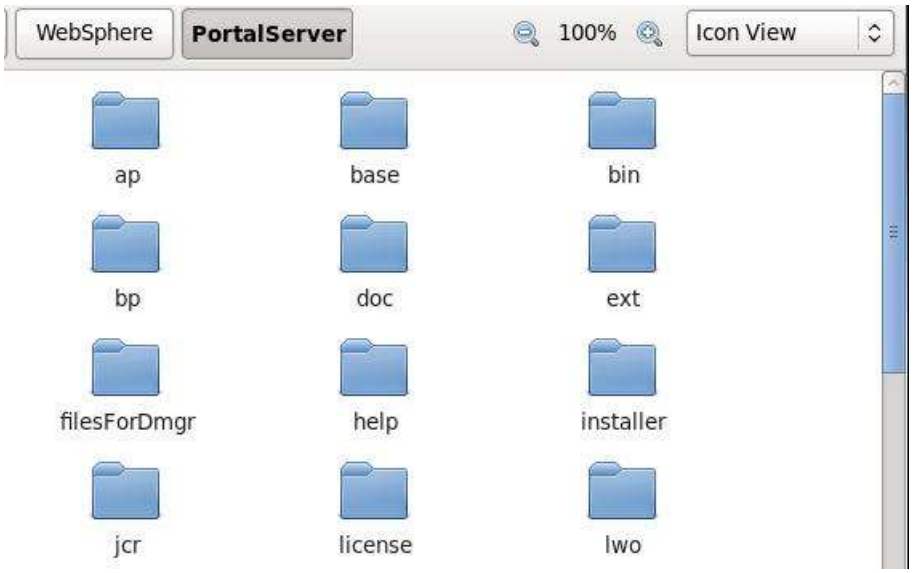


35. Ensure that the newly created dmgr is stopped:

cd /opt/HCL/WebSphere/AppServer/profiles/dmgr01/bin

./stopManager.sh -user *dmgrAdminID* -password *dmgrAdminPswd*

36. Back on the Primary Portal Server, navigate to *WebSphereInstallationRoot*/PortalServer:



/opt/IBM/WebSphere/PortalServer

37. Copy the folder named "filesforDmgr" and save it in the /tmp directory on the Deployment Manager Server.

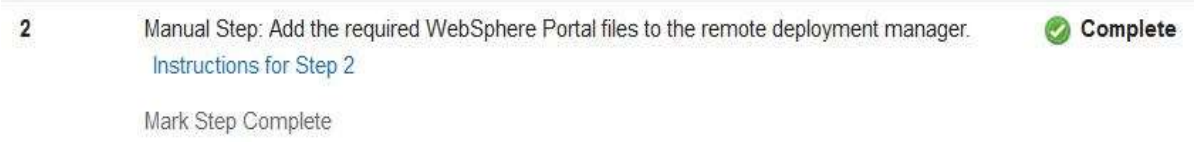
38. Open the filesforDmgr folder on the dmgr Server. Move the filesforDmgr.zip file in this directory to the AppServer directory and unzip it there. Example:

    mv /tmp/filesForDmgr/filesForDmgr.zip /opt/HCL/WebSphere/AppServer
    cd /opt/HCL/WebSphere/AppServer
    unzip filesforDmgr.zip

39. If the deployment manager profile was not created in the default ${WasHome}/profiles/Dmgr01 directory, then the metadata_wkplc.xml file, which is in the ${WasHome}/profiles/Dmgr01/config/.repository directory in the compressed file, must be copied into the config/.repository subdirectory under the deployment manager profile directory.

    Please notice:
    This guide used a non-default name of dmgr01and thus ran the following command:
    cp /opt/HCL/WebSphere/AppServer/profiles/Dmgr01/config/.repository/metadata_wkplc.xml /opt/HCL/WebSphere/AppServer/profiles/dmgr01/config/.repository/

40. Back on the Config Wizard, click **Mark Step Complete** for Step 2 – Add the required WebSphere Portal files to the remote deployment manager.



41. On the dmgr Server, change the name of the file

    AugmentRemoteDeploymentManagerProfile
    to
    AugmentRemoteDeploymentManagerProfile.sh

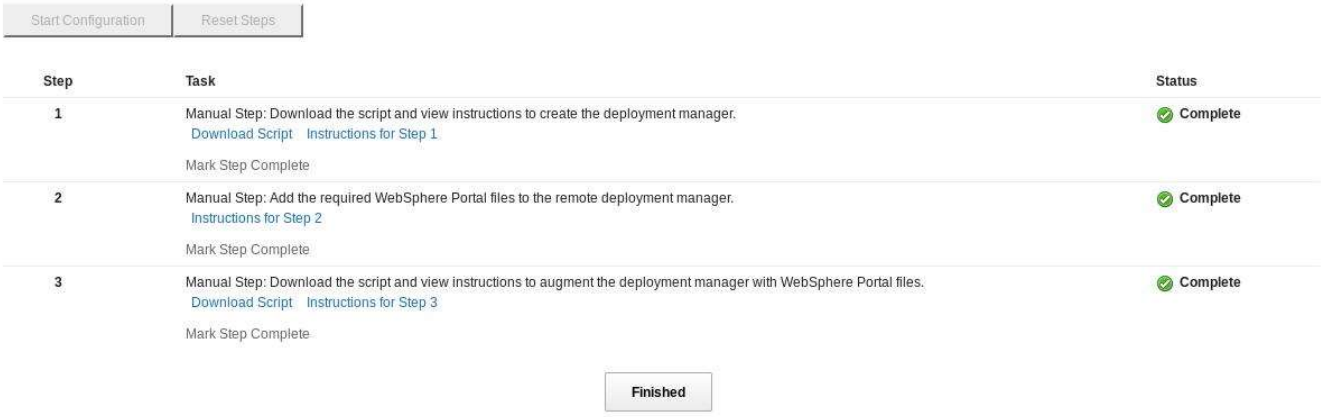
42. Run the AugmentRemoteDeploymentManagerProfile.sh script
    cd /tmp
    ./AugmentRemoteDeploymentManagerProfile.sh

    When this is complete you should see the line "Profile augmentation succussed" about one third of the way down in the command line output.

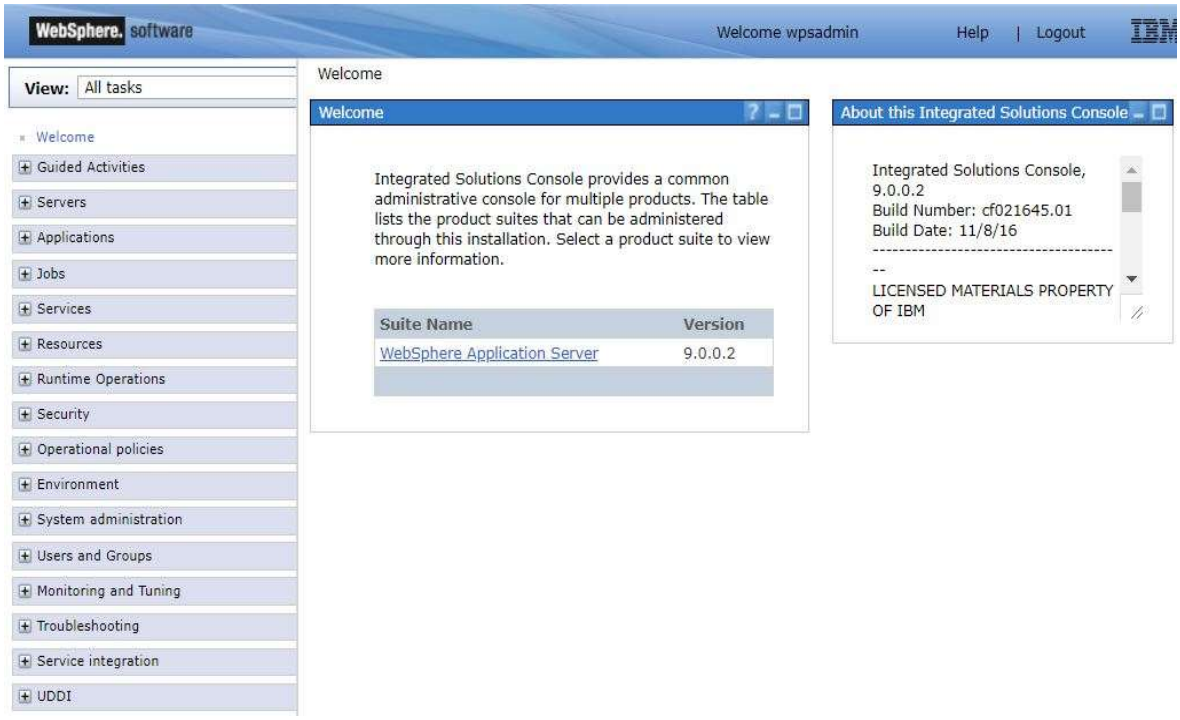
```
[root@myprimaryportal scripts]# ./AugmentRemoteDeploymentManagerProfile.sh
ADMU0116I: Tool information is being logged in file
           /opt/HCL/WebSphere/AppServer/profiles/dmgr01/logs/dmgr/startServer.log
ADMU0128I: Starting tool with the dmgr01 profile
ADMU3100I: Reading configuration for server: dmgr
ADMU3200I: Server launched. Waiting for initialization status.
ADMU3000I: Server dmgr open for e-business; process id is 8878
INSTCONFSUCCESS: Profile augmentation succeeded.
ADMU0116I: Tool information is being logged in file
           /opt/HCL/WebSphere/AppServer/profiles/dmgr01/logs/dmgr/stopServer.log
ADMU0128I: Starting tool with the dmgr01 profile
ADMU3100I: Reading configuration for server: dmgr
ADMU3201I: Server stop request issued. Waiting for stop status.
ADMU4000I: Server dmgr stop completed.

ADMU0116I: Tool information is being logged in file
           /opt/HCL/WebSphere/AppServer/profiles/dmgr01/logs/dmgr/startServer.log
ADMU0128I: Starting tool with the dmgr01 profile
ADMU3100I: Reading configuration for server: dmgr
ADMU3200I: Server launched. Waiting for initialization status.
ADMU3000I: Server dmgr open for e-business; process id is 9401
[root@myprimaryportal scripts]#
```

43. Click **Mark Step Complete** for Step 3 – Download the script and view instructions to augment the deployment manager with HCL® Portal files

44. Click Finished



45. Verify that you can access your newly created Deployment Manager's console by opening a web browser and navigation to:
https://mydmgr.ibm.com:9043/ibm/console



At this point, you have installed the Deployment Manager and created a dmgr profile.

46. Add Portal admin user (PortalAdminID) in WAS Admin console then add to wasadmins group

Chapter 4 – Federating and Clustering the Primary Node

In this section you will create a cluster using the Configuration Wizard, add the Primary Portal Node to this cluster, and federate the Primary Node.

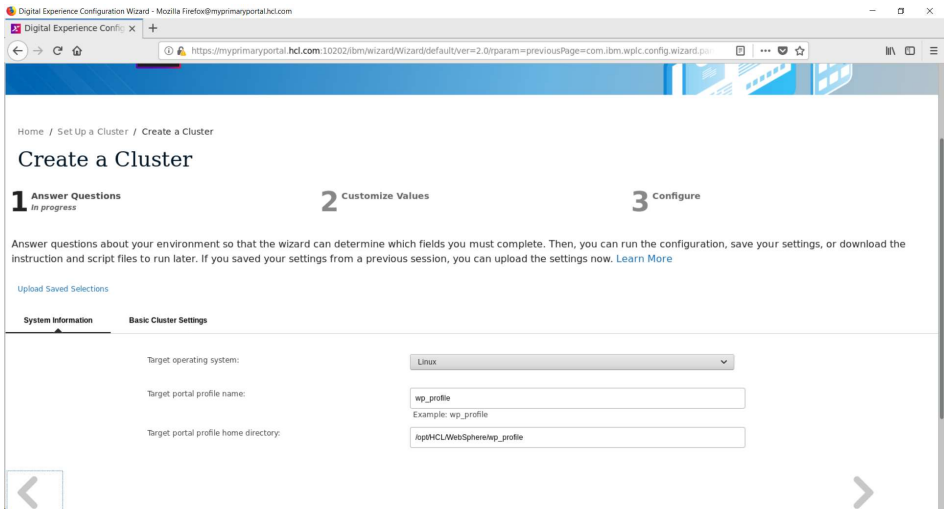
1. Open the Configuration Wizard in a web browser:

   http://myprimaryportal.hcl.com:10200/hcl/wizard

   and sign in with your *ConfigWizardID and ConfigWizardPswd*.

2. On the Config Wizard Home screen, Click **Set Up a Cluster>Create a Cluster**.

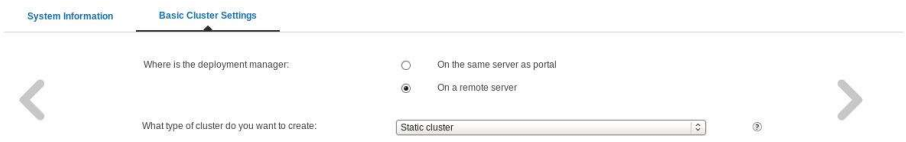
3. Select your target operating system, Portal profile name, and Portal profile home directory.



   Click the right arrow.

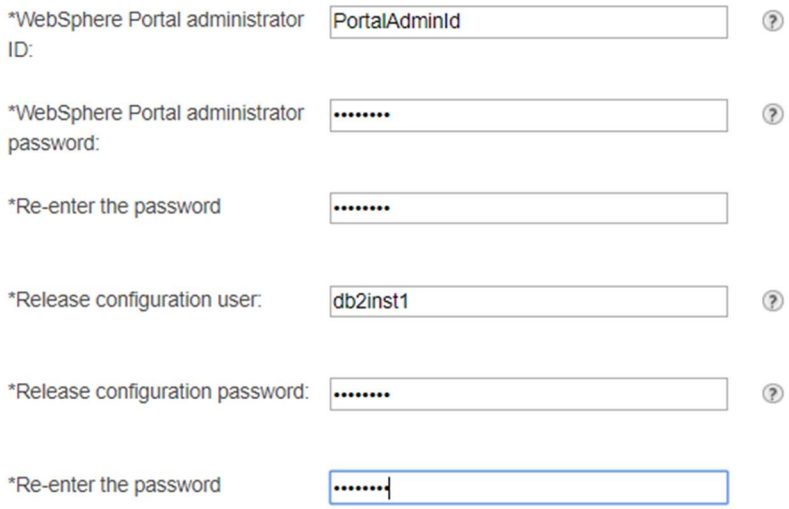
4. Select the deployment manager's location and the type of cluster you are creating. This guide uses a static cluster with a remote Deployment Manager. For more information on static and dynamic clustering, see the following documentation:

   https://help.hcltechsw.com/digital-experience/9.5/plan/plan_clus_ovr.html
   https://help.hcltechsw.com/digital-experience/9.5/plan/plan_xdclus.html



   Click the right arrow.

5. Fill in your Portal Administrator ID, Portal Administrator password, release database configuration userID and release configuration user database password.

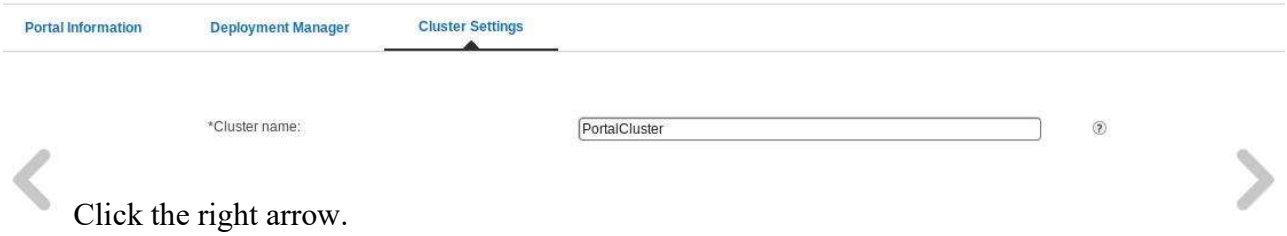


Click the right arrow.

6. Fill in your *dmgrAdminID*, *dmgrAdminPswd*, *dmgrAdminPswd* again, dmgr Cell name, dmgr Node name, dmgr profile path dmgr host name, and dmgr soap port. All values were specified previously during dmgr installation. The SOAP port default is 8879, which this guide uses.

Click the right arrow.

7. Choose a cluster name. For this guide, the default, **PortalCluster**, is used.



Click the right arrow.

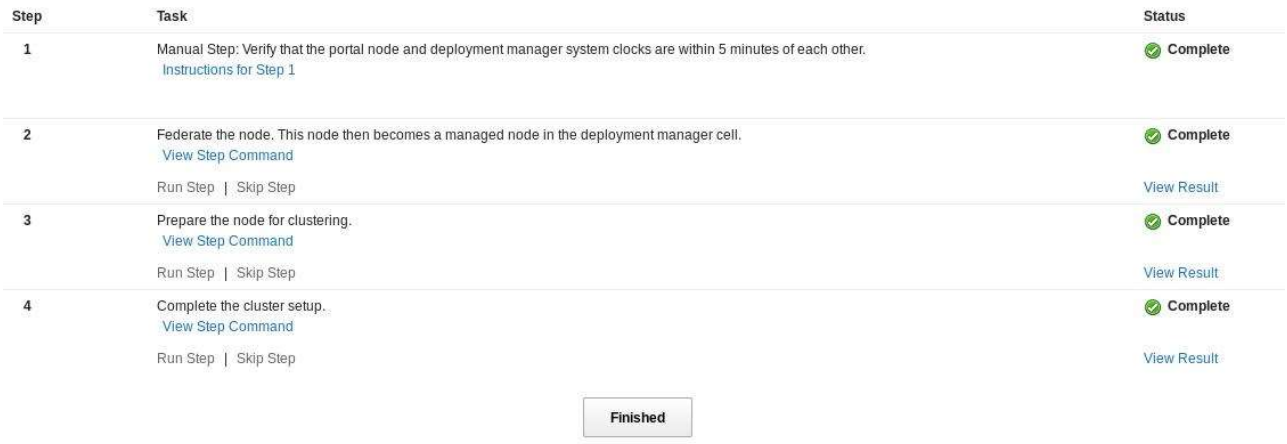
8. Check the system clocks on the Primary Portal Server and the Deployment Manager Server and ensure that their times are within five minutes of each other. Mark Step 1 on the Config Wizard **Create a Cluster** page complete.

9. For Step 2 – Federate the node, click **Run Step**.

10. For Step 3 – Prepare the node for clustering, click **Run Step**. This will run the post-federation configuration engine task.

11. For Step 4 – Complete the cluster setup, click **Run Step**. This will run the cluster-setup configuration engine task.

12. After all four steps have been successfully completed, click **Finish**.

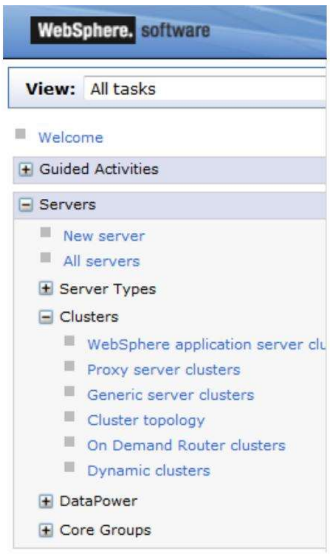


13. Verify that you can access your Portal in a web browser:
http://myprimaryportal.hcl.com:10039/wps/portal

14. Open the dmgr console in a web browser:
https://mydmgr.hcl.com:9043/ibm/console

15. Login to the dmgr using your *dmgrAdminID* and *dmgrAdminPswd*.

16. On the left side, click **Servers>Clusters>WebSphere application server clusters** and ensure that your newly created cluster **PortalCluster** is present. Click to the Portal Cluster name.

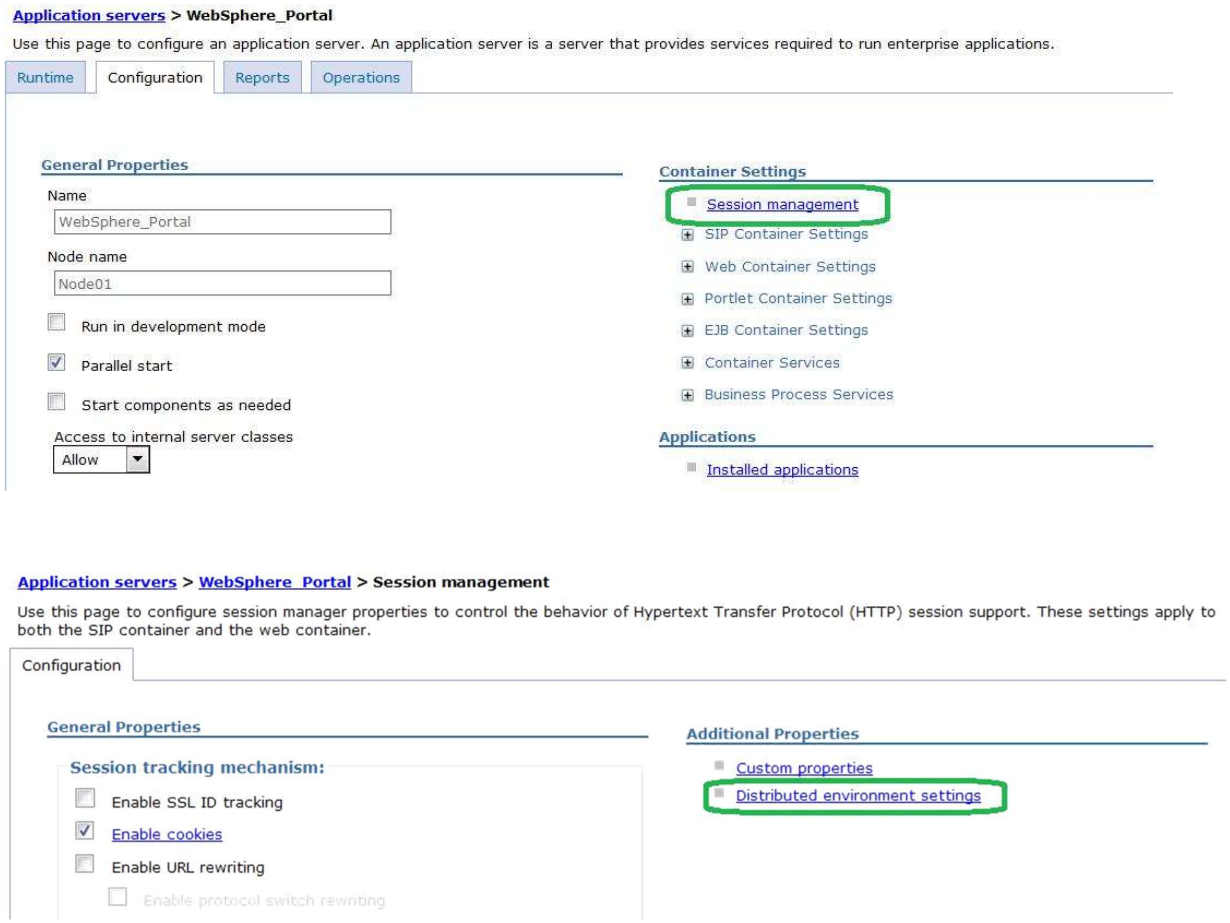


In the following steps, you will enable Memory-to-Memory replication for the primary cluster member.

Special note on Memory-to-Memory (M2M) replication: M2M replication takes session data from one Portal sever and copies it to another Portal server. This is useful in situations where one Portal server catastrophically fails. Failover to an additional Portal server in the cluster can occur with no disruption for the end user. The user's session data will be retained. M2M's disadvantage is the additional overhead needed to store and replicate the session data across all cluster members.
Suppose you have a two server cluster without M2M enabled. Each server utilizes 1GB of memory to store session data. With M2M enabled, each server would now consume 2GB of session data. In a ten server cluster, assuming similar scaling, it would be 10GB of session data. Similar scaling with CPU would be needed to ensure replication of data could occur, which is necessary for successful failover.

HCL® has generally found that most Portal environments can safely enable M2M replication. For larger scale Portal deployments M2M does not scale and alternatives are recommended. Replication domains, session databases and WebSphere Extreme Scale caching are three examples of many alternatives that may perform better for scaling purposes. Open a case with HCL® software support to discuss details of options available if you have a larger-scale Portal environment.

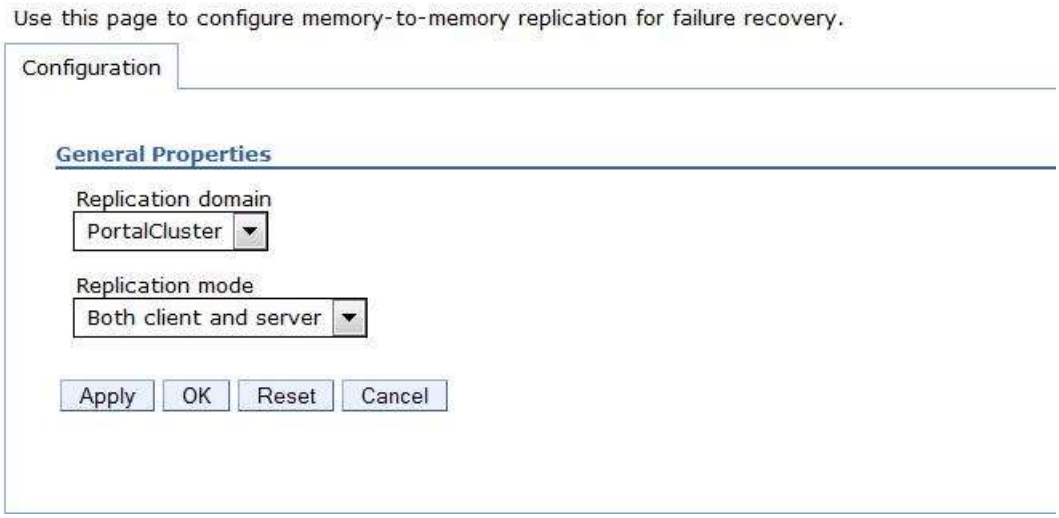
17. While logged in to the dmgr, navigate to **Servers → Server Types → WebSphere application servers → WebSphere_Portal → Session Management → Distributed Environment Settings**.



18. Click the blue link for **Memory-to-memory replication**.

19. In the Replication Domain drop-down menu, select your cluster (e.g. PortalCluster).

20. In the Replication Mode drop-down menu, select **Both client and server**.



21. Click **OK** and Save all changes.

22. Back on the **Session management** page (which you should see after saving the changes), click **Custom Properties**.

23. Create a new custom property by clicking **New**.

24. For the **Name**, type in “UseInvalidatedId” and for the **Value**, type in “false”

25. Click **OK** and save the changes.

26. Restart the DMGR, NodeAgent, and WebSphere_Portal server.

27. Verify Portal is functional by accessing it in your web browser:

    http://myprimaryportal.hcl.com:10039/wps/portal

At this point you have successfully completed building a one-node cluster using the out of the box security configuration. In the remaining sections, you will configure the Portal cluster with a federated LDAP and add an additional horizontal node to the cluster.

Chapter 5 – Configuring the Portal Cluster for Federated LDAP Security

This section covers adding a federated LDAP Server to the cluster's security configuration. For more details about LDAP/Security configuration, refer to the product documentation:

https://help.hcltechsw.com/digital-experience/9.5/config/cw_ldap.html?

NOTE:
The screenshots in this chapter are taken from a Portal system with cumulative fix 17 installed. If your installation has a different cumulative fix level, your Config Wizard options and screens could differ slightly from those shown in this guide.

If you have user ID's stored in your LDAP that are the same as your Portal or WAS administrator ID's, or if you have a preexisting LDAP group named wpsadmins, either of these conditions will cause a failure while executing the steps in this chapter. See Appendix D2 if this condition applies to you and before executing the steps in this chapter.

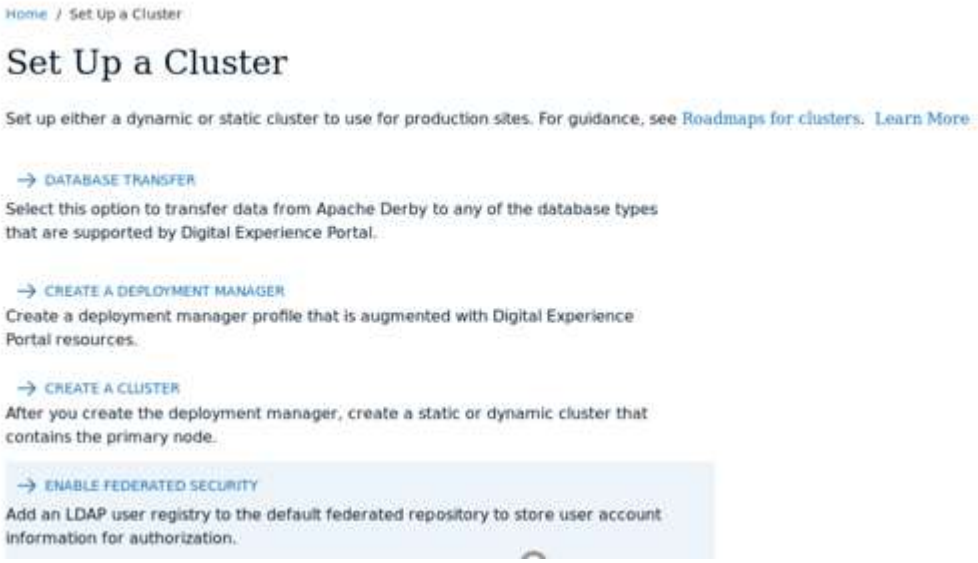
This guide uses an IBM® Directory Server LDAP server to configure security in the cluster. Your LDAP server may be different. Review the following Portal and LDAP Integration guide, especially if this is your first time configuring Portal with an LDAP server.

https://manualzz.com/doc/35945197/guide-to-integrating-websphere-portal-v8.5-with-ldap

The guide is applicable to both HCL® Portal v8.5, v9.0 and v9.5. The guide will help you identify the configuration values needed for this section.

1. Open the Configuration Wizard (Config Wizard) in a web browser
   http://myprimaryportal.hcl.com:10200/hcl/wizard

2. Click **Set Up a Cluster>Enable Federated Security**.

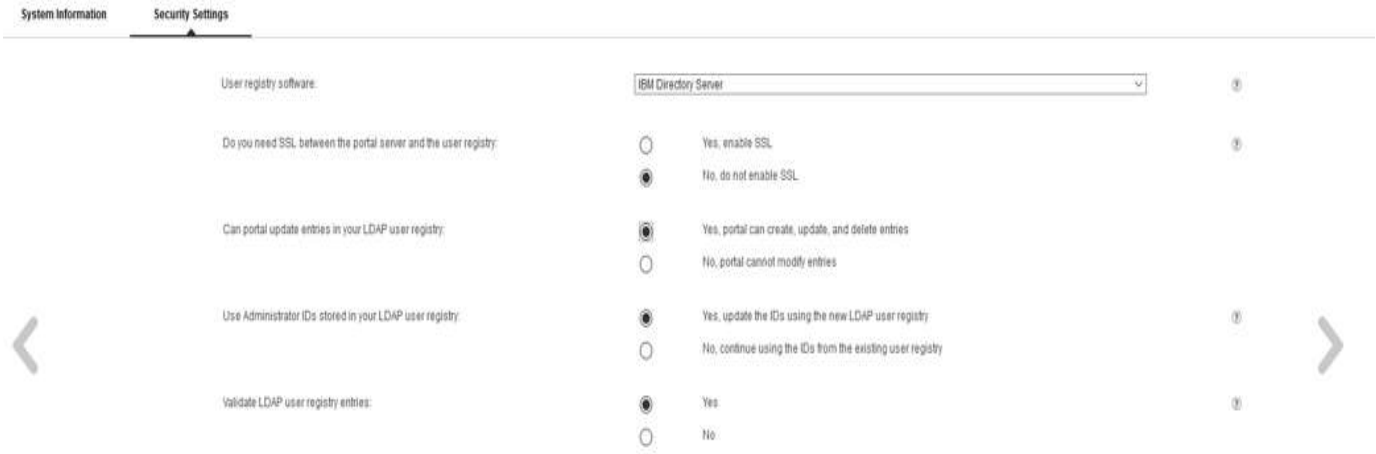


3. Specify your target operating system, primary Portal profile name, and path to the primary Portal profile.

   Click the right arrow.

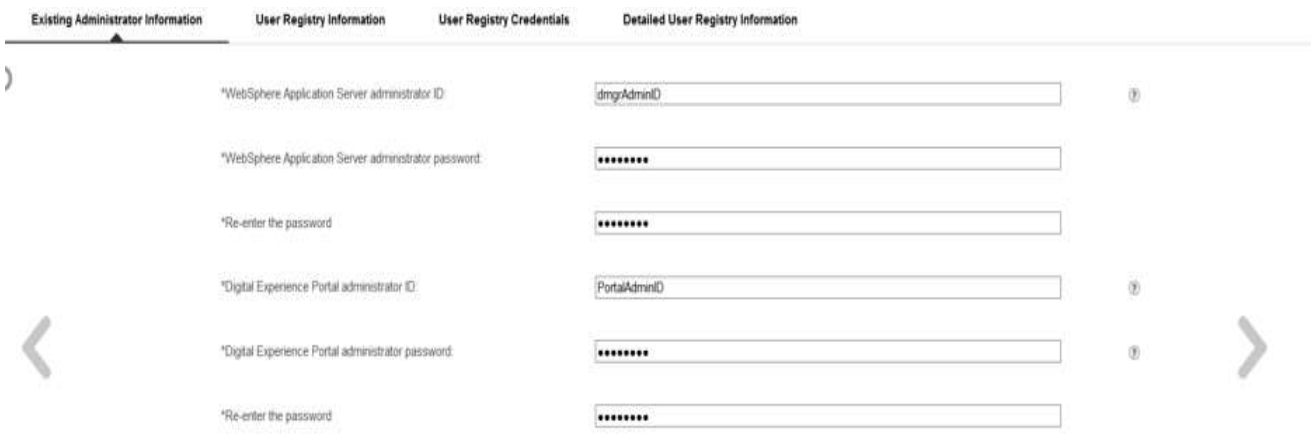
4. Specify the following values:

    - User registry software: Your LDAP software type; **IBM Directory Serve**r for this guide.
    - Do you need SSL between the portal server and the user registry: **No** for this guide.
    - Can portal update entries in your LDAP registry: **Yes** if Portal is used for user registration or similar information creation/updates. No if Portal will use your LDAP data as read only. Yes for this guide.
    - Use Administrator ID's stored in your LDAP user registry: **Yes** if you want your Portal administrator credentials to be stored in your LDAP system. If this is a production system, you MUST select Yes. No if you want to continue to use the Portal administrator credentials stored in the Portal file system AND this is a non-production system. Yes for this guide.
    - Validate LDAP user registry entries: Choosing **Yes** and the configuration wizard will do real-time value checks against the ldap server.



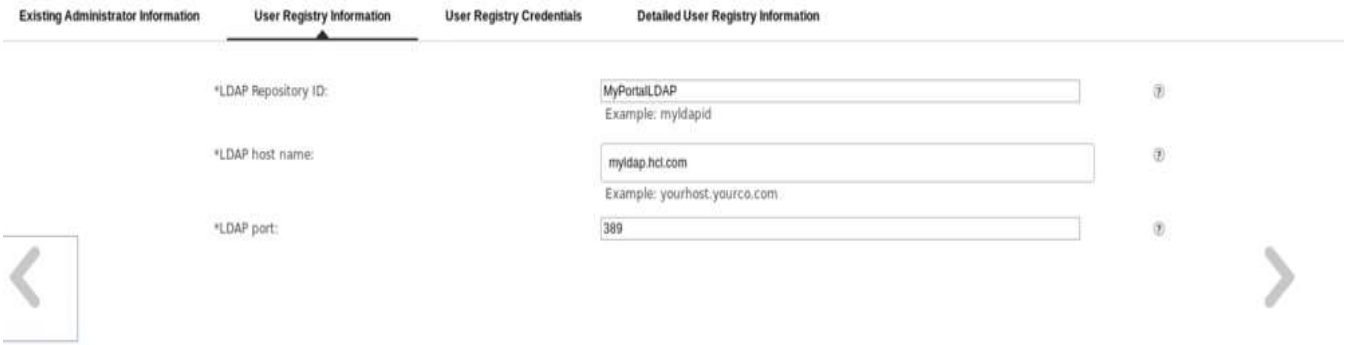
Click the right arrow.

5. Specify your *PortalAdminID*, *PortalAdminPswd* and *PortalAdminPswd* again. These values will match those that were specified during the Portal installation. Do not input values for userIDs or passwords in LDAP - those will be entered in a later step.



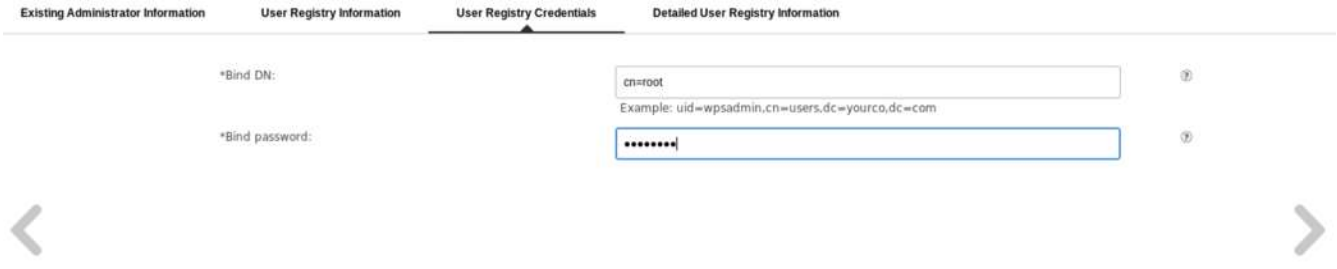
Click the right arrow.

6. Enter a repository ID value. This is a descriptive label used to identify this LDAP in your Portal configuration. Also specify your LDAP host name and LDAP port number. The default LDAP port for most LDAP servers is port 389.



Click the right arrow

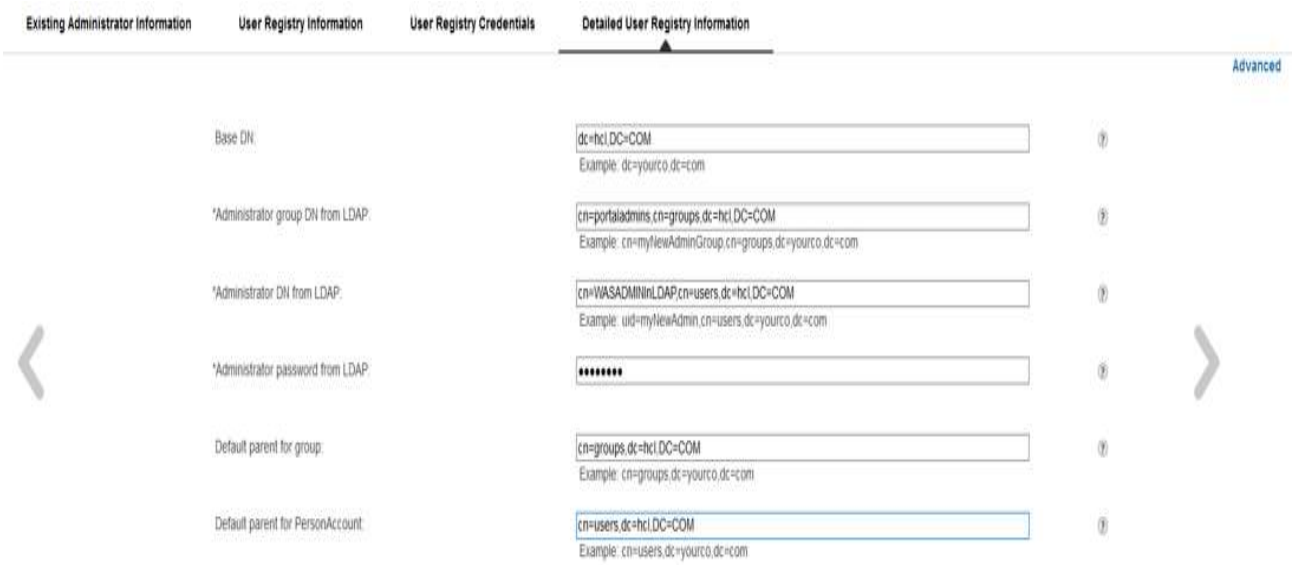
7. Enter the Bind DN and Bind password.



Click the right arrow

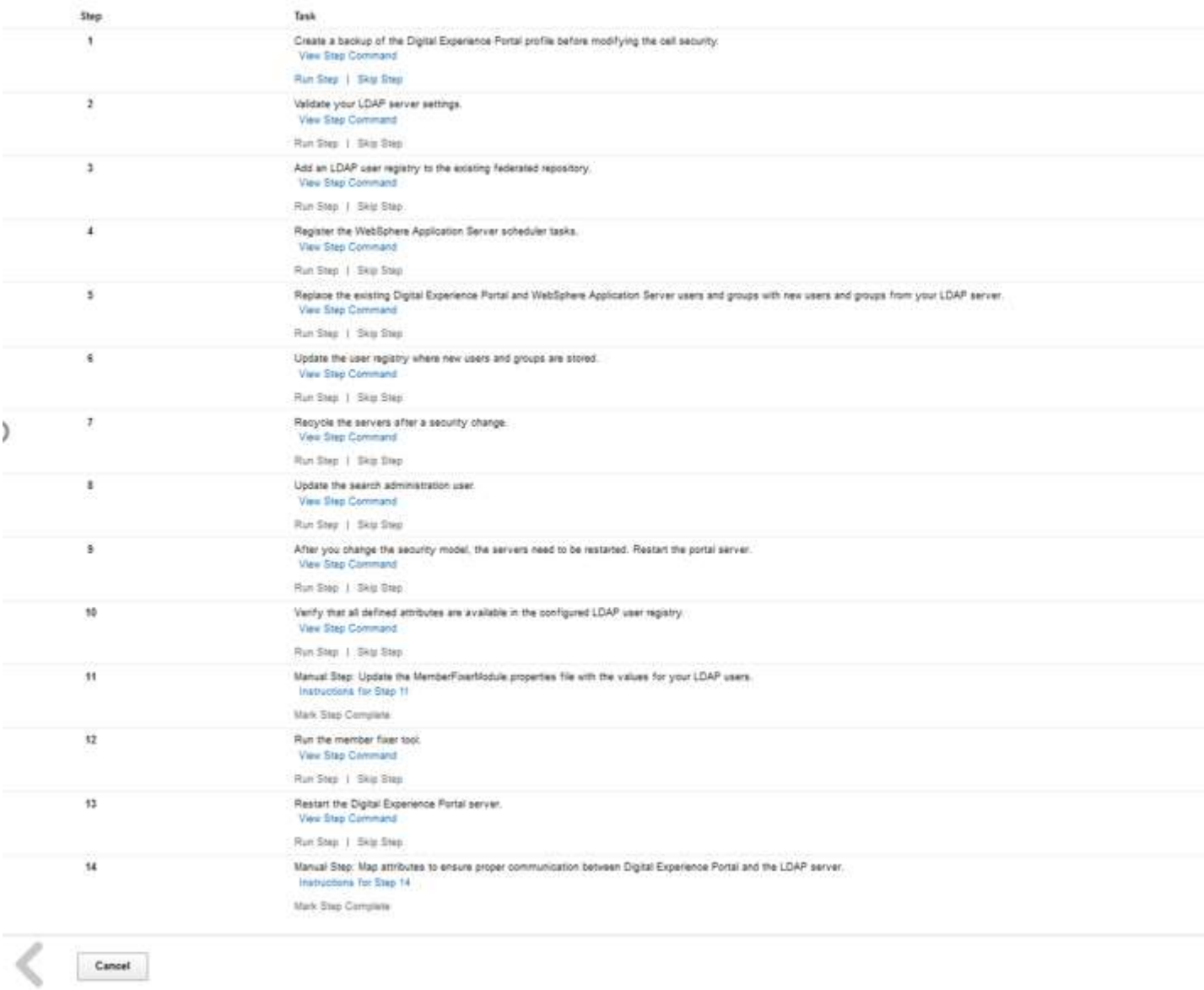
8. Enter the Base DN, Administrator group/user DN, LDAP Administrator password, default parent for new groups created by Portal, and the default parent for entry type PersonAccount.

   This guide followed the LDAP Integration Guide link at the beginning of this chapter to determine appropriate values to enter. Consult with your LDAP administrator if you are uncertain which values to use for your LDAP:



   Click the right arrow.

9. You will see the following screen



Step	Task
1	Create a backup of the Digital Experience Portal profile before modifying the cell security. View Step Command Run Step | Skip Step
2	Validate your LDAP server settings. View Step Command Run Step | Skip Step
3	Add an LDAP user registry to the existing federated repository. View Step Command Run Step | Skip Step
4	Register the WebSphere Application Server scheduler tasks. View Step Command Run Step | Skip Step
5	Replace the existing Digital Experience Portal and WebSphere Application Server users and groups with new users and groups from your LDAP server. View Step Command Run Step | Skip Step
6	Update the user registry where new users and groups are stored. View Step Command Run Step | Skip Step
7	Recycle the servers after a security change. View Step Command Run Step | Skip Step
8	Update the search administration user. View Step Command Run Step | Skip Step
9	After you change the security model, the servers need to be restarted. Restart the portal server. View Step Command Run Step | Skip Step
10	Verify that all defined attributes are available in the configured LDAP user registry. View Step Command Run Step | Skip Step
11	Manual Step: Update the MemberFixerModule.properties file with the values for your LDAP users. Instructions for Step 11 Mark Step Complete
12	Run the member fixer tool. View Step Command Run Step | Skip Step
13	Restart the Digital Experience Portal server. View Step Command Run Step | Skip Step
14	Manual Step: Map attributes to ensure proper communication between Digital Experience Portal and the LDAP server. Instructions for Step 14 Mark Step Complete

Cancel

Click **Run Step** for Steps 1 - 10

10. On the Primary portal server, locate the file named“MemberFixerModule.properties” in following directory:
/opt/HCL/WebSphere/wp_profile/PortalServer/wcm/shared/app/config/wcmservices

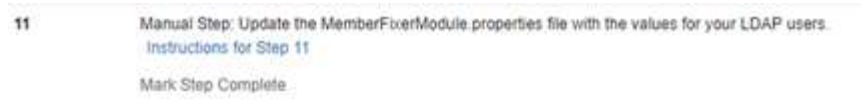
Open the MemberFixerModule.properties file with a text editor. Add the following line, using the full Distinguished Name for the *WASAdminInLDAP* userID. This guide added the following line:

uid=PortalAdminID,o=defaultWIMFileBasedRealm -> uid=WASADMINInLDAP,cn=users,dc=hcl,DC=COM

and save the changes to the file.
For more information on this step, click **Instructions for Step 10** in the Config Wizard.

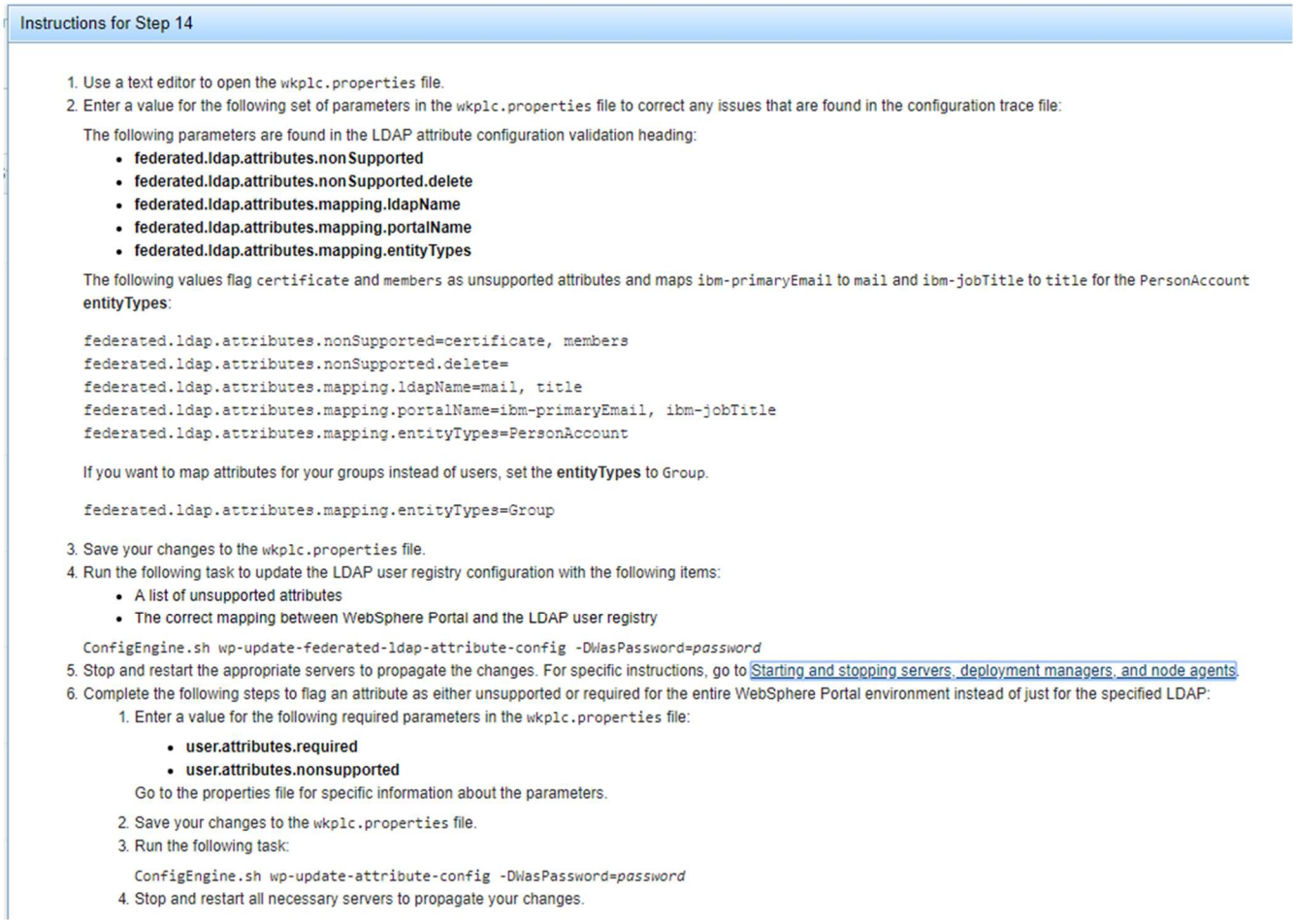
```
################################################################################
#
# Member Fixer Module Configuration Properties
#
# This file can be configured to provide custom distinguished name (DN)
# mapping for the member fixer module.
#
################################################################################

# Configure full replacement of one distinguished name with another
#
# Example: To replace any instance of cn=group1,dc=lotus,o=ibm with cn=group2,dc=rational,o=ibm, use:
# cn=group1,dc=lotus,o=ibm -> cn=group2,dc=rational,o=ibm
#
# uid=user1,ou=websphere,c=au,o=ibm -> uid=user2,ou=tivoli,c=au,o=ibm
# cn=group1,dc=lotus,o=ibm -> cn=group2,dc=rational,o=ibm

# Configure part replacement of a distinguished names. This will
# change all of the distinguished name except the ID
#
# Example: To replace all DNs like cn=[ID],dc=websphere,o=ibm with cn=[ID],dc=tivoli,o=ibm, use:
# cn=[ID],dc=websphere,o=ibm -> cn=[ID],dc=tivoli,o=ibm
#
# uid=[ID],ou=websphere,c=au,o=ibm -> uid=user2,ou=tivoli,c=au,o=ibm
# cn=[ID],dc=websphere,o=ibm -> cn=[ID],dc=tivoli,o=ibm
uid=PortalAdminID,o=defaultWIMFileBasedRealm -> uid=WASADMINInLDAP,cn=users,dc=hcl,DC=COM
```

Click **Mark Step Complete** for step 11 in the Config Wizard.



11. Click **Run Step** for Step 12. Click **Run Step** for Step 13.

12. **NOTE**: The final step ,Step 14, was skipped for this guide as no additional attribute mapping was required. If you need to complete this step, Click "**Instructions for Step 14**" and follow the provided steps. Otherwise Click **Mark Step Complete.**



Instructions for Step 14

1. Use a text editor to open the `wkplc.properties` file.
2. Enter a value for the following set of parameters in the `wkplc.properties` file to correct any issues that are found in the configuration trace file:

   The following parameters are found in the LDAP attribute configuration validation heading:
   - **federated.ldap.attributes.nonSupported**
   - **federated.ldap.attributes.nonSupported.delete**
   - **federated.ldap.attributes.mapping.ldapName**
   - **federated.ldap.attributes.mapping.portalName**
   - **federated.ldap.attributes.mapping.entityTypes**

   The following values flag `certificate` and `members` as unsupported attributes and maps `ibm-primaryEmail` to `mail` and `ibm-jobTitle` to `title` for the `PersonAccount` **entityTypes**:

   ```
   federated.ldap.attributes.nonSupported=certificate, members
   federated.ldap.attributes.nonSupported.delete=
   federated.ldap.attributes.mapping.ldapName=mail, title
   federated.ldap.attributes.mapping.portalName=ibm-primaryEmail, ibm-jobTitle
   federated.ldap.attributes.mapping.entityTypes=PersonAccount
   ```

   If you want to map attributes for your groups instead of users, set the **entityTypes** to `Group`.

   ```
   federated.ldap.attributes.mapping.entityTypes=Group
   ```

3. Save your changes to the `wkplc.properties` file.
4. Run the following task to update the LDAP user registry configuration with the following items:
   - A list of unsupported attributes
   - The correct mapping between WebSphere Portal and the LDAP user registry

   ```
   ConfigEngine.sh wp-update-federated-ldap-attribute-config -DWasPassword=password
   ```
5. Stop and restart the appropriate servers to propagate the changes. For specific instructions, go to Starting and stopping servers, deployment managers, and node agents.
6. Complete the following steps to flag an attribute as either unsupported or required for the entire WebSphere Portal environment instead of just for the specified LDAP:
   1. Enter a value for the following required parameters in the `wkplc.properties` file:
      - **user.attributes.required**
      - **user.attributes.nonsupported**

      Go to the properties file for specific information about the parameters.
   2. Save your changes to the `wkplc.properties` file.
   3. Run the following task:

      ```
      ConfigEngine.sh wp-update-attribute-config -DWasPassword=password
      ```
   4. Stop and restart all necessary servers to propagate your changes.

13. On the Config Wizard, click **Finish**.

14. Verify that you can login to your dmgr with the *WASAdminInLDAP* and *WASPswdInLDAP* https://mydmgr.hcl.com:9043/ibm/console

15. Verify that you can log into the primary the *WASAdminInLDAP* and *WASPswdInLDAP* http://myprimaryportal.hcl.com:10039/wps/portal

At this point, you have successfully built a single node cluster using a remote database and a federated LDAP server.

Chapter 6 – Installing HCL® Digital Experience v9.5 on an additional horizontal Node

Chapter Overview

This chapter will demonstrate how to install HCL® Digital Experience v9.5 on an additional horizontal node. In this guide, the installation was completed with a graphical user interface (GUI) using the root user with installation images on a local hard drive.

This chapter contains multiple sections each performing a specific action within the IBM® Installation Manager (IIM) tool. Ensure you complete each section as outlined before proceeding to the section.

Section 1 – Installing IBM® Installation Manager
Section 2 – Installing HCL® Portal (WebSphere Portal) v8.5 Binaries only
Section 3 – Upgrading HCL® Portal (WebSphere Portal) v8.5 to Cumulative Fix (CF) 17 or a later CF
Section 4 – Upgrading HCL® Portal (WebSphere Portal) v8.5 CF17 or a later CF to HCL® Portal v9.5

Before installing HCL® Portal v9.5, ensure you review the planning documentation:

https://help.hcltechsw.com/digital-experience/9.5/config/cw_add_node.html?

NOTE: Many of the steps in this chapter will repeat steps executed in Chapter 1 - Installing HCL® Portal v8.5 on the Primary Node. There are critical steps which are applicable only to the additional horizontal node. Hence a separate chapter was created for this guide.

Section 1 - Installing IBM® Installation Manager

1. Open a terminal window on your additional horizontal Portal node and run:

   ping *mysecondaryportal.ibm.com*

   where *mysecondaryportal.ibm.com* is your fully qualified hostname.

2. In the same terminal window,run:

   ping localhost

   to verify that the localhost settings are properly configured on your server.

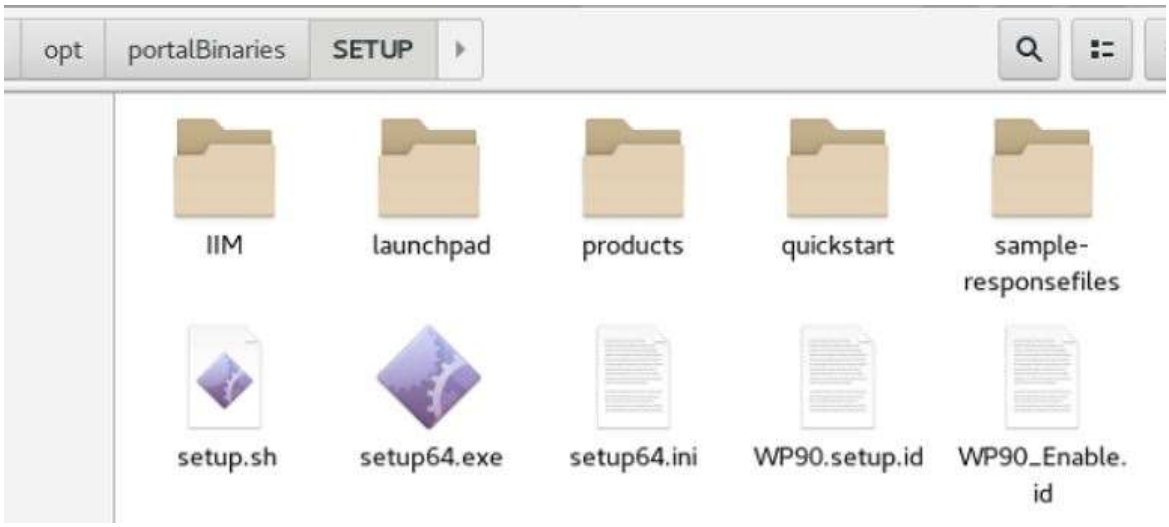
3. **Linux/UNIX environments only:** Ensure ulimit is set to 10240 or higher by

   running: ulimit -n 10240

   in the command line.

4. Unzip all .zip files provided with your Portal media into a single folder. This folder will be referred to as the *installationMediaRoot* folder.

   For this guide the following directory is used for the *installationMediaRoot* folder: /opt/portalBinaries/SETUP/products



5. From the HCL® Portal v95 SETUP directory, navigate to:

   SETUP/IIM/*yourEnvironment*

   and run

   ./install

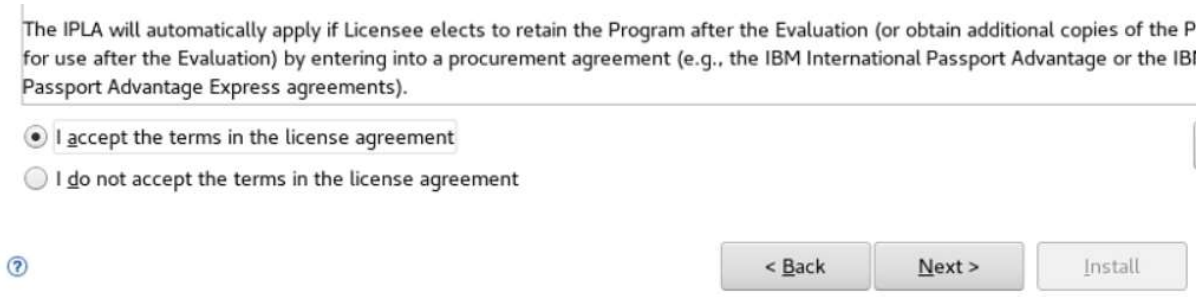
   where *yourEnvironment* is the folder that best describes the operating system of the environment in which you are installing HCL® Portal. For this guide the following is used:

   installationMediaRoot/SETUP/IIM/linux_x86_64

   The following window will appear:

6. Click **Next**.

7. Accept the license agreement and click **Next**.



8. Choose a directory in which to install IIM. This guide uses:

   /opt/IBM/InstallationManager/eclipse

   for Windows this guide recommends:

   c:\IBM\InstallationManager\eclipse

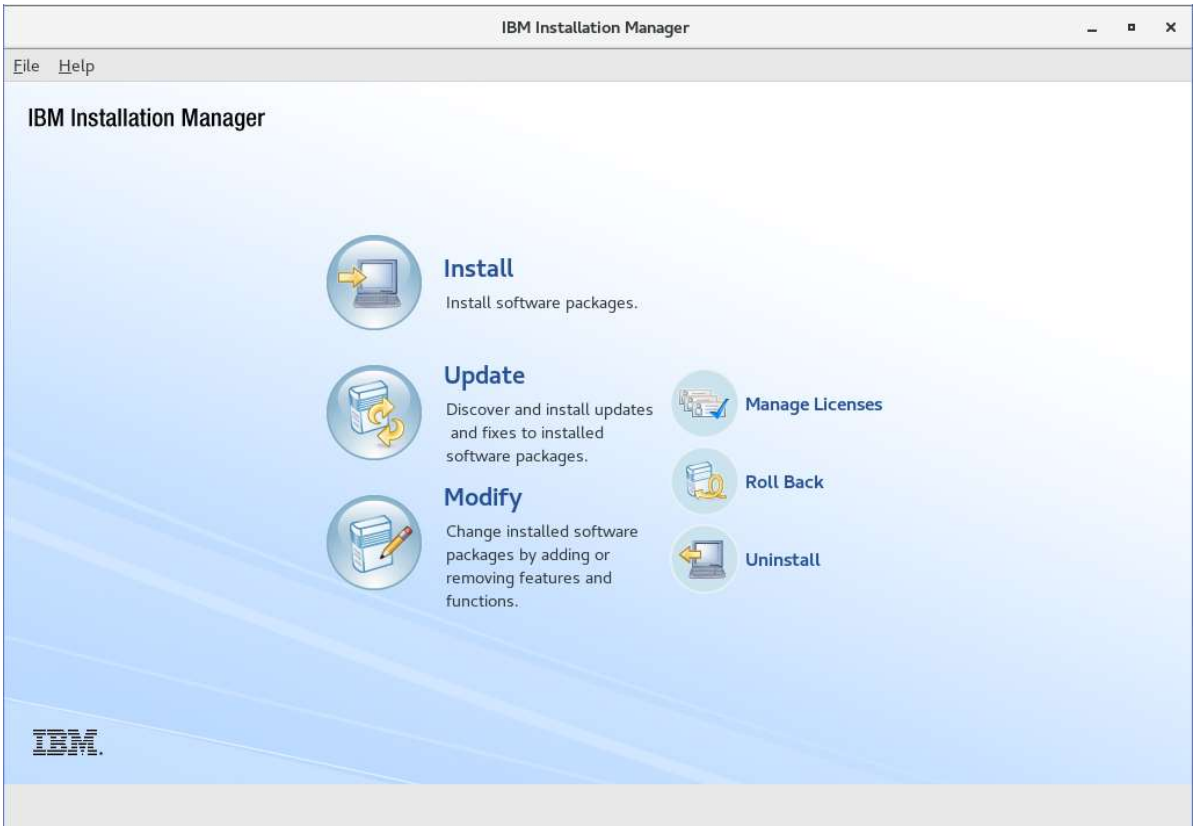
   NOTE: In Windows environments, the default location will likely be C:\Program Files\IBM\InstallationManager. Spaces in the file path can cause problems later in the installation/Configuration of Portal. It is good practice to create a folder called “IBM” at C:\IBM or a similar location into which IIM and HCL® Portal can be installed.

9. Click Next.

10. On the Summary screen, click **Install** to begin the installation.

11. When the installation is complete, click **Restart Installation Manager**.

12. The following screen will appear:



7

At the end of this section, you have successfully installed IBM® Installation Manager1.8.5.

Section 2 - Installing HCL® Portal (WebSphere Portal) v8.5 Binaries only

This section will cover the installation of HCL® Portal v8.5. HCL® Portal v8.5 must be installed and thereafter upgraded to HCL® Portal v9.5. It is not possible to install HCL Portal® v9.5 directly.

1. In IIM, click **File > Preferences > Repositories**

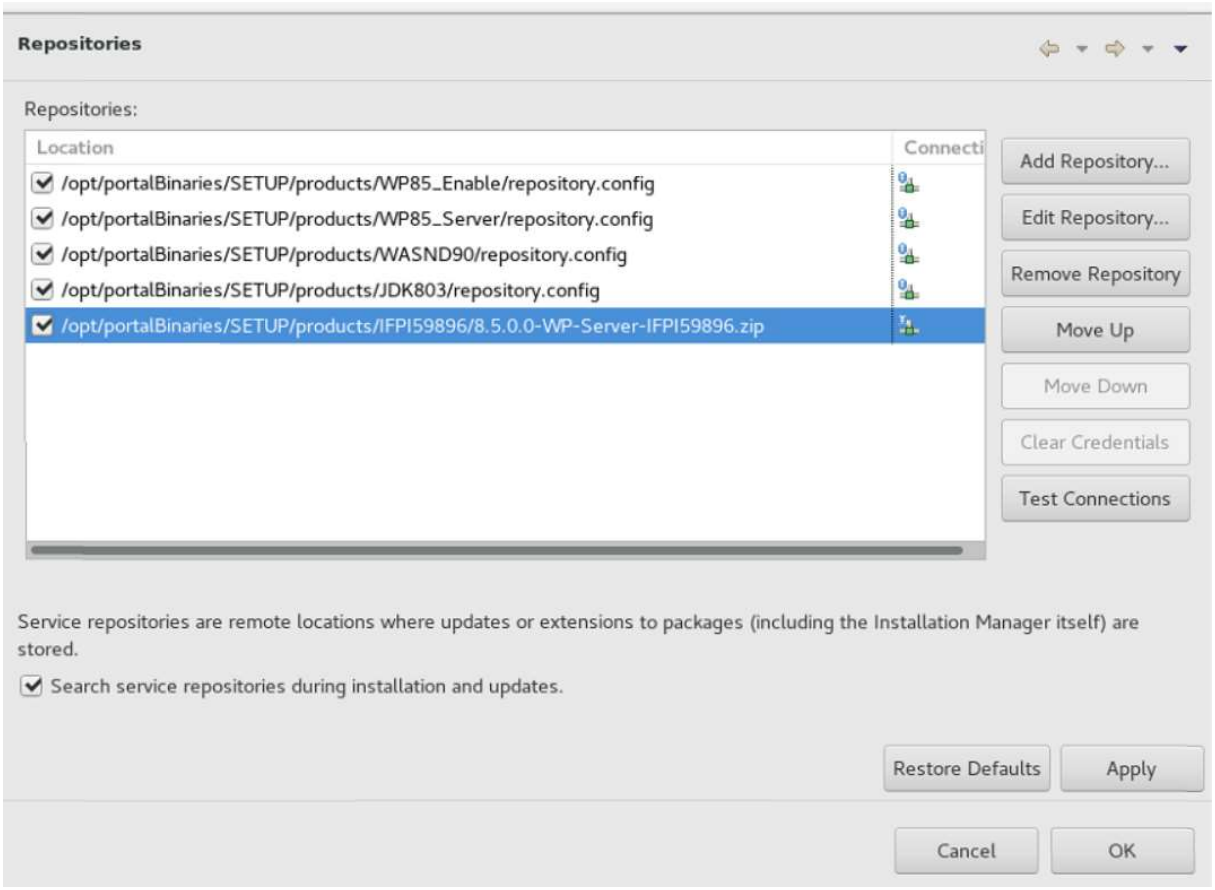
2. Click **Add Repository**, navigate to

   installationMediaRoot/WP85_Enable/repository.config

   and click **OK**.

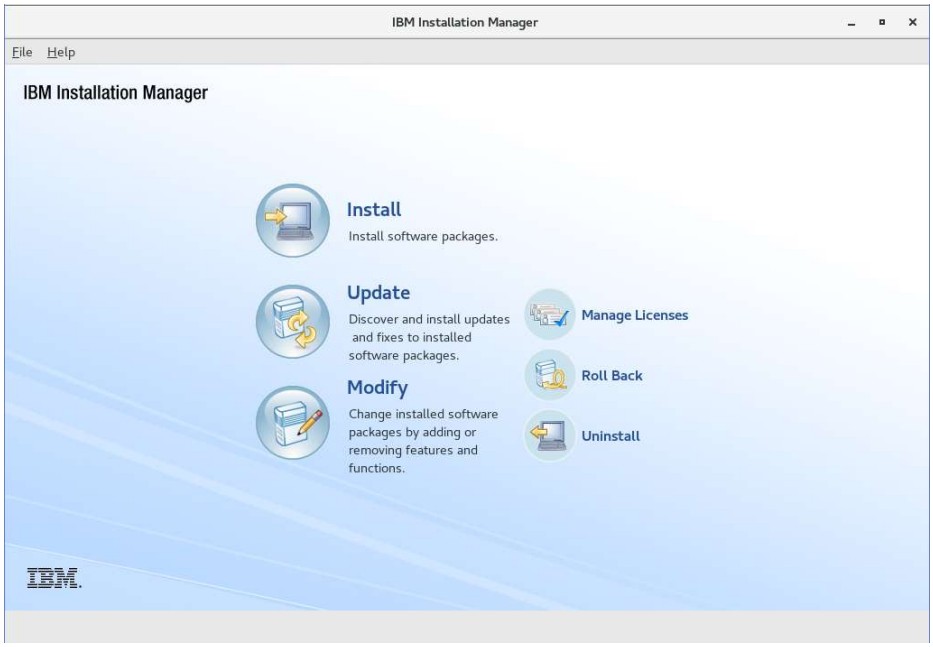
3. Repeat step 2 for the following repositories:

   installationMediaRoot/WP85_Server/repository.config
   installationMediaRoot/WASND90/repository.config
   installationMediaRoot/JDK803/repository.config
   installationMediaRoot/IFPI59896/8.5.0.0-WP-Server-PI59896.zip

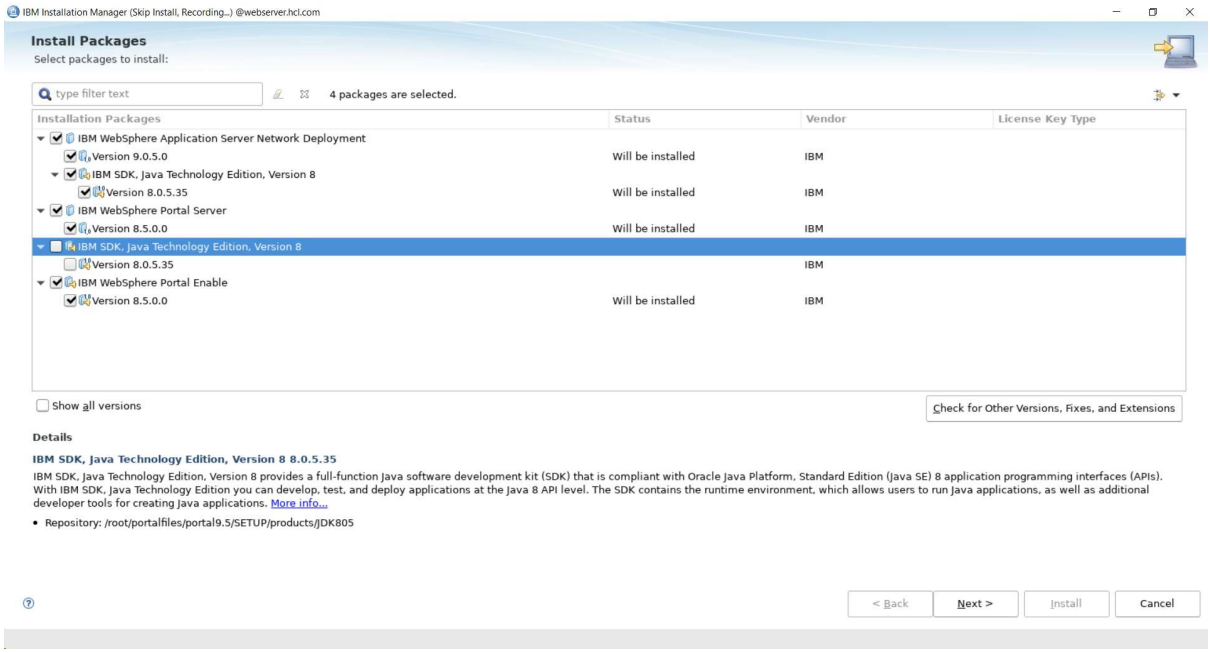


4. Ensure that all the repositories you just added are selected (i.e. there is a check mark in the box next to them) and click **Apply** then **OK**.

5. Back on the IIM Home Screen, click **Install**.

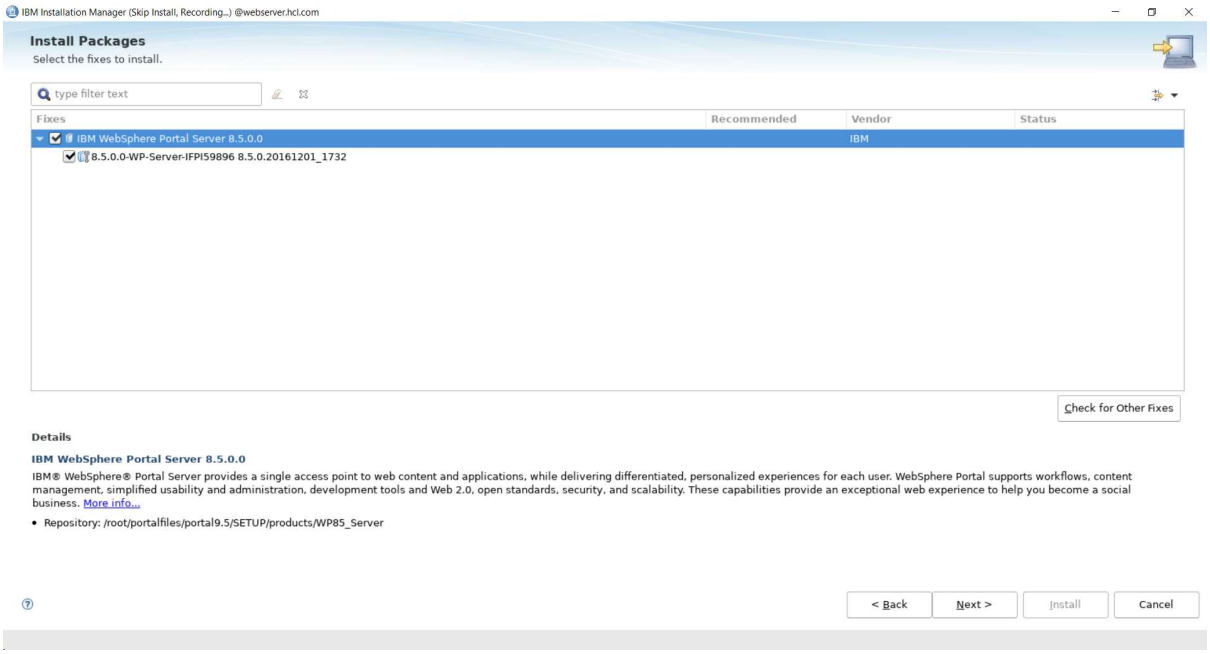


6. Check the boxes to install IBM WebSphere Application Server Network Deployment, IBM WebSphere Portal Server, and IBM WebSphere Portal Enable (or the offering you are installing, e.g. Extend, Express, etc.). IBM SDK, Java Technology Edition, Version 8 package should not be elected as it is will be automatically installed with the IBM WebSphere Application Server Network Deployment package.

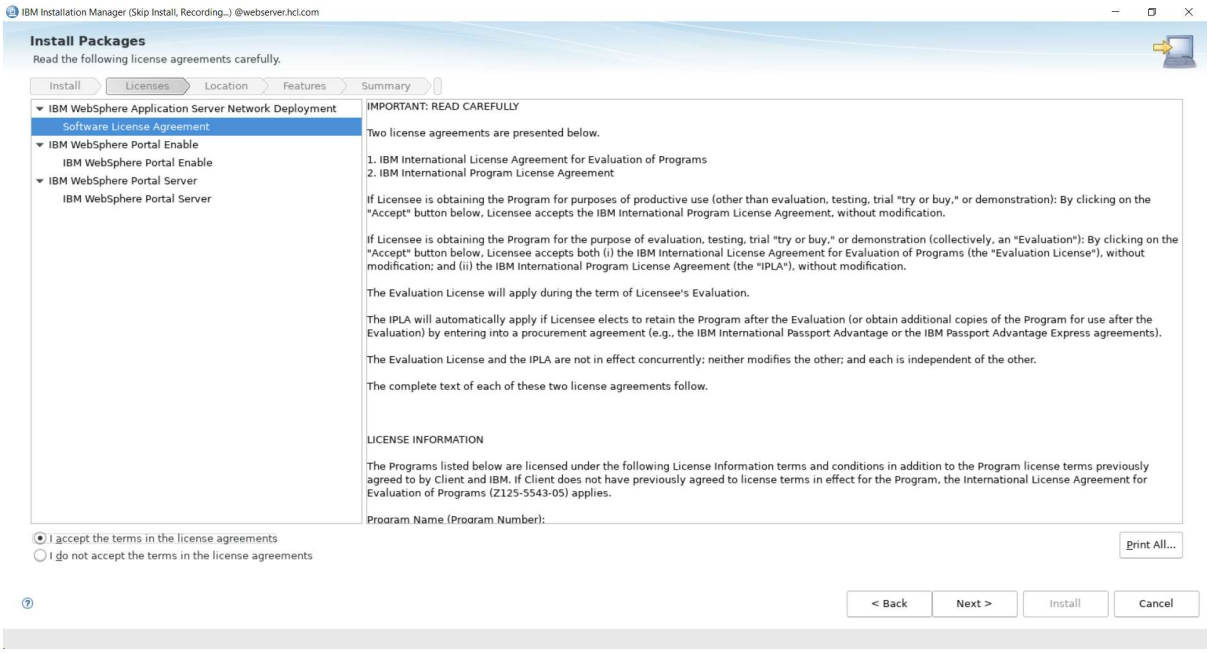


7. Click **Next**.

8. **Select** the iFix IFPI59896 and click **Next**

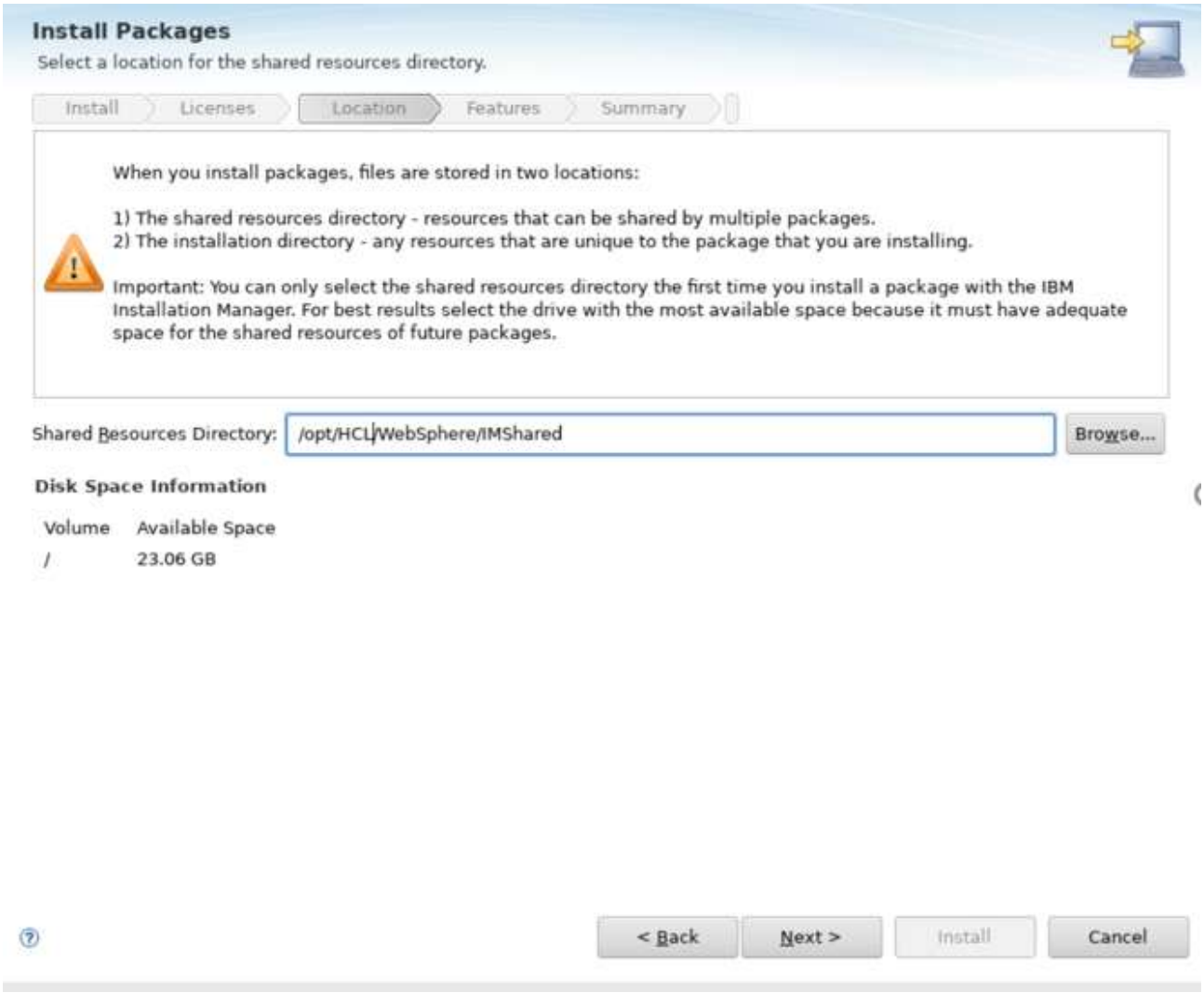


9. **Accept** license agreement and click **Next**



10. Select a location for the IIM Shared Resources Directory. This guide uses: /opt/HCL/WebSphere/IMShared

    for Windows this guide recommends: c:\HCL\WebSphere\IMShared


Install Packages
Select a location for the shared resources directory.
Install
Licenses
Location
Features
Summary
When you install packages, files are stored in two locations:
1) The shared resources directory - resources that can be shared by multiple packages.
2) The installation directory - any resources that are unique to the package that you are installing.
Important: You can only select the shared resources directory the first time you install a package with the IBM Installation Manager. For best results select the drive with the most available space because it must have adequate space for the shared resources of future packages.
Shared Resources Directory:
/opt/HCL/WebSphere/IMShared
Browse...
Disk Space Information
Volume
Available Space
/
23.06 GB
< Back
Next >
Install
Cancel

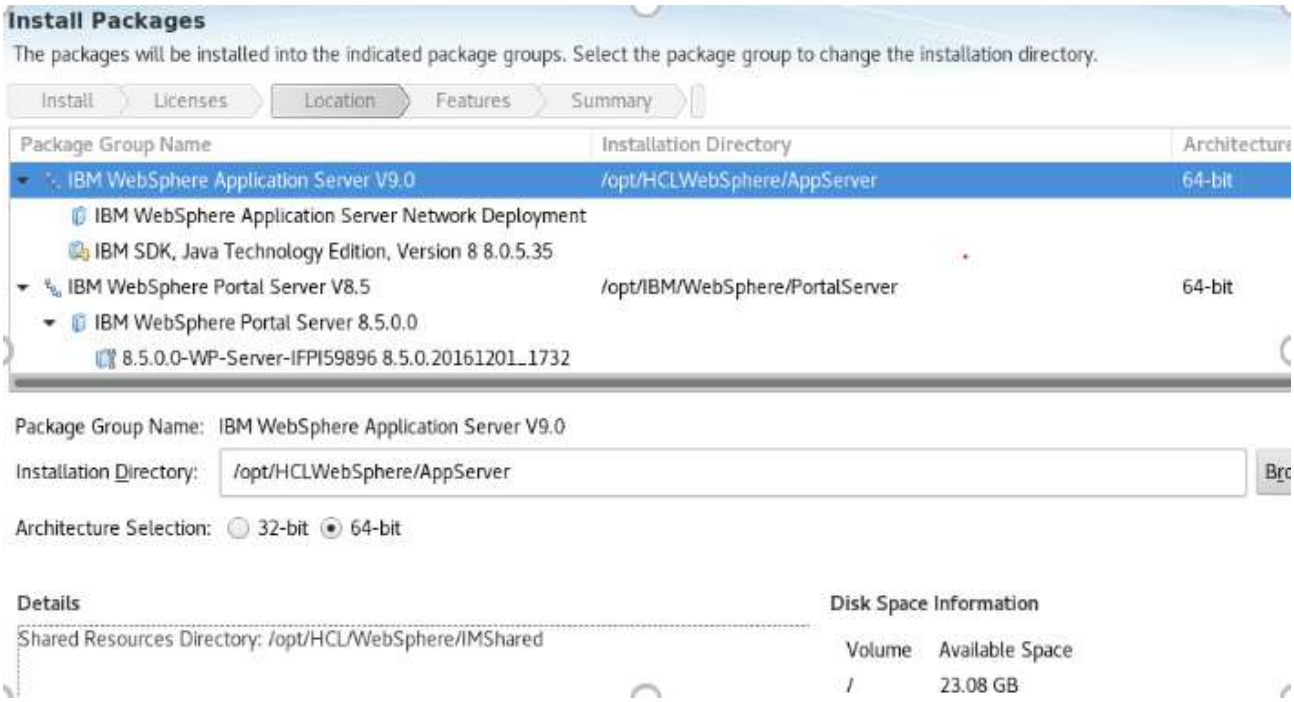
Click **Next.**

11. Click **IBM WebSphere Application Server** to set the WAS installation location. This guide uses:

    /opt/IBM/WebSphere/AppServer

    for Windows this guide recommends:

    C:\IBM\WebSphere\AppServer



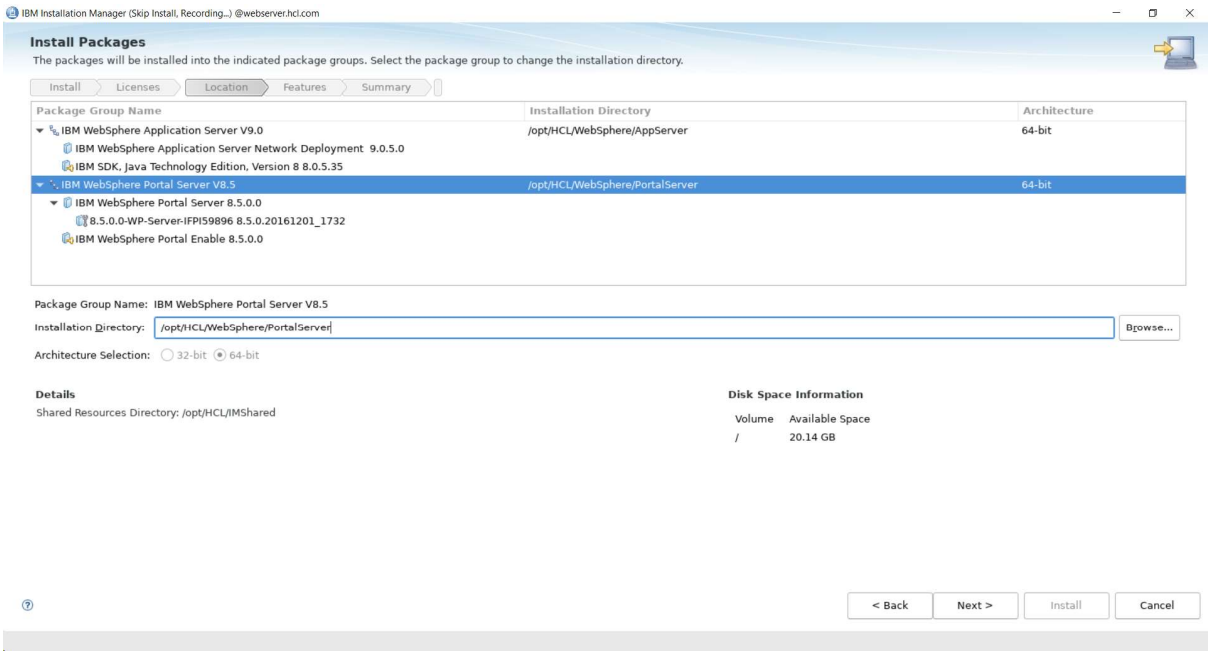
Click **Next.**

12. Click **IBM WebSphere Portal Server V8.5** to set the Portal Server installation directory:

    /opt/HCL/WebSphere/PortalServer

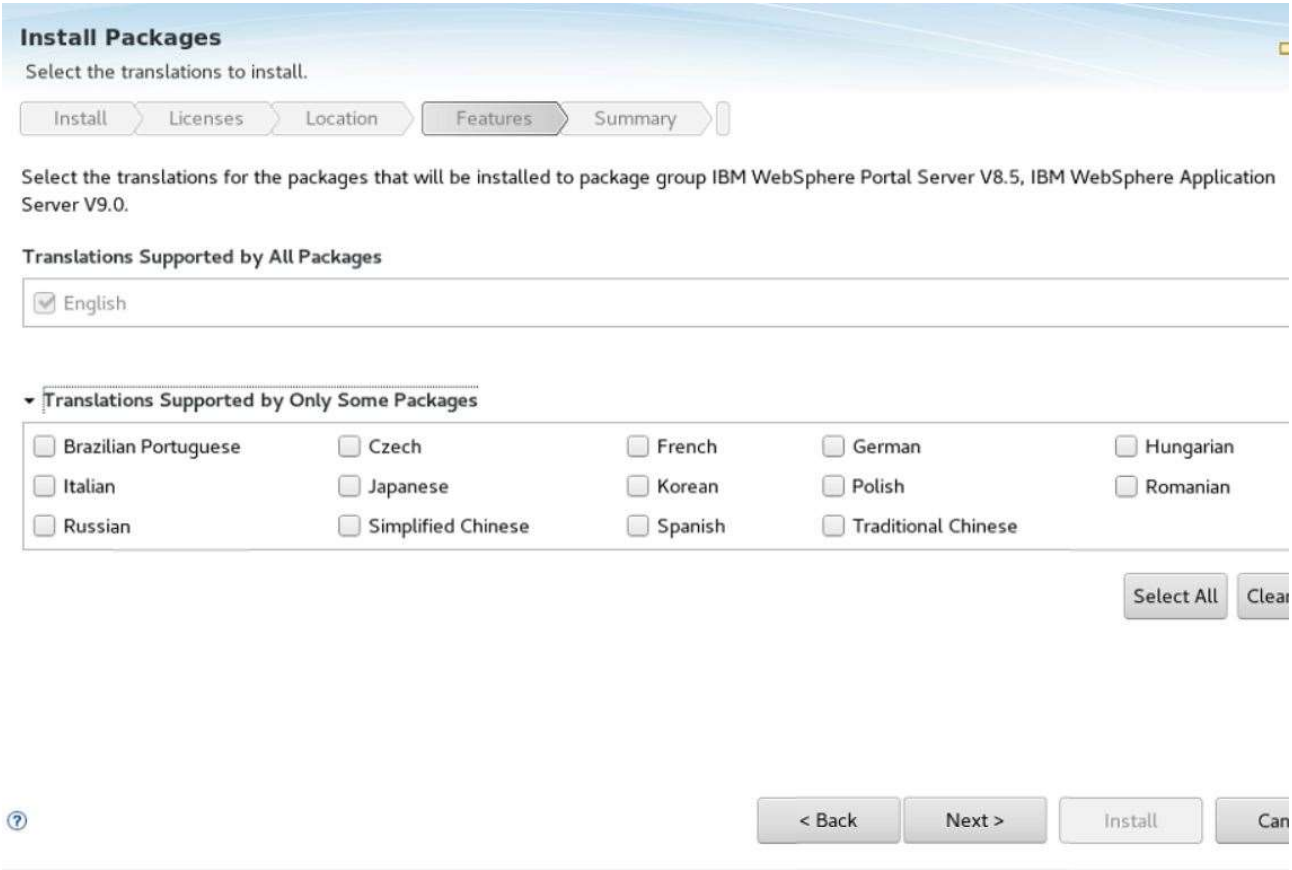
    for Windows this guide recommends:

    C:\HCL\WebSphere\PortalServer



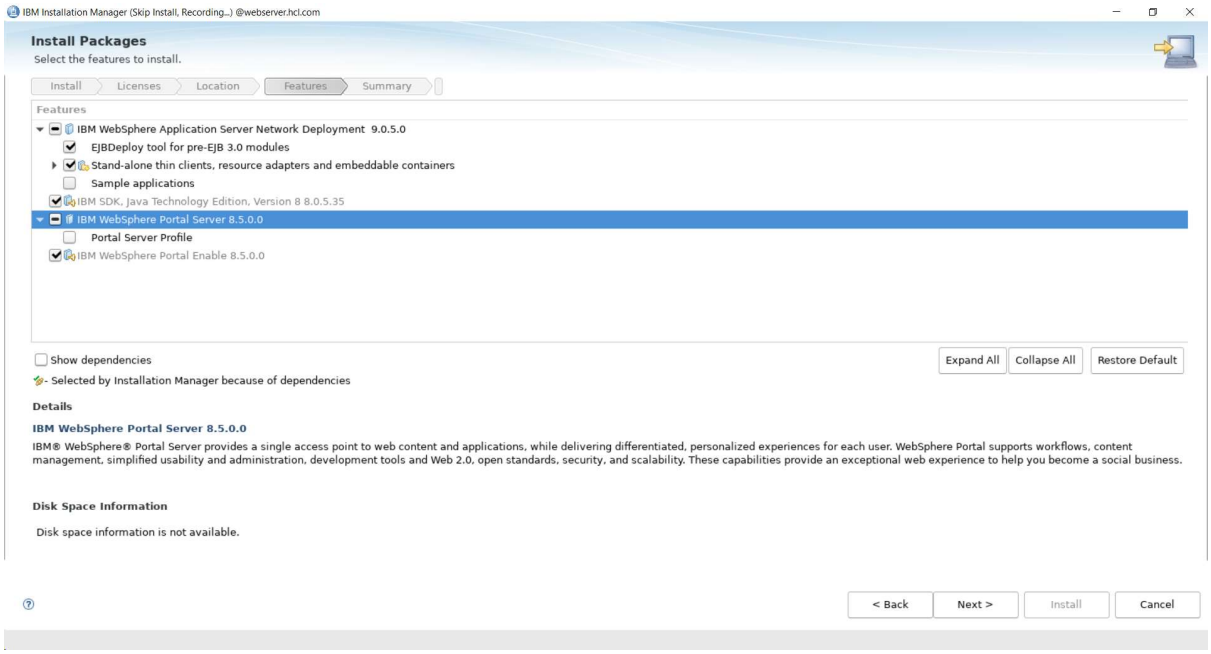
Click **Next**.

13. Select any additional language translations your environment requires.
    Only English was selected for this guide. Click **Next**.



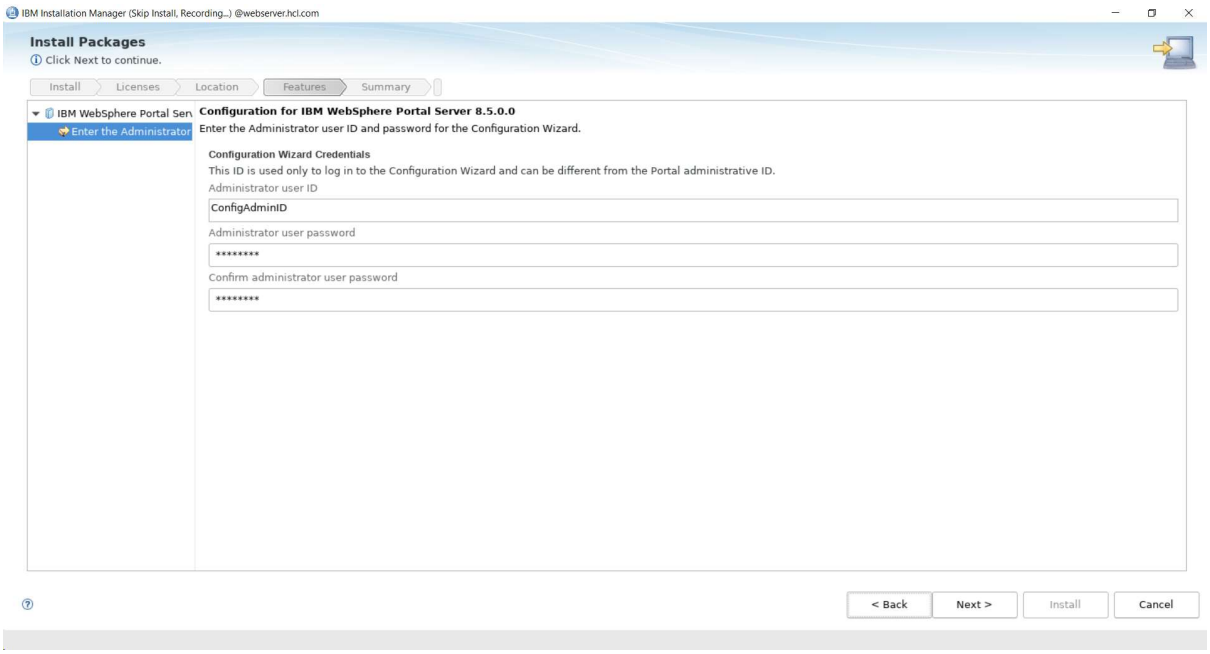
14. Review the features to install for both WebSphere Application Server and WebSphere Portal. **UNCHECK the box for WebSphere Portal profile**.

NOTE: Do not de-select any WebSphere Application Server features. Ensure you do not install a WebSphere Portal profile. You will copy over profile information from the primary Portal server and create a profile for this server in a later step.



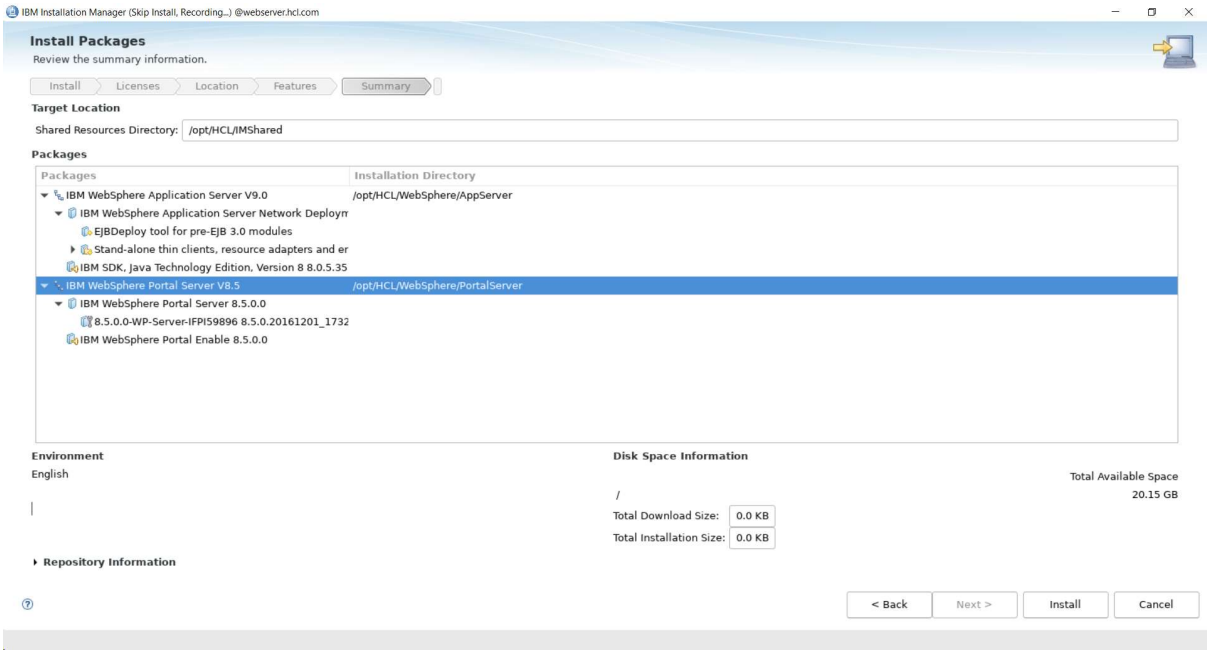
Click **Next**

15. Set the Configuration Wizard (Config Wizard) username and password. You can set these to any values you want to use for the Config Wizard credentials. “ConfigWizardID” is used for this guide.



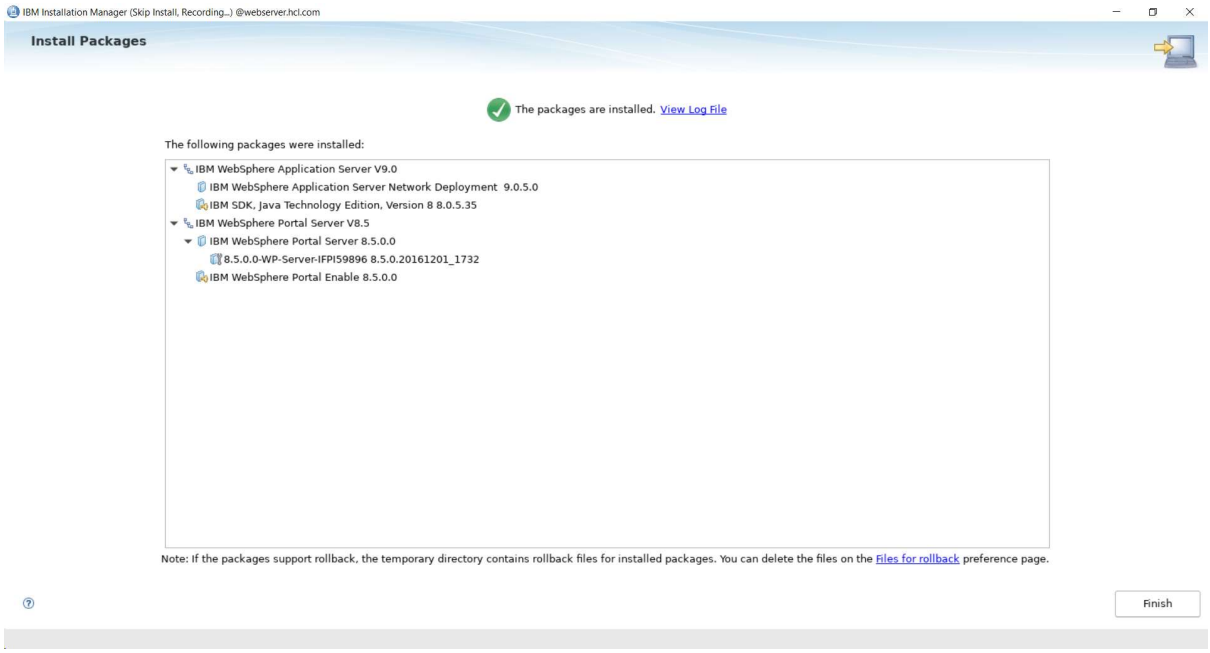
Click **Next.**

16. Review your installation selections and click **Install**.



NOTE: The installation will take 30-60 minutes; don't be concerned if the Installation Manager seems to be stuck on one task for several minutes

17. When the installation is finished, select **None** for **Which program do you want to start?** and click **Finish**.



NOTE: There is not yet a profile on this system. Therefore, you cannot access this Portal in a web browser at this time. You can access the Config Wizard on the additional horizontal node. You will use the Config Wizard in the next chapter to create a profile on the additional horizontal node. Complete all sections of this chapter first before proceeding to the next chapter.

At this point, you have successfully installed HCL® Portal (IBM® WebSphere Portal) v8.5 with IBM® WebSphere Application Server v9.0.5.0 binaries on an additional horizontal node.

Section 3 – Upgrading HCL® Portal (WebSphere Portal) v8.5 to Cumulative Fix (CF)

HCL® Portal v8.5 now needs to be upgraded to Cumulative Fix 17 or a later CF to support the installation of HCL® Portal v9.5. You will need to stop the Configuration Wizard to proceed with the upgrade.

1. Navigate to the location you installed WebSphere Application Server. Continue in the directory structure to the /profiles/cw_profile/bin subdirectory. This guide uses the following directory for the full path:

   /opt/IBM/WebSphere/AppServer/cw_profile/bin

2. Execute the following command:
   ./stopServer.sh server1 -user *ConfigWizardID* -password *ConfigWizardPswd*

3. You will be prompted for a userID and password.
   Enter your *ConfigWizardID* for the userID and *ConfigWizardPswd* for the password.

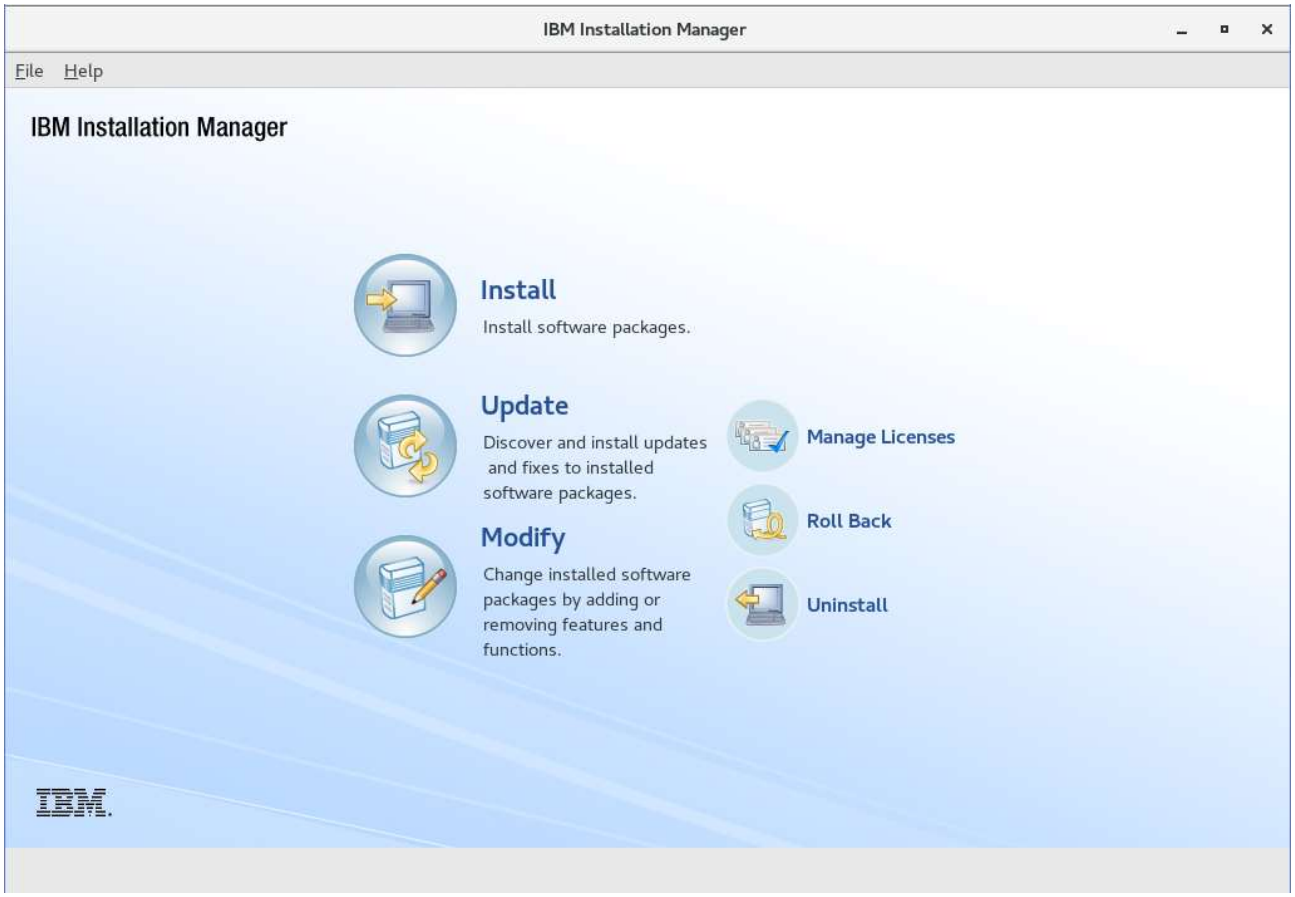
```
[root@      /]# cd /opt/IBM/WebSphere/AppServer/profiles/cw_profile/bin/
[root@      bin]# ./stopServer.sh server1
ADMU0116I: Tool information is being logged in file
           /opt/IBM/WebSphere/AppServer/profiles/cw_profile/logs/server1/stopSer
ver.log
ADMU0128I: Starting tool with the cw_profile profile
ADMU3100I: Reading configuration for server: server1
```

4. Return to IBM® Installation Manager. Click **File > Preferences > Repositories.**
5. Select each of the existing Repositories and Click **Remove Repository.**

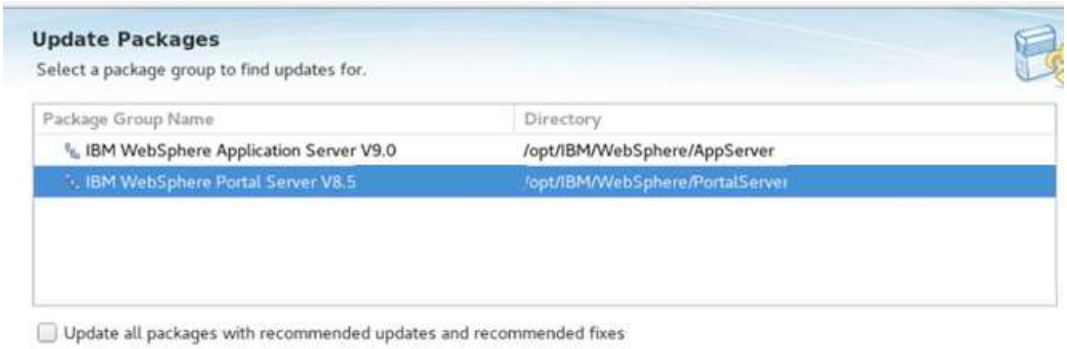
6. Click **Add Repository**, navigate to:
installationMediaRoot/SETUP/products/WP8500CF17_Server/repository.config

Click **OK** twice.

7. In IBM® Installation Manager, click the Update icon:



8. Select the IBM WebSphere Portal Server 8.5 package.



9. Click **Next** to proceed with the Version 8.5.0.0 CF17 package.

10. Click **Next** to proceed beyond the Validation Results.

NOTE: HCL highly recommends that you backup of your entire Portal architecture when installing a cumulative fix on an established Portal system. Backups will be covered in more detail in Appendix As the system in this guide represents a brand new system, a backup is not required at this time.

11. Click the radio icon for "I accept the terms in the license agreement". Click **Next.**

12. Click **Next** to Accept the terms of the licensing agreement.

13. Click **Next** to Install the IBM WebSphere Portal CF17 feature.

14. Click **Update.** This step will take approximately 20-30 minutes to execute.

15. Click **Finish.**

NOTE: The applyCF.sh command to update the <wp_profile> cannot be run at this time as a profile does not exist on the additional horizontal node at this time. The next chapter will guide you through creating a profile on the additional horizontal node.

At the end of this section, you have successfully installed Cumulative Fix 17 for HCL® Portal 8.5 on IBM® WebSphere Application Server v9.0.0.2.

Section 4 – Upgrading HCL® Portal (WebSphere Portal) v8.5 CF17 to HCL® Portal v9.5

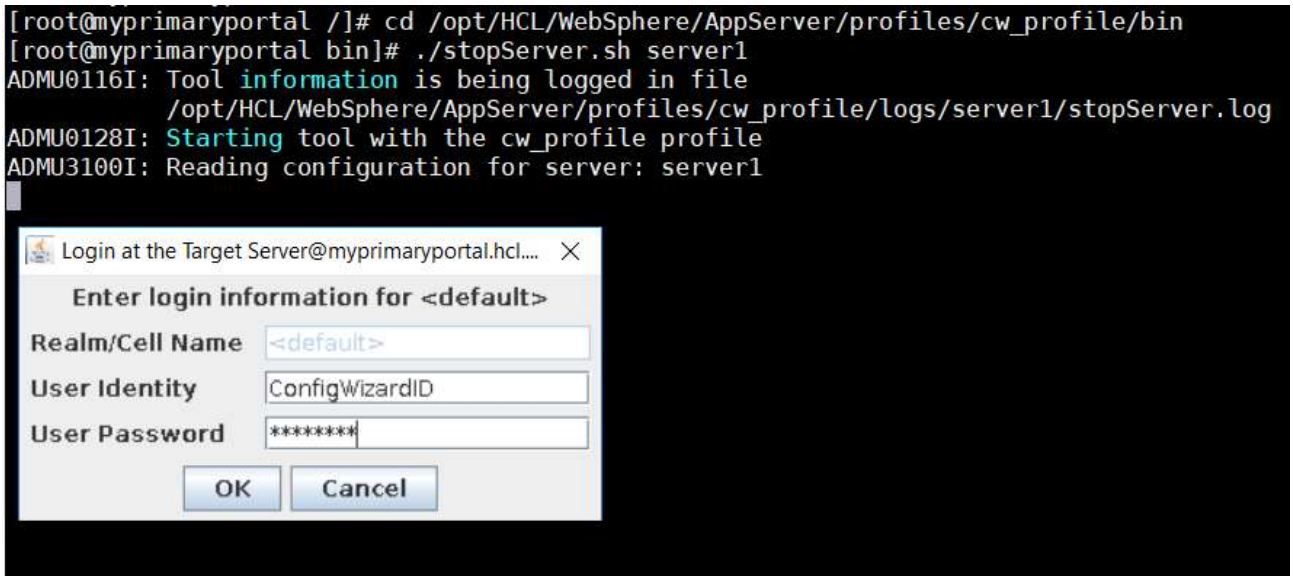
In this final section HCL® Portal v8.5 CF17 will be upgraded to HCL® Portal v9.5. You will need to stop the Configuration Wizard to proceed with the upgrade.

1. Navigate to the location you installed IBM® WebSphere Application Server. Continue in the directory structure to the /profiles/cw_profile/bin subdirectory. This guide uses the following directory for the full path:

   /opt/HCL/WebSphere/AppServer/cw_profile/bin

2. Execute the following command:
   ./stopServer.sh server1

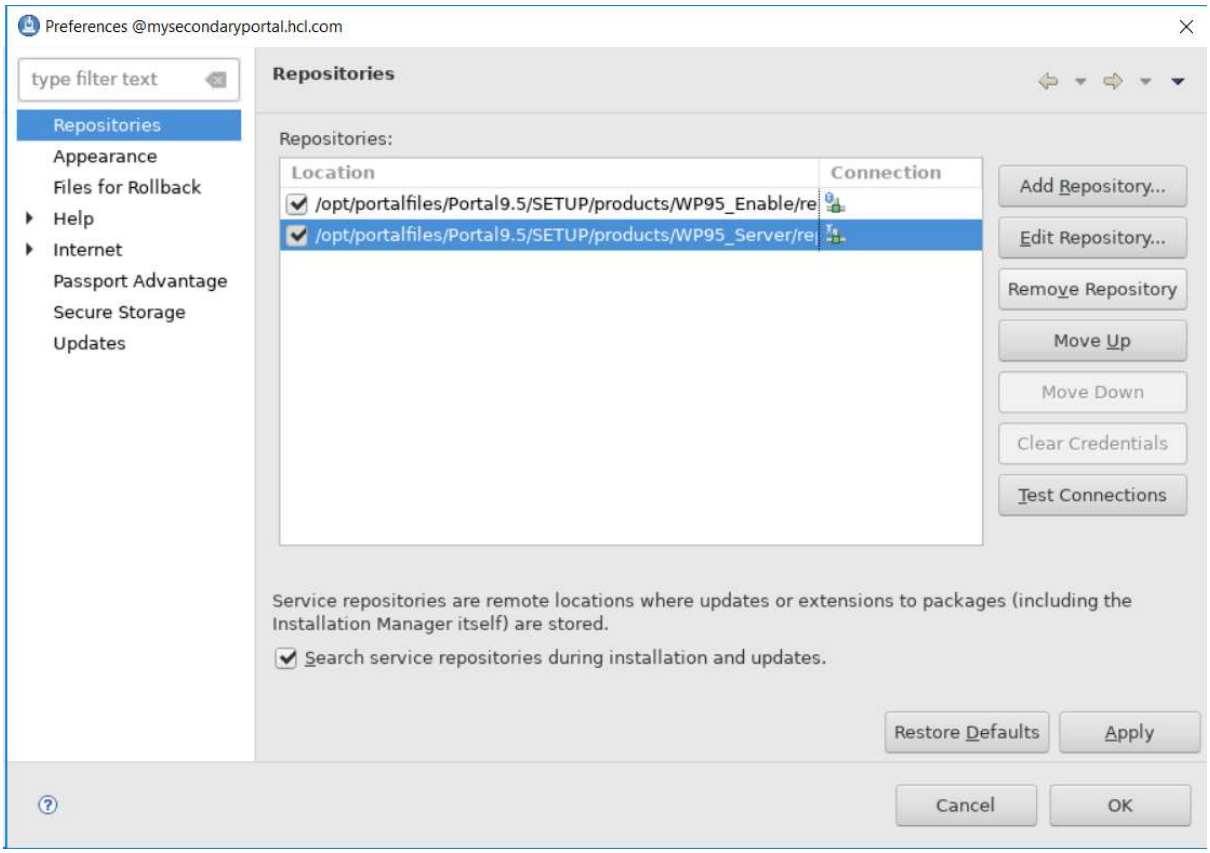
3. You will be prompted for a userID and password. Enter your *ConfigWizardID* for the userID and *ConfigWizardPswd* for the password.



4. Return to IBM® Installation Manager. Click **File > Preferences > Repositories.**
5. Select each of the existing Repositories and Click **Remove Repository.**
6. Click **Add Repository**, navigate to:
   installationMediaRoot/SETUP/products/WP95_Portal/repository.config

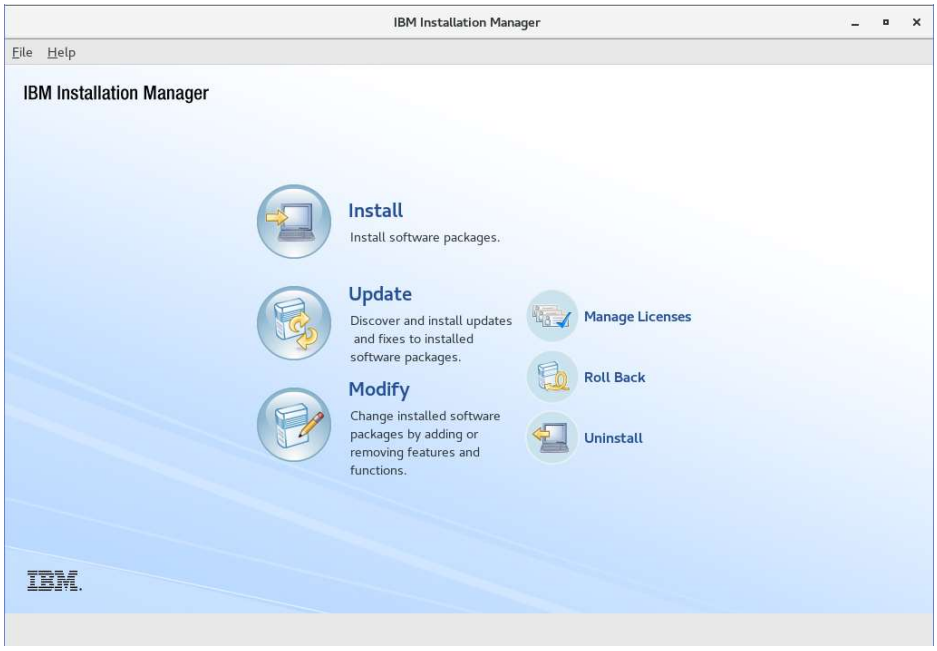
   Click **OK.**

7. Click **Add Repository**, navigate to:
   installationMediaRoot/SETUP/products/WP95_Enable/repository.config

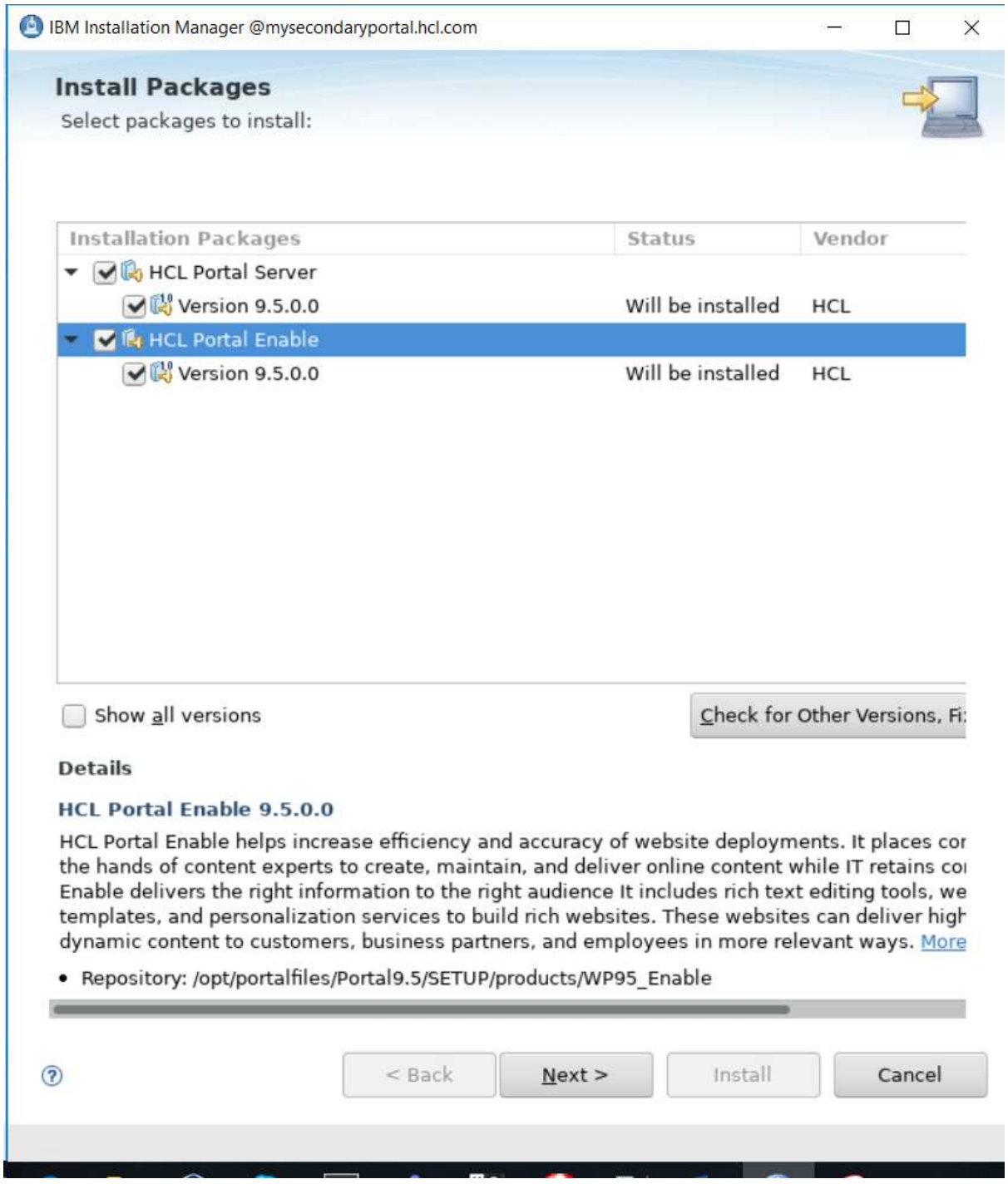


Click **OK** twice.

8. In IBM® Installation Manager, click the Install icon:

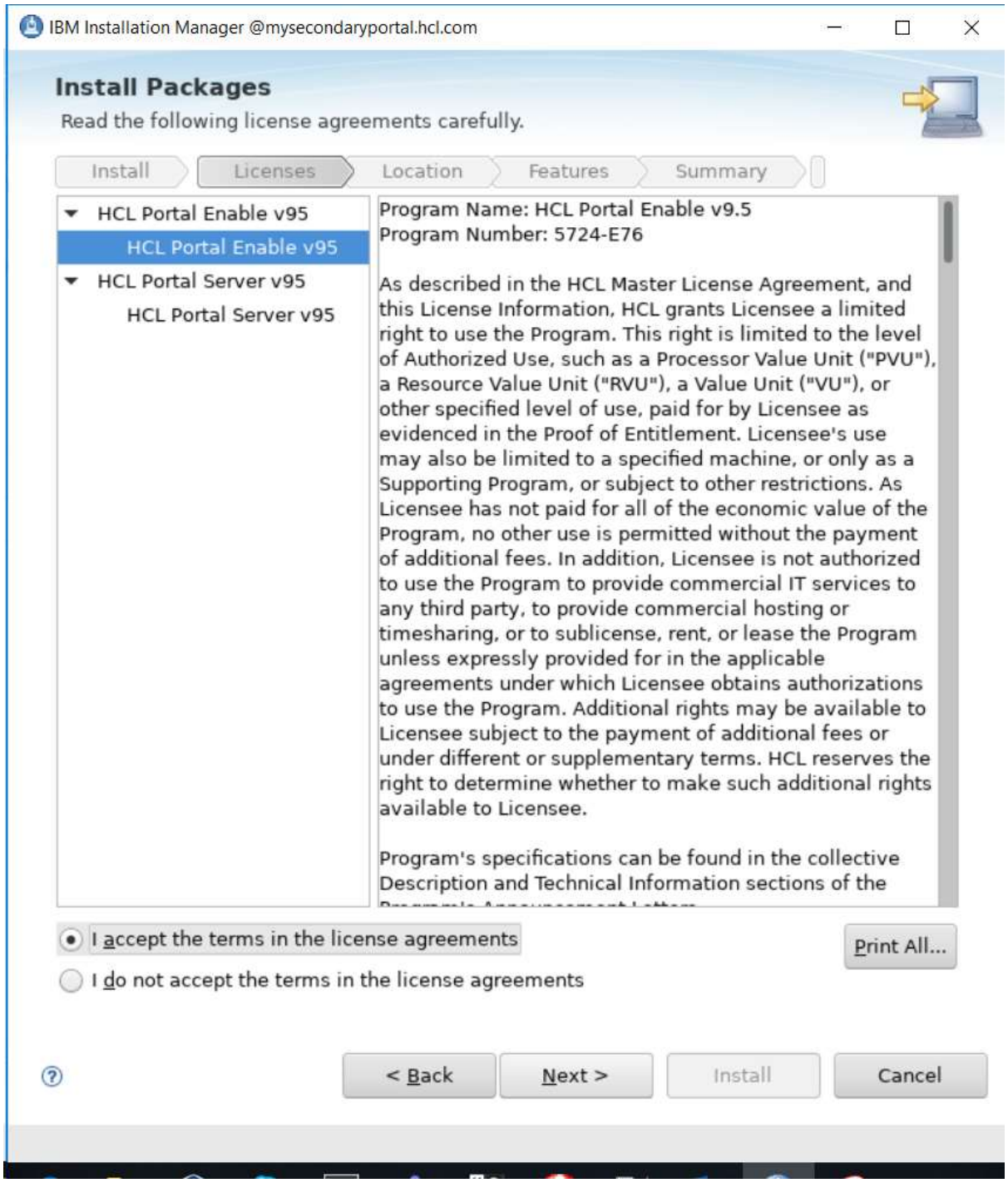


9. Check the boxes to install the HCL Portal Server and HCL Portal Enable (or the offering you are installing, e.g. Extend, Express, etc.) packages.

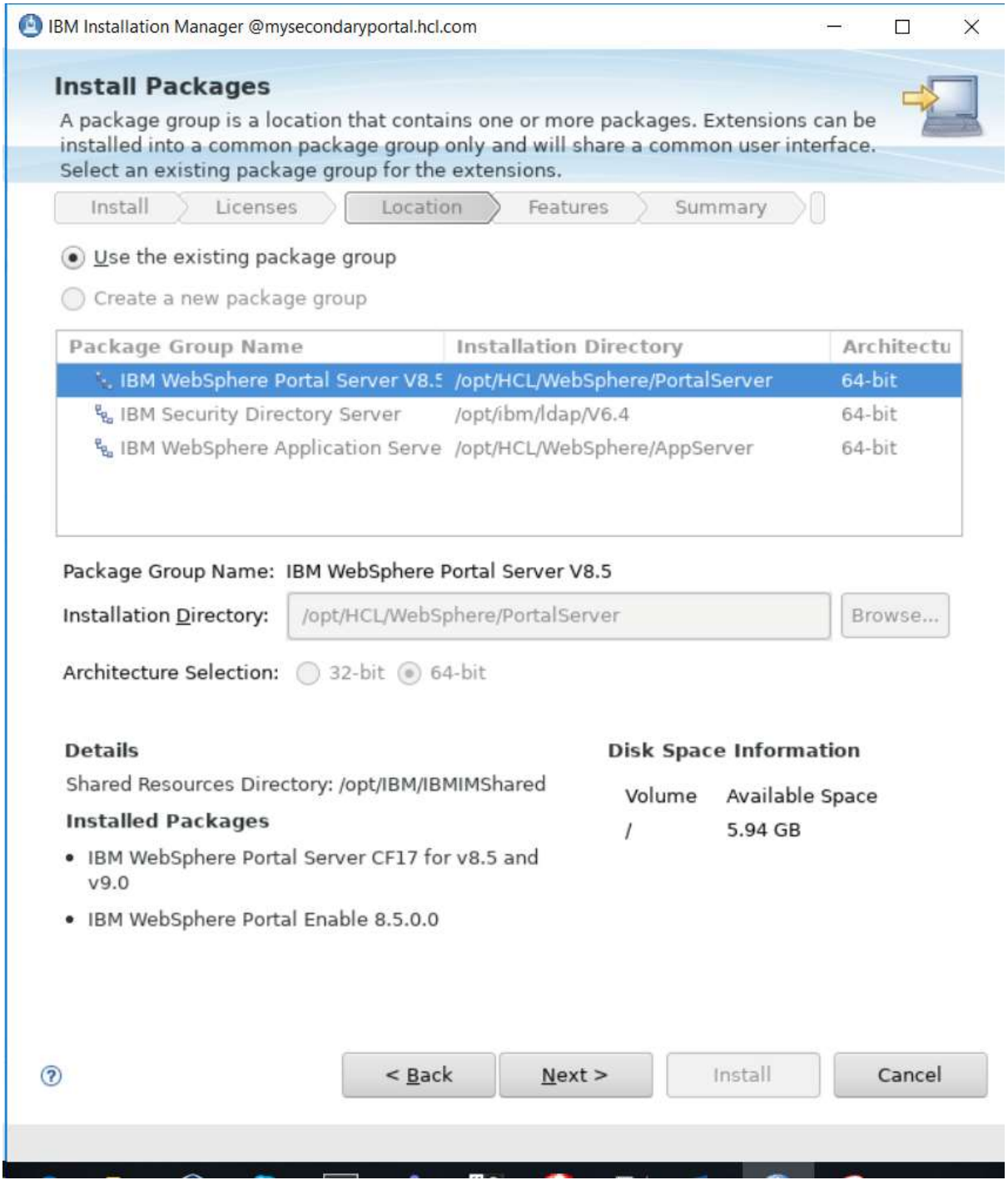


Click **Next**

10. Accept terms of licensing agreement. Click **Next.**

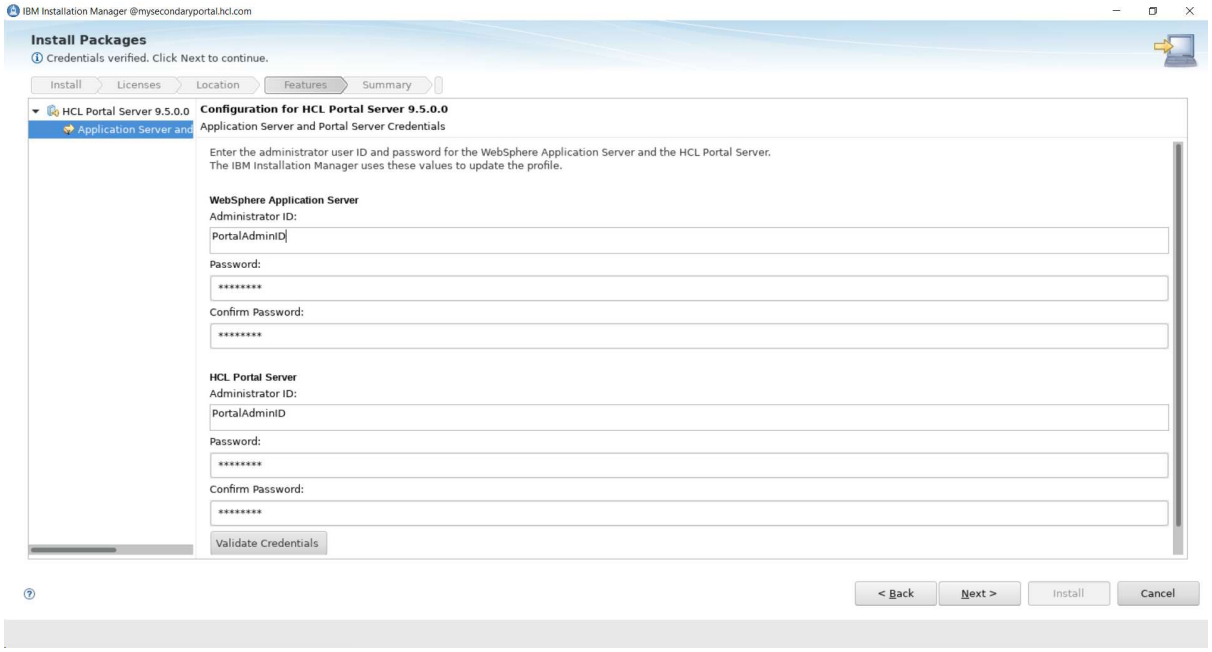


11. Select the option **Use the existing package group** and click on **IBM WebSphere Portal v8.5.**

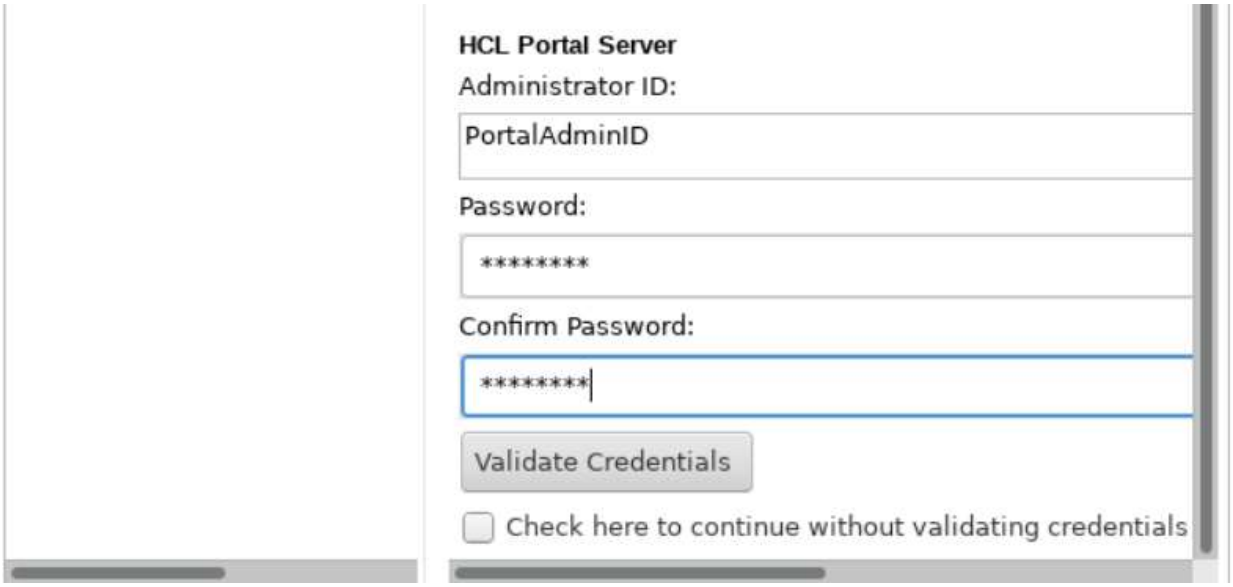


Click **Next**

12. Enter your *PortalAdminID* and *PortalAdminPswd* for the Websphere Application Server credentials. Scroll down. Enter your *PortalAdminID* and *PortalAdminPswd* for the Portal Server credentials.

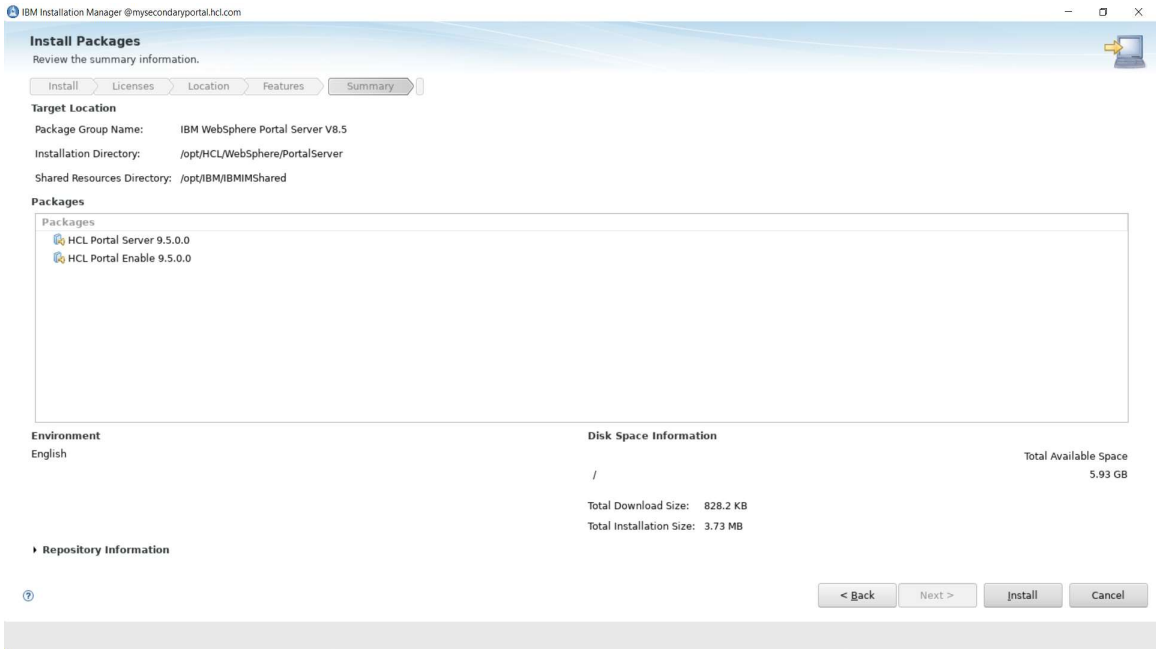


13. Click **Validate Credentials**

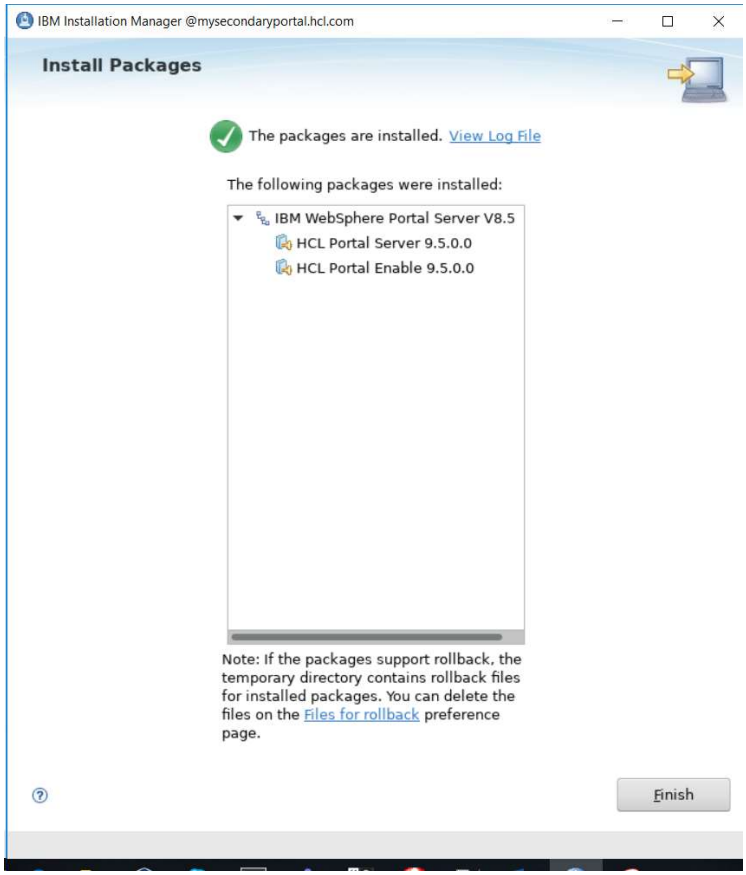


Wait a few minutes for validation to complete. Click **Next**.

14. Review Summary. Select **Install.**



When the installation is finished, you should see:



Verify that you can access your Portal in an internet browser by navigating to:
http://mysecondaryserver.hcl.com:10039/wps/portal

Chapter 7 – Federating and Clustering an Additional Horizontal Node

This section covers adding the additional node to the Deployment Manager cell and adding a new HCL® Portal server as a horizontal cluster member to the previously created cluster. Once this section is completed, you will have a functional two-node horizontal cluster using federated LDAP security.

IMPORTANT: If you have applied a Cumulative Fix (CF) to the primary Portal node, you need to apply the same CF to the additional horizontal Portal node before adding it to the cluster. All Portal binaries and profiles must be on the same CF level before being added to a cluster.

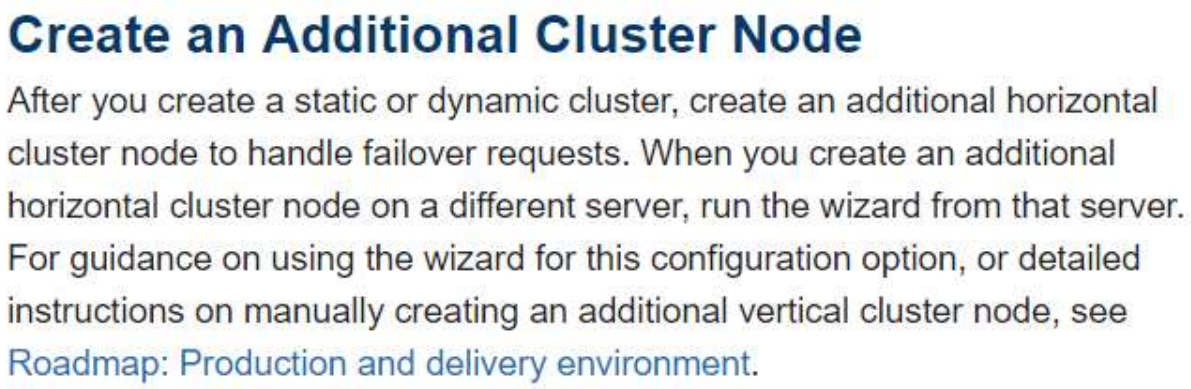
This guide installed Cumulative Fix 17 to the primary node in Chapter 1, and Cumulative Fix 17 to the additional horizontal node in Chapter 6. Thus, the additional horizontal node may be safely added to the existing Portal cluster.

1. Open the Config Wizard for the additional horizontal node in a web browser:

   http://mysecondaryportal.hcl.com:10200/hcl/wizard

   Sign in with your *ConfigWizardID* and *ConfigWizardPswd* Config Wizard credentials.

2. On the Config Wizard home screen, click **Set Up a Cluster>Create an Additional Cluster Node.**



3. Select your target operating system, Portal profile name, and Portal profile home directory. **NOTE:** A Portal profile does not exist yet on the additional horizontal node. Fill in the values that would correspond to the profile if it did exist.

Click the right arrow.

4. Select the location of the Deployment Manager for your environment and the type of cluster you created.

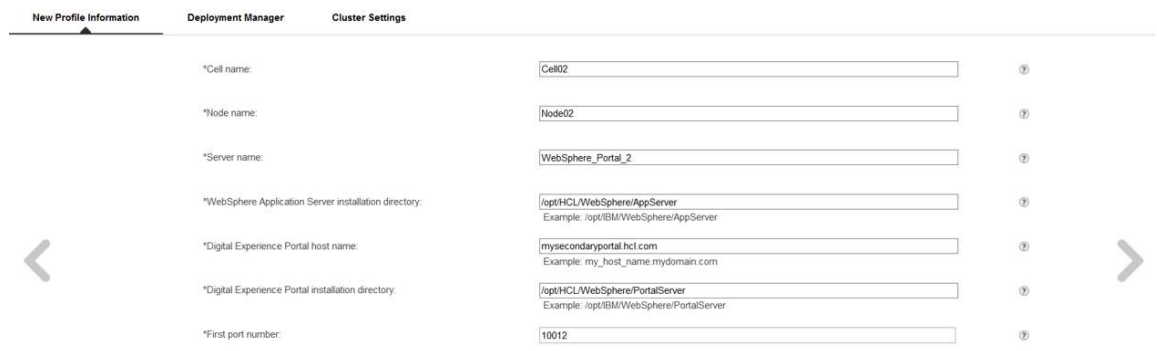
Click the right arrow.

5. Specify the following:

- Cell name: a new cell name for the new profile. **Cell02** for this guide.
- Node name: a new node name for the new profile. **Node02** for this guide.

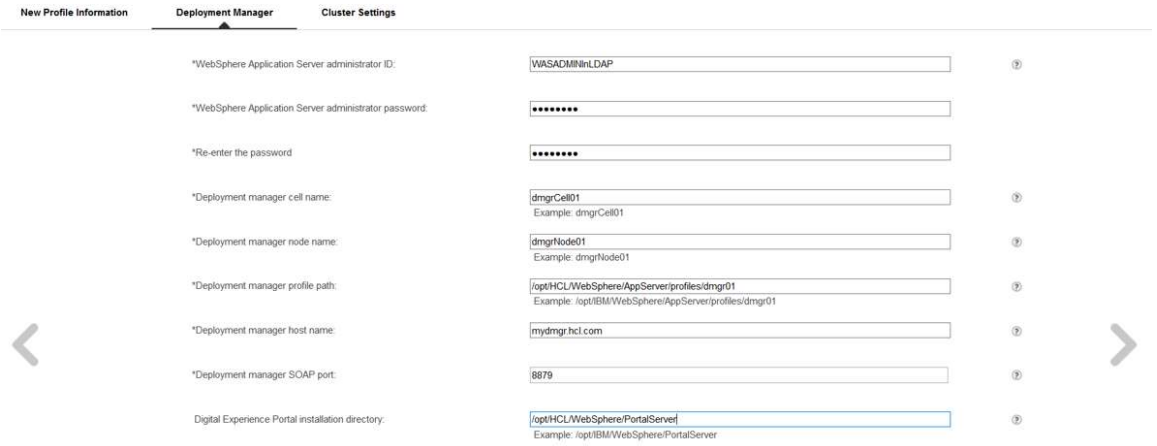
  NOTE: Choose a node name and cell name different from the Deployment Manager node name and cell name.

- WAS installation directory: **/opt/HCL/WebSphere/AppServer**, set to default
- Portal host name: **mysecondaryportal.ibm.com**
- Portal installation directory: **/opt/HCL/WebSphere/PortalServer**, set to default
- First port number: This value will be pre-populated to **10012** but can be set to any available port number. If set to the default you will access your additional horizontal portal server in a web browser via port 10039 at the end of this chapter.



Click the right arrow.

6. Specify your WAS administrator ID from your LDAP, WAS administrator password from your LDAP, dmgr cell name, dmgr node name, dmgr profile path, dmgr host name, and Portal installation directory.

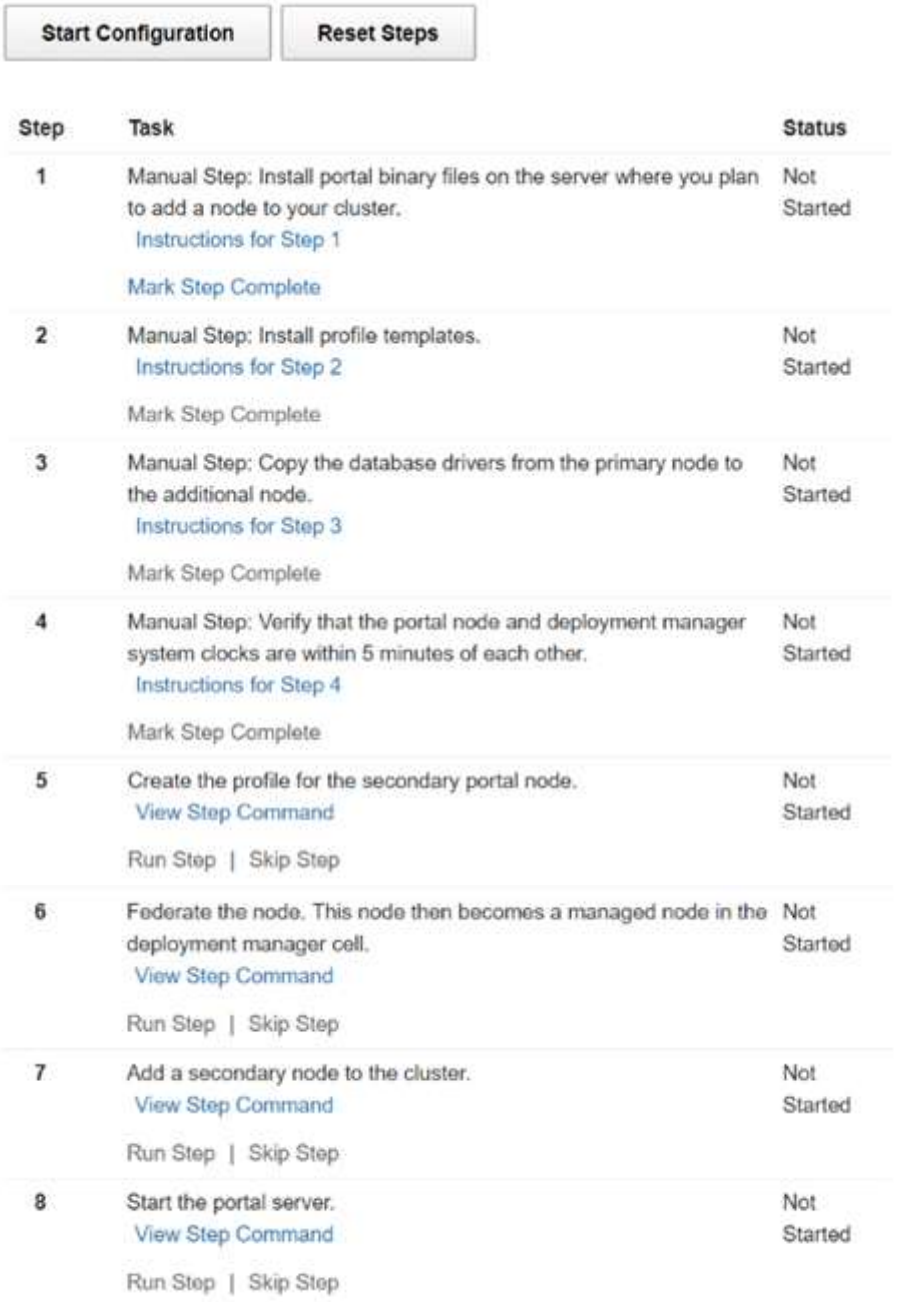


Click the right arrow.

7. Specify your cluster name.

Click the right arrow.

8. You will see the following screen:

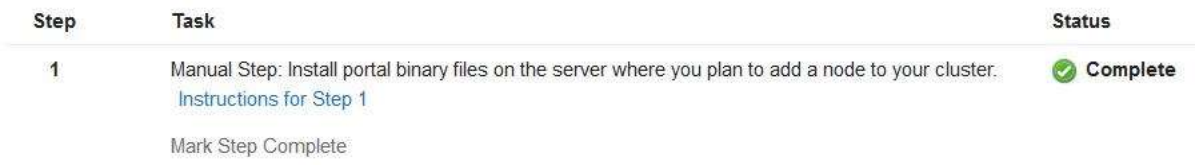


9. Click **Mark Step Complete** for Step 1, since you have already installed the Portal binaries on this server.

10. On the primary Portal server, copy the following file to the additional horizontal node.

    /opt/HCL/WebSphere/PortalServer/profileTemplates/profileTemplates.zip

    Save the .zip file in the /opt/HCL/WebSphere/PortalServer/profileTemplates folder on the additional horizontal Portal node. If the profileTemplates folder does not exist on the additional horizontal Portal node, create it.



11. Run the following to unzip the file:

    cd /opt/HCL/WebSphere/PortalServer/profileTemplates

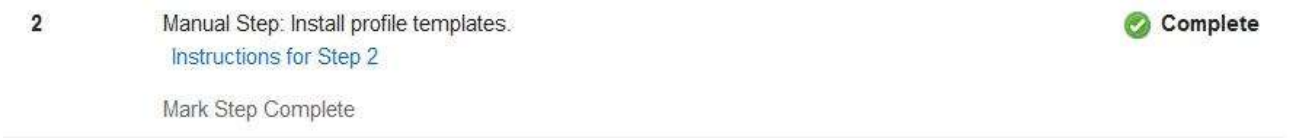
    unzip profileTemplates.zip

12. Run the following to install the profile templates copied from the primary server:

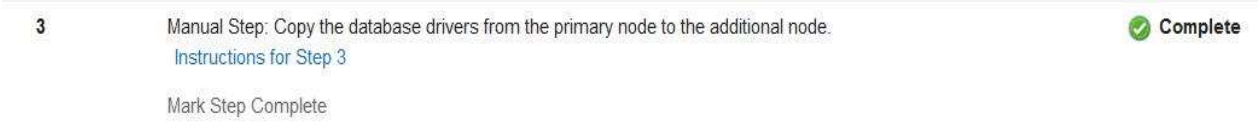
    ./installPortalTemplates.sh /opt/HCL/WebSphere/AppServer

    Adjust the path to the AppServer directory to match your environment if necessary.

13. Click **Mark Step Complete** for Step 2.



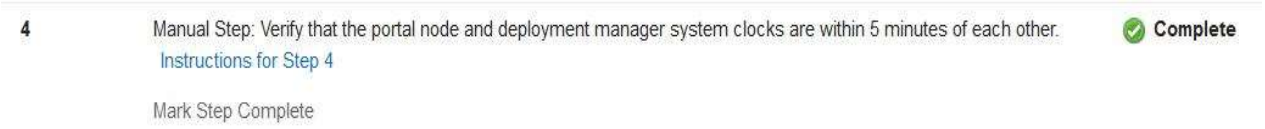
14. Click **Mark Step Complete** for Step 3.



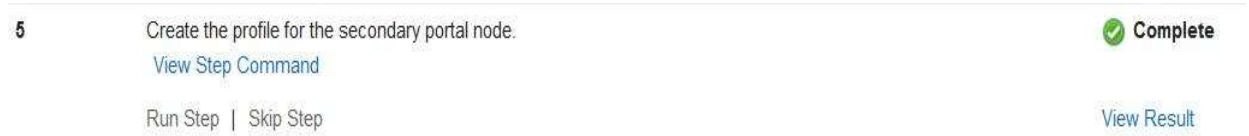
NOTE: This guide specified in Chapter 2 to place the database drivers in the <wp_profile>/PortalServer/dbdrivers directory. They will be automatically copied over as a part of the profileTemplates.zip file. Therefore, this guide required no additional actions to complete this step. If the database drivers are outside of the wp_profile directory in your environment, then they will not get packaged up in the profileTemplates.zip file. You will need to do the manual copy the drivers to the additional horizontal node in the same directory location as primary node.

15. Ensure that the system clocks on the Primary Portal server, additional horizontal Portal node Portal, and the dmgr server are all within five minutes of one another.

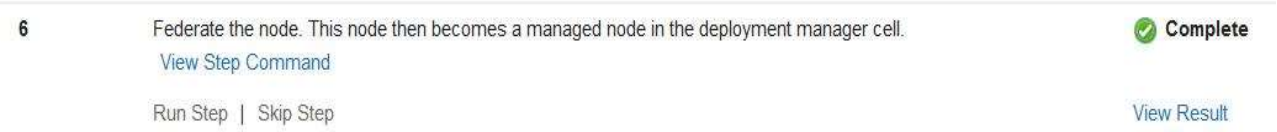
16. Click **Mark Step Complete** for Step 4



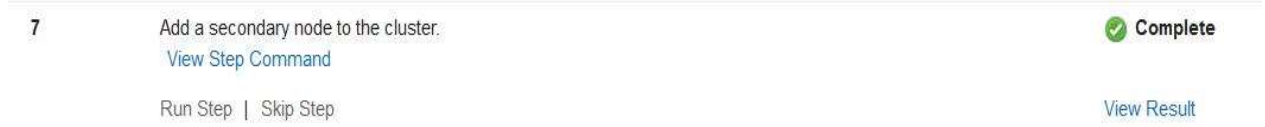
17. Click **Run Step** for Step 5 – Create the profile for the second portal node.



18. Click **Run Step** for Step 6 – Federate the node.

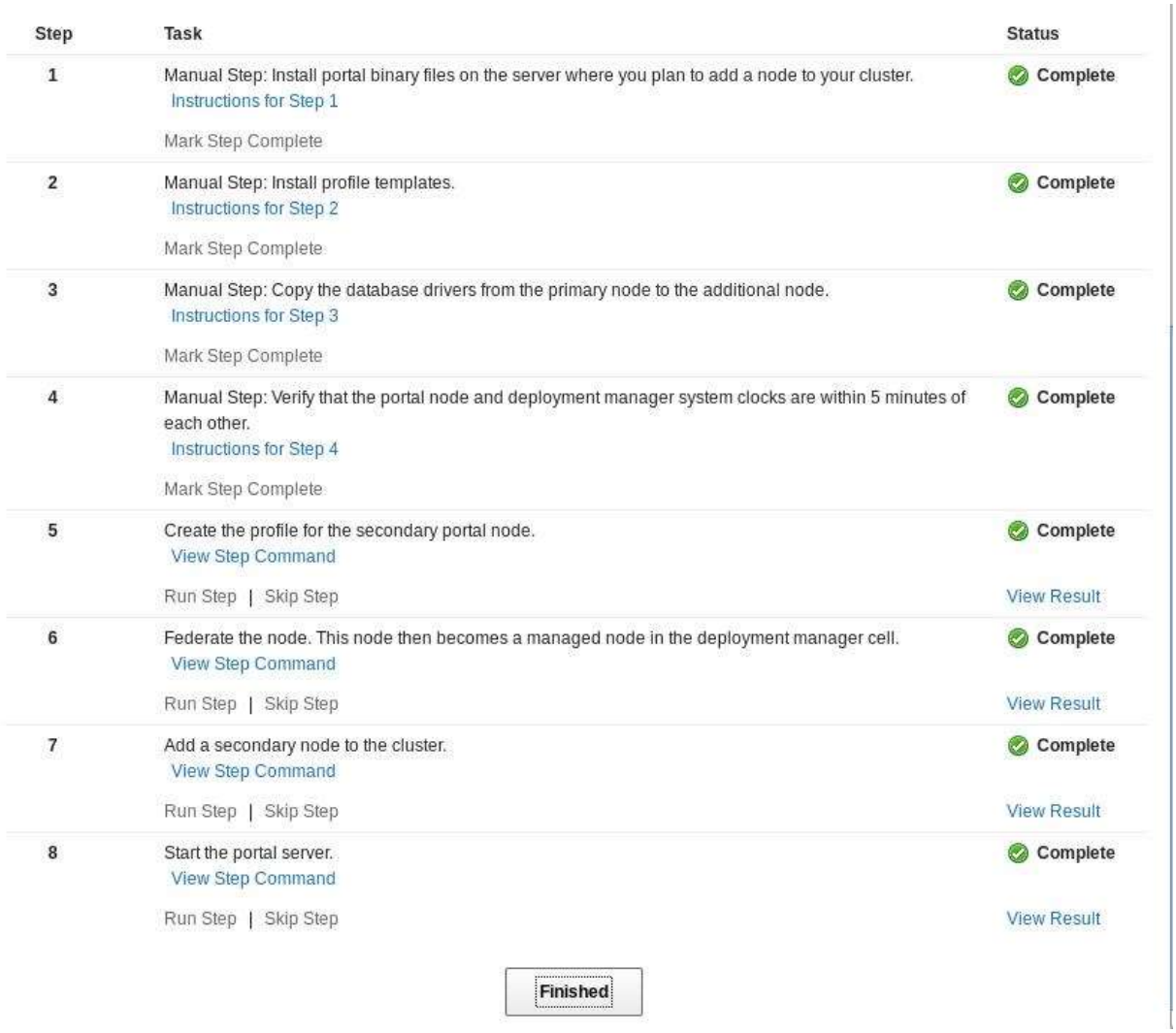


19. Click **Run Step** for Step 7 – Add a secondary node to the cluster.



20. Click **Run Step** for Step 8 – Start the portal server.

21. After each step is successfully completed, the Config Wizard page will match the following:



Step	Task	Status
1	Manual Step: Install portal binary files on the server where you plan to add a node to your cluster. Instructions for Step 1 Mark Step Complete	Complete
2	Manual Step: Install profile templates. Instructions for Step 2 Mark Step Complete	Complete
3	Manual Step: Copy the database drivers from the primary node to the additional node. Instructions for Step 3 Mark Step Complete	Complete
4	Manual Step: Verify that the portal node and deployment manager system clocks are within 5 minutes of each other. Instructions for Step 4 Mark Step Complete	Complete
5	Create the profile for the secondary portal node. View Step Command Run Step | Skip Step	Complete View Result
6	Federate the node. This node then becomes a managed node in the deployment manager cell. View Step Command Run Step | Skip Step	Complete View Result
7	Add a secondary node to the cluster. View Step Command Run Step | Skip Step	Complete View Result
8	Start the portal server. View Step Command Run Step | Skip Step	Complete View Result

Finished

Click **Finished.**

22. Verify that you can access both your Primary Portal:

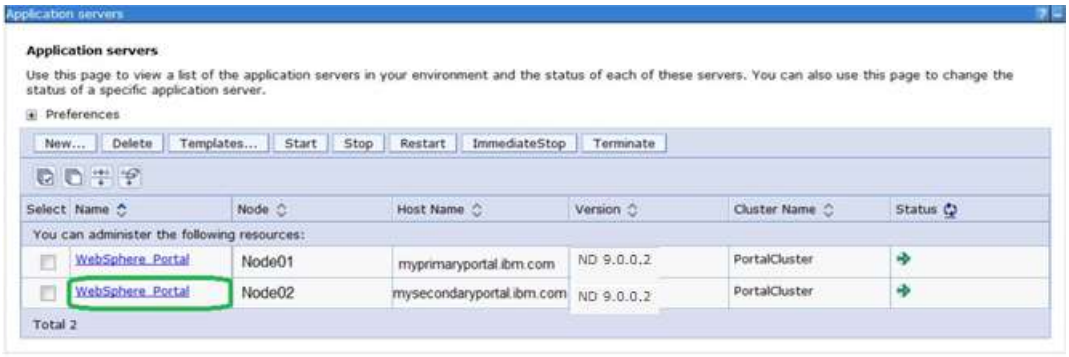
    http://myprimaryportal.hcl.com:10039/wps/portal

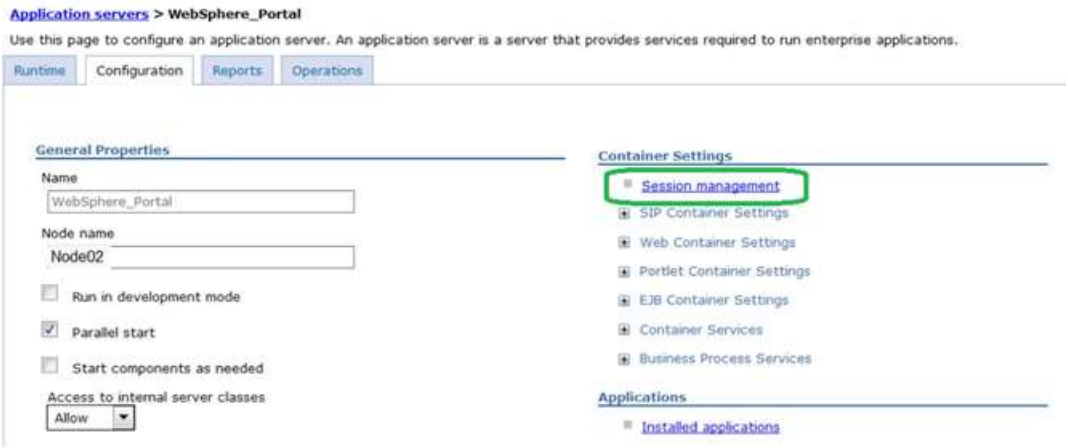
    and your additional horizontal Portal node:

    http://mysecondaryportal.hcl.com:10039/wps/portal

    In the following steps, you will enable memory to memory replication for the additional horizontal node you created.

23. While logged in to the dmgr, navigate to **Servers → Server Types → WebSphere application servers → WebSphere_Portal** (additional horizontal Node02) **→ Session Management → Distributed Environment Settings**.

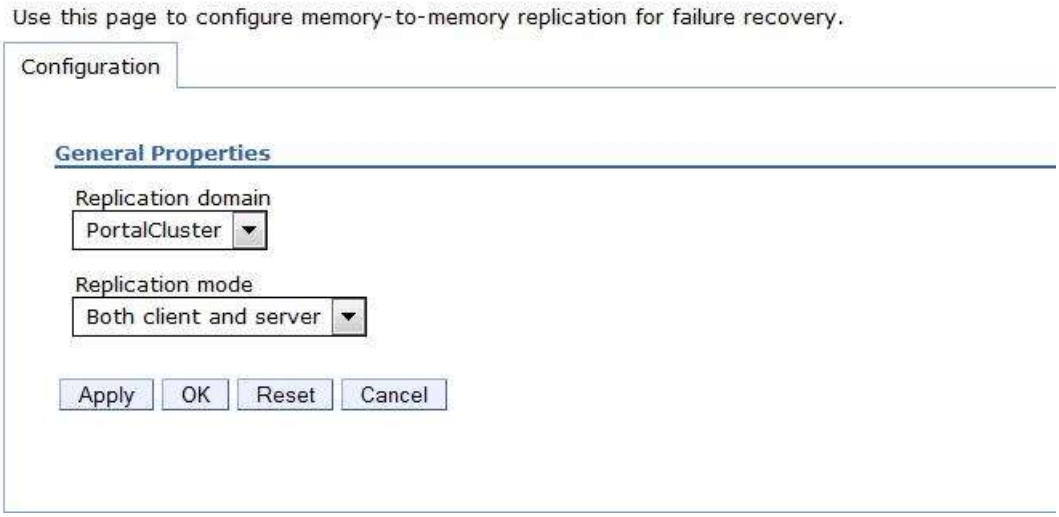




24. Click the blue link for **Memory-to-memory replication**.

25. In the Replication Domain drop-down menu, select your cluster (e.g. PortalCluster).

26. In the Replication Mode drop-down menu, select **Both client and server**.



28. Click **OK** and Save all changes.

29. Back on the **Session management** page (which you should see after saving the changes), click **Custom Properties**.

30. Create a new custom property by clicking **New.**

31. For the **Name**, type in “UseInvalidatedId” and for the **Value**, type in “false”

32. Click **OK** and save the changes.

33. Restart the DMGR, NodeAgent, and WebSphere_Portal server on the additional horizontal node.

34. Verify Portal is functional by accessing it in your web browser:

    http://mysecondaryportal.hcl.com:10039/wps/portal

At this point, you have successfully built a two-node WebSphere Portal cluster using a remote database and federated LDAP security.

Chapter 8 – Configuring the Cluster with an External Web Server

This chapter describes how to configure the Portal cluster with an external web server. In this guide, you will configure the Portal cluster with IBM® HTTP Server (IHS) v9.0.5.0. In previous chapters, the IBM® WebSphere Application Server and HCL® Portal code levels were required to be those shipped with the Portal installation media. In this chapter, no such requirement exists, and you will install IBM® HTTP Server with the latest code levels available

NOTE: Appendix B1 describes how to enable SSL on your web server after completing the steps in this chapter. The authors of this guide strongly recommend SSL be enabled on your Portal cluster. However, SSL is not required for a HCL® Portal cluster to function correctly.

1. IBM® HTTP Server version v9.0 is not included with HCL® Portal installation media. You will need to download the IBM® HTTP Server media separately from HCL® FlexNet: https://www.ibm.com/software/passportadvantage/

This guide uses the following part numbers:
- IBM® WebSphere Application Server v9.0.5 Supplements - IBM® HTTP Server
- IBM® WebSphere Application Server v9.0.5 - Web Server Plugins
- IBM® WebSphere Application Server v9.0.5 Supplements WebSphere Customization Toolkit

2. Download the latest fixpack of IBM® HTTP Server v9 and WebServer Plugin v9 from IBM® Fix Central. Both items are available in a single download.

   This guide uses version v9.0.0.7, available at the following link:
   http://www.ibm.com/support/docview.wss?uid=swg24044620#Supple

3. Copy the downloaded files to your IHS server environment. Extract each of the downloads. This guide the following directory structure:
   - /opt/ihsBinaries/IHS
   - /opt/ihsBinaries/Plugin
   - /opt/ihsBinaries/WCT
   - /opt/ihsBinaries/FP7

4. Copy the following two directories from your primary Portal server to your IHS server:
   - IIM
   - JDK805

5. You will see the following directory structure

```
[root@webserver ihsBinaries]# ls -la
total 0
drwxr-xr-x  7 root root  68 Nov 25 13:19 .
drwxr-xr-x. 6 root root  58 Nov 25 13:13 ..
drwxr-xr-x  9 root root 174 Nov 12 20:09 IHS
drwxr-xr-x  9 root root 122 Sep 29 13:05 IIM
drwxrwxr-x  7 root root 134 Sep 29 13:04 JDK805
drwxr-xr-x  9 root root 174 Nov 12 20:12 Plugins
drwxr-xr-x  9 root root 174 Nov 12 20:12 WCT
```

6. Navigate to:

   /opt/ihsBinaries/IIM/*yourEnvironment*

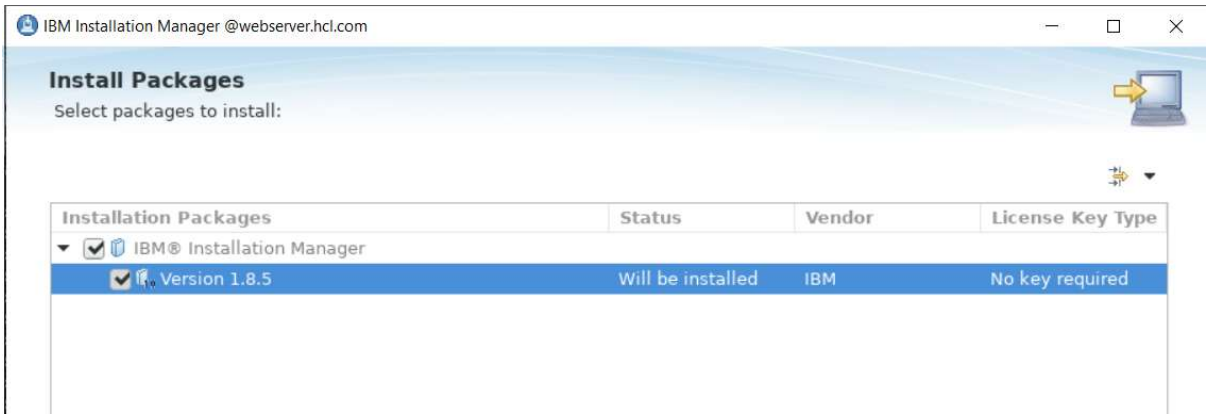
   and run

   ./install

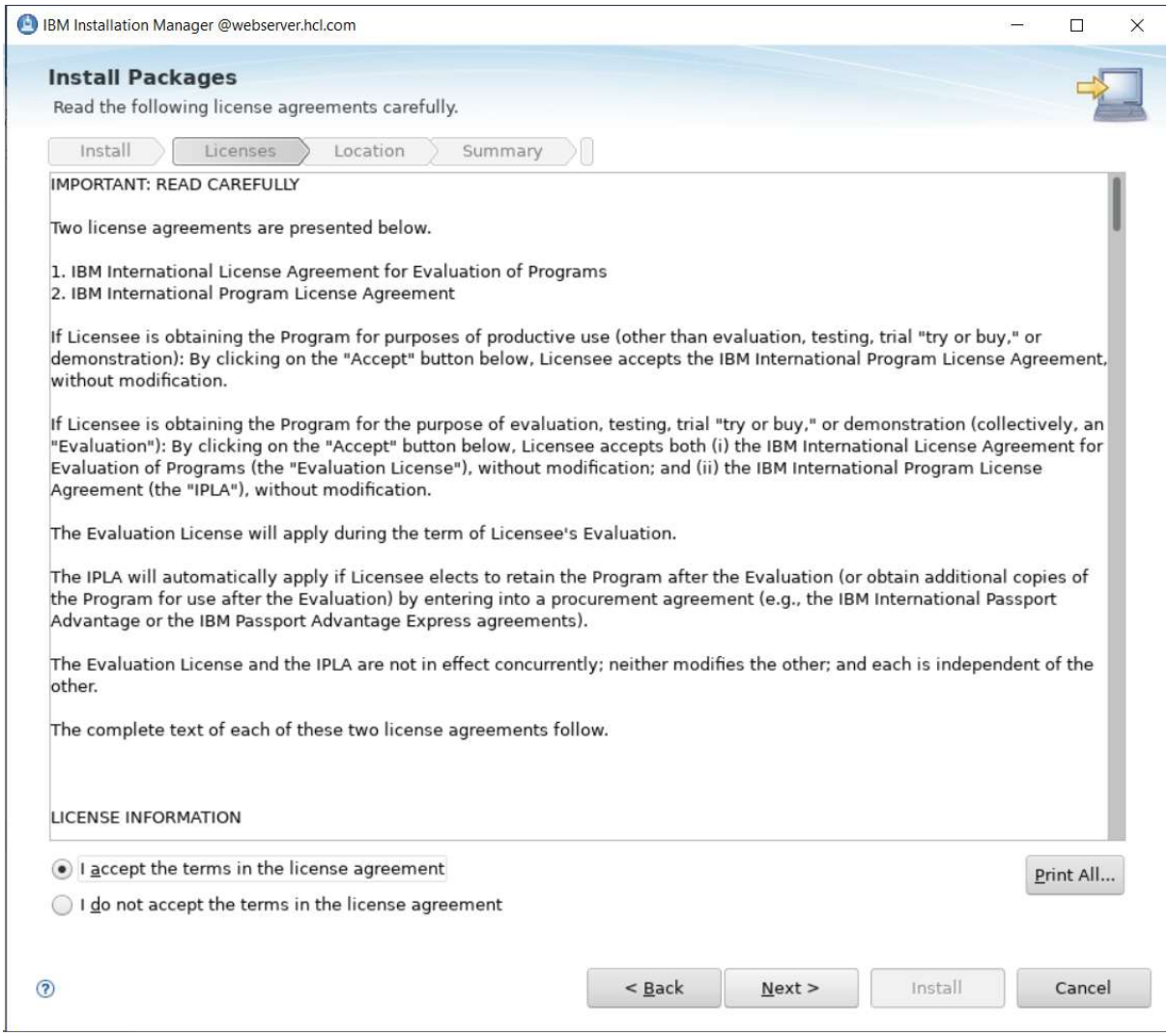
   where *yourEnvironment* is the folder that best describes the operating system of the environment in which you are installing HCL® Portal. For this guide the following is used:

   /opt/ihsBinaries/IIM/linux_x86_64

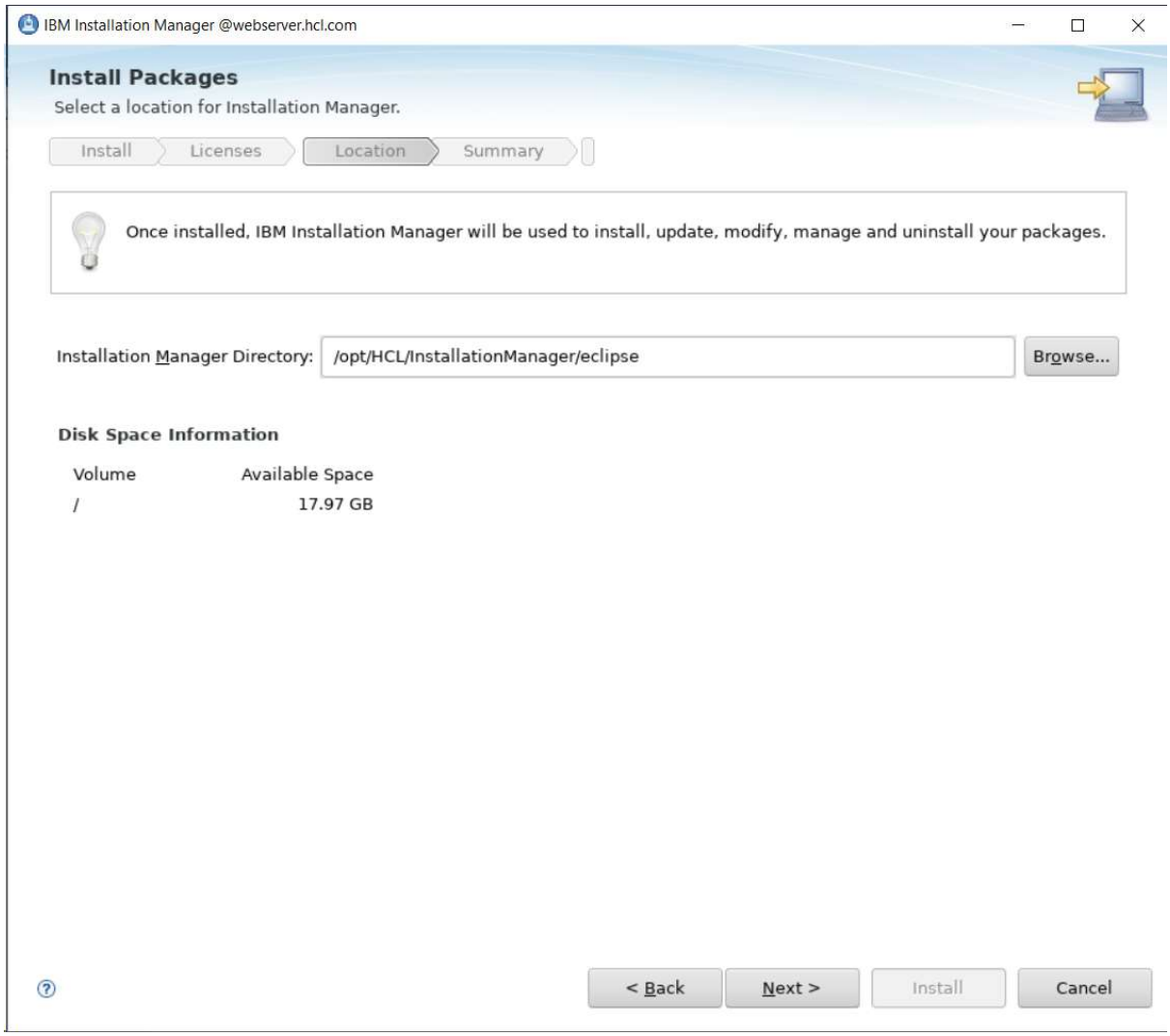
   The following window will appear:



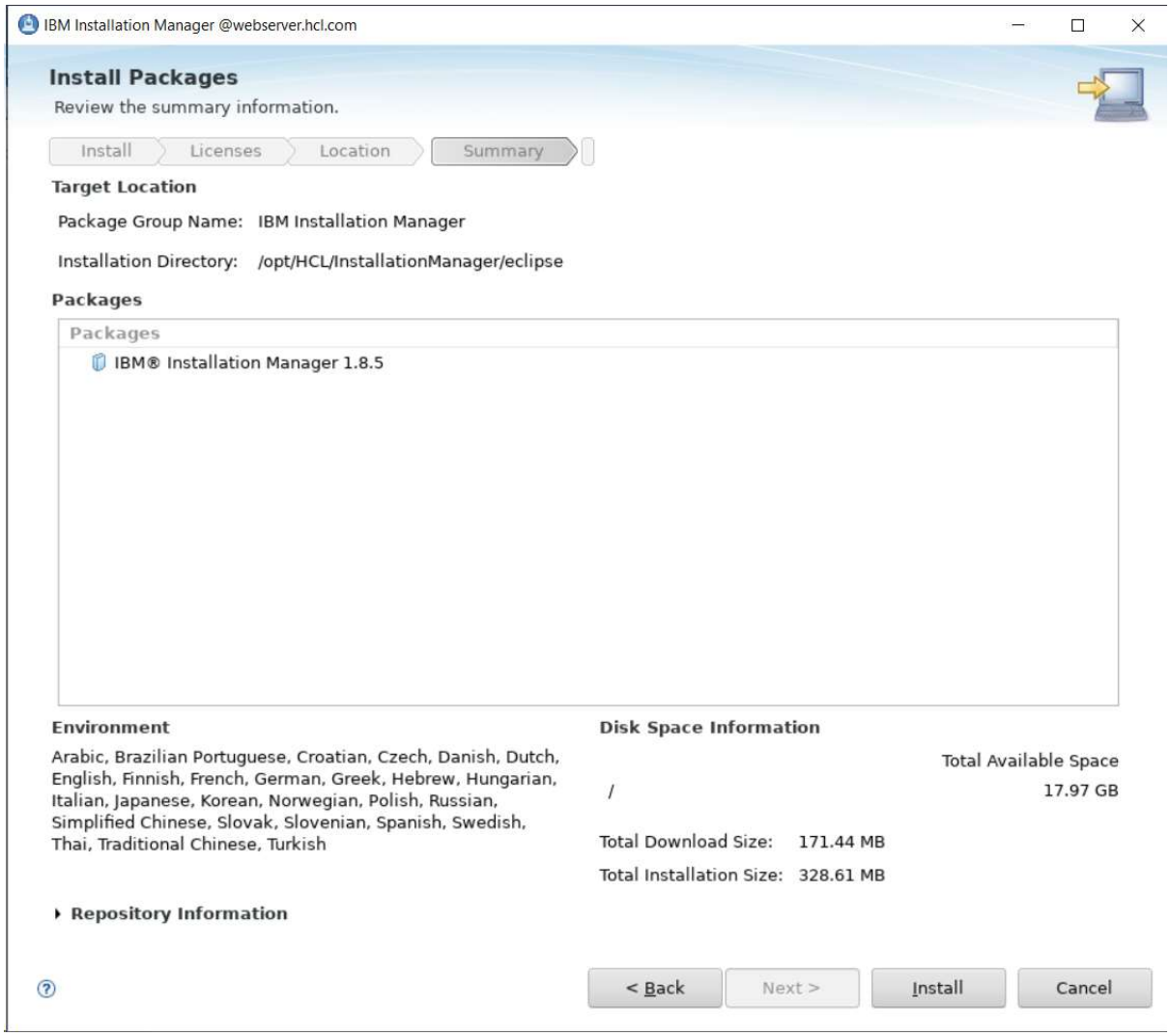
7. Click **Next**.



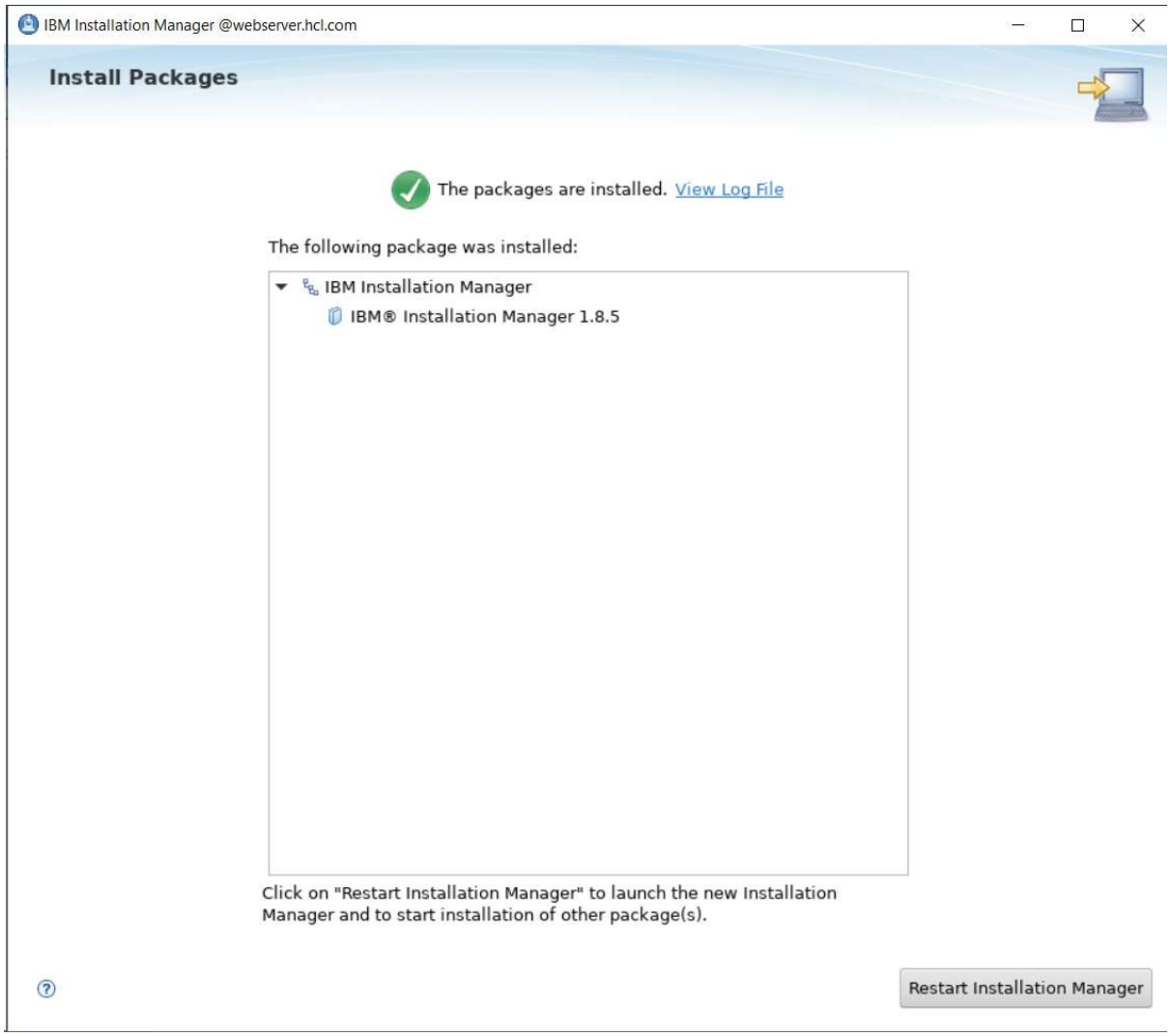
8. Accept the license agreement and click **Next**.



9. Update the Installation Manager Directory and Click **Next**

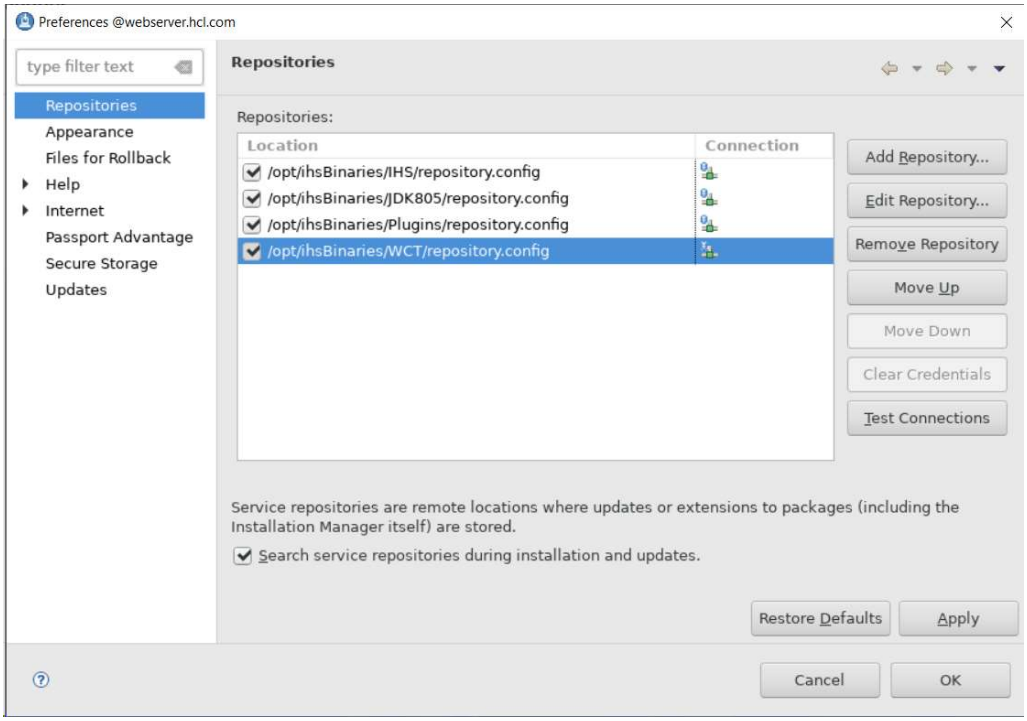


10. Click on Install



11. Click on **Restart Installation Manager**

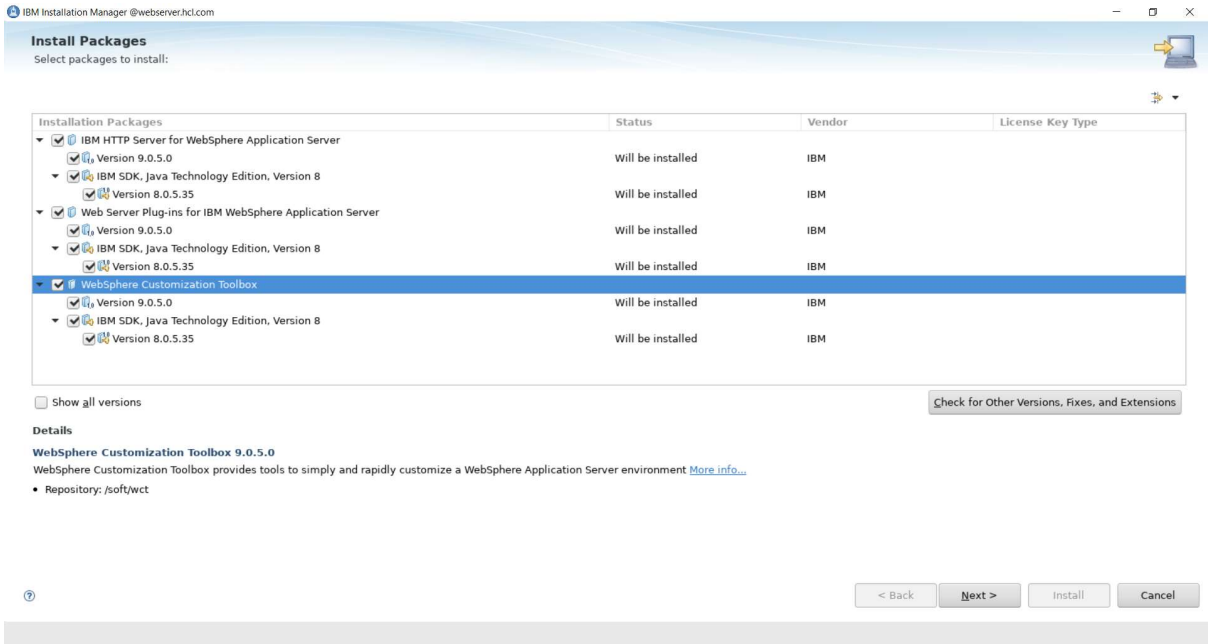
12. Add the repositories for the IBM® HTTP Server, WebServer Plugin and WebSphere Customization Toolbox, and Java805. Your end result should look like:



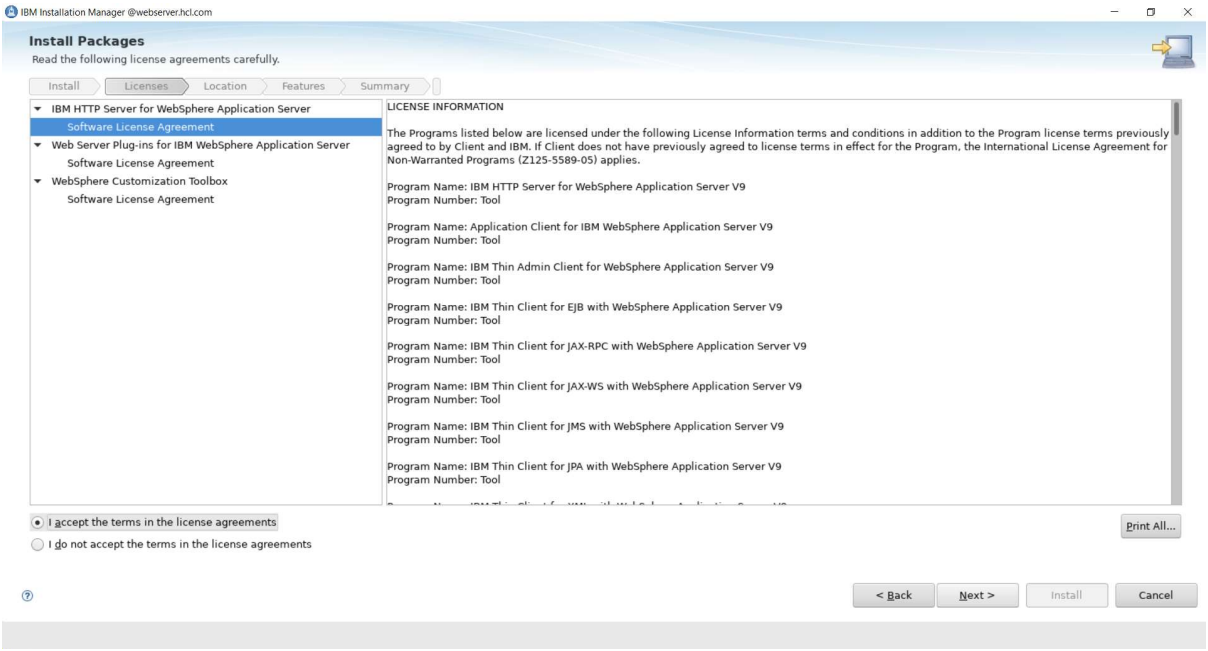
13. Click OK to save the changes.

14. On the Installation Manager screen, click Install.

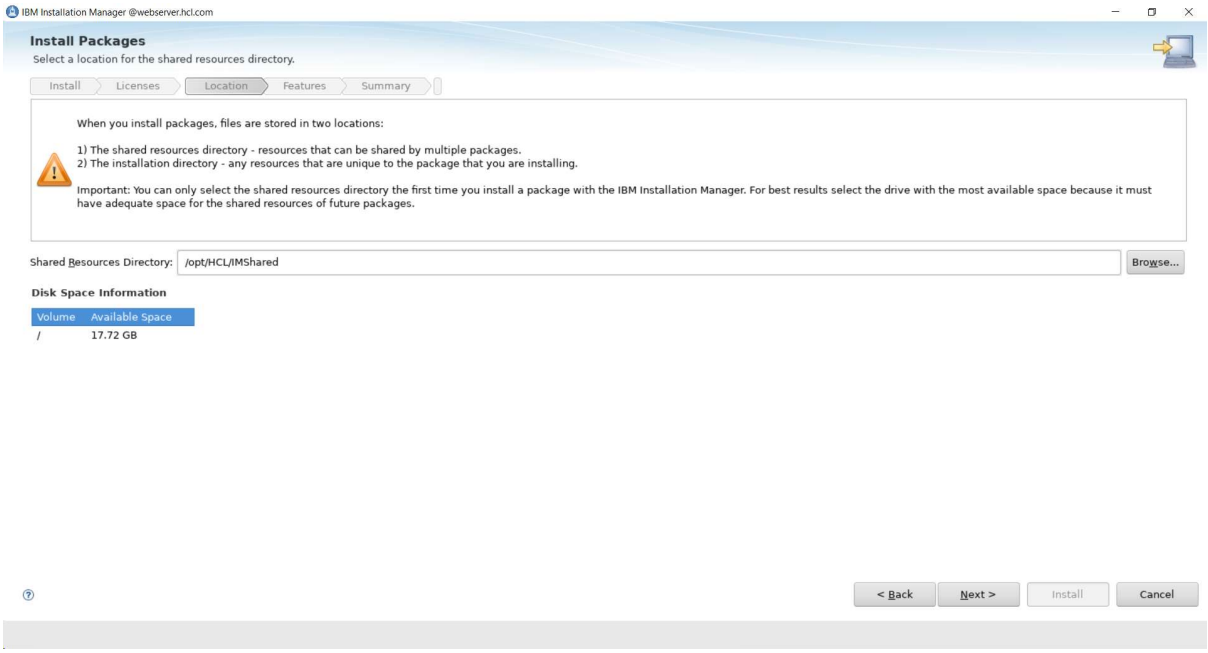
15. Check the box for IBM HTTP Server for WebSphere Application Server, Web Server Plug-ins, and WebSphere Customization Toolbox. Click Next:



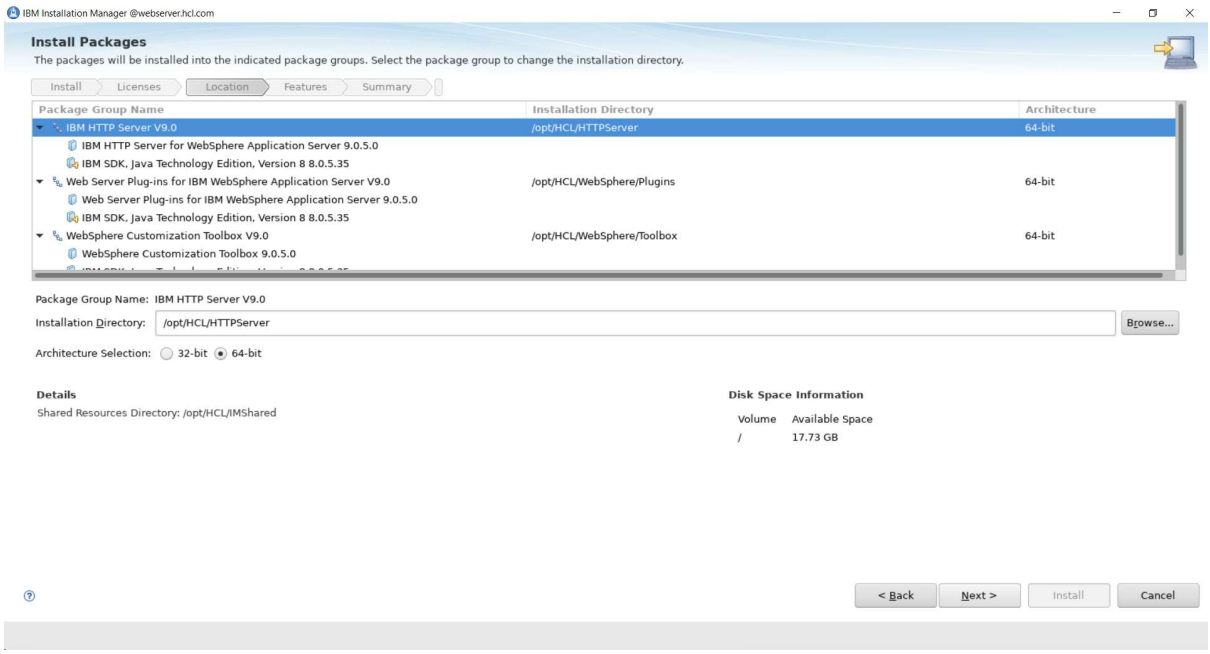
16. Accept the license agreement and click Next.



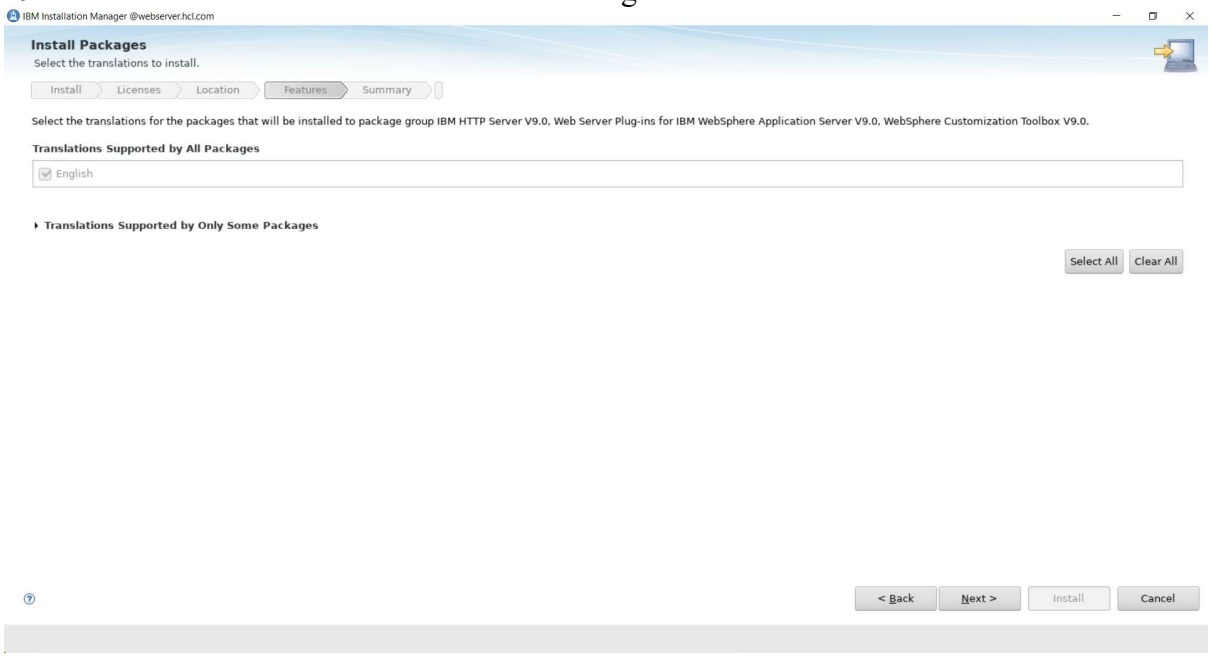
17. You will see a screen to select the Installation directory for shared objects used by IIM. Choose a directory and click Next.



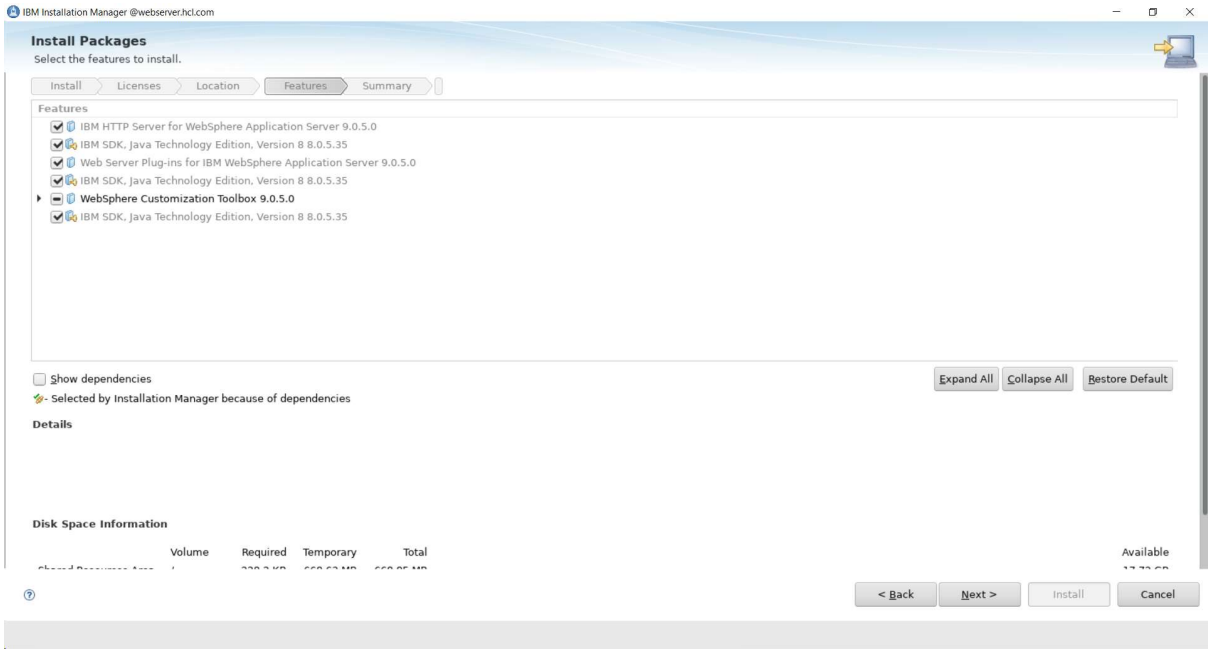
18. Click the Package Group Name for each component and select an Installation Directory. This guide uses the prepopulated defaults. Click **Next**.



19. Select additional translations to install. This guide chose no additional translations. Click **Next**:

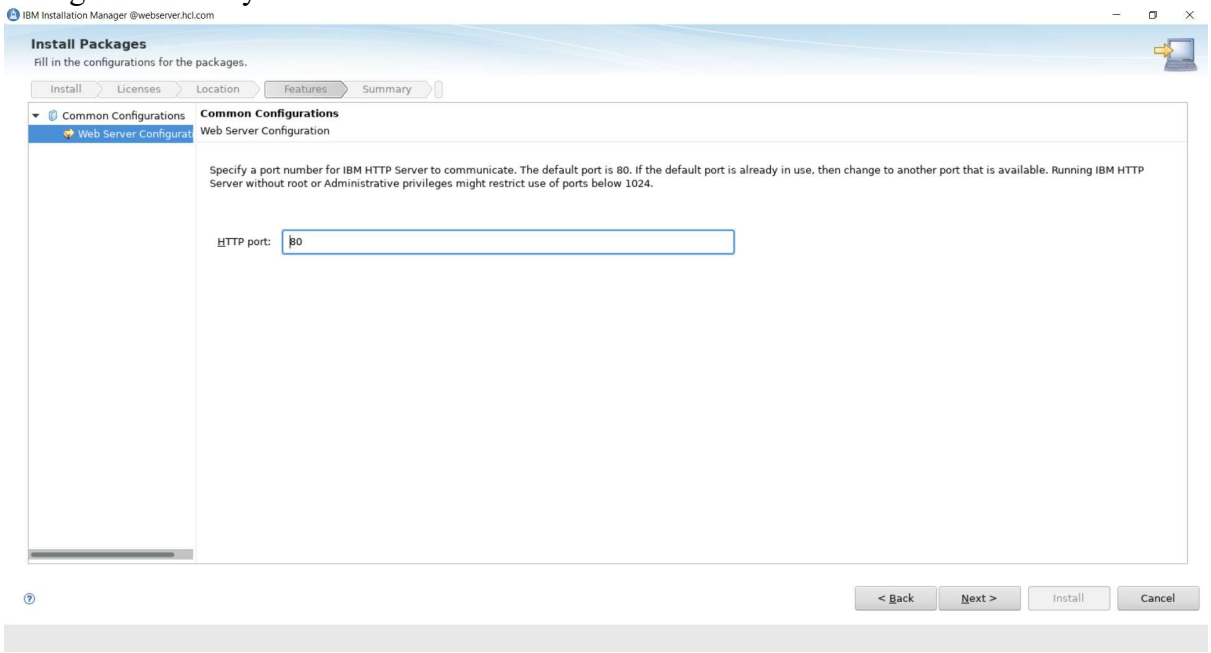


20. Select any additional features you'd like for the WebSphere Customization Toolbox. For this guide, the defaults were used. Click **Next**:

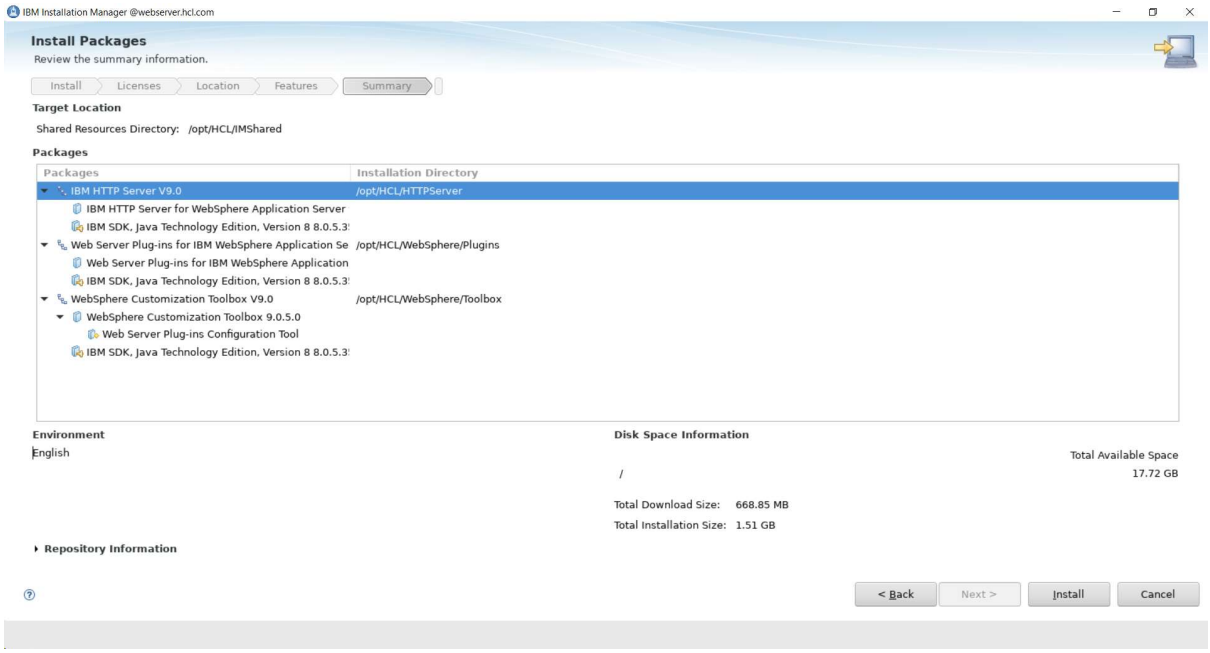


21. Select the non-SSL HTTP Port for the web server. This guide recommends the prepopulated default port 80. Click **Next**:

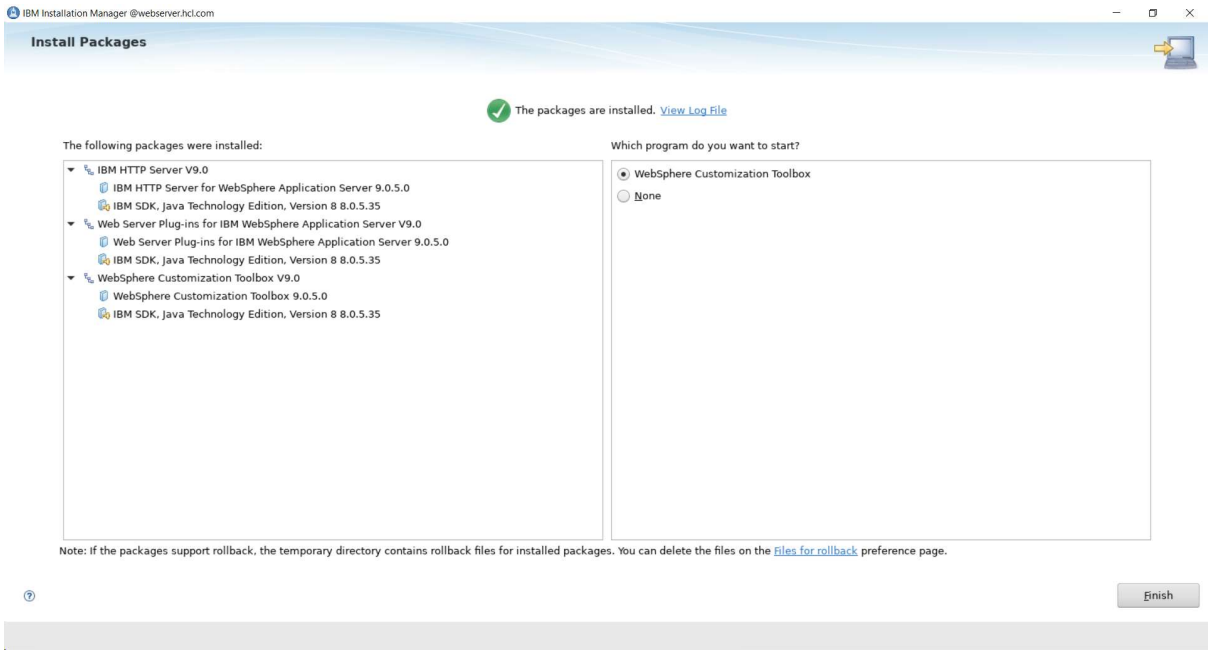
NOTE: You can modify your IHS configuration post-installation to remove the HTTP port and configure SSL for your web server.



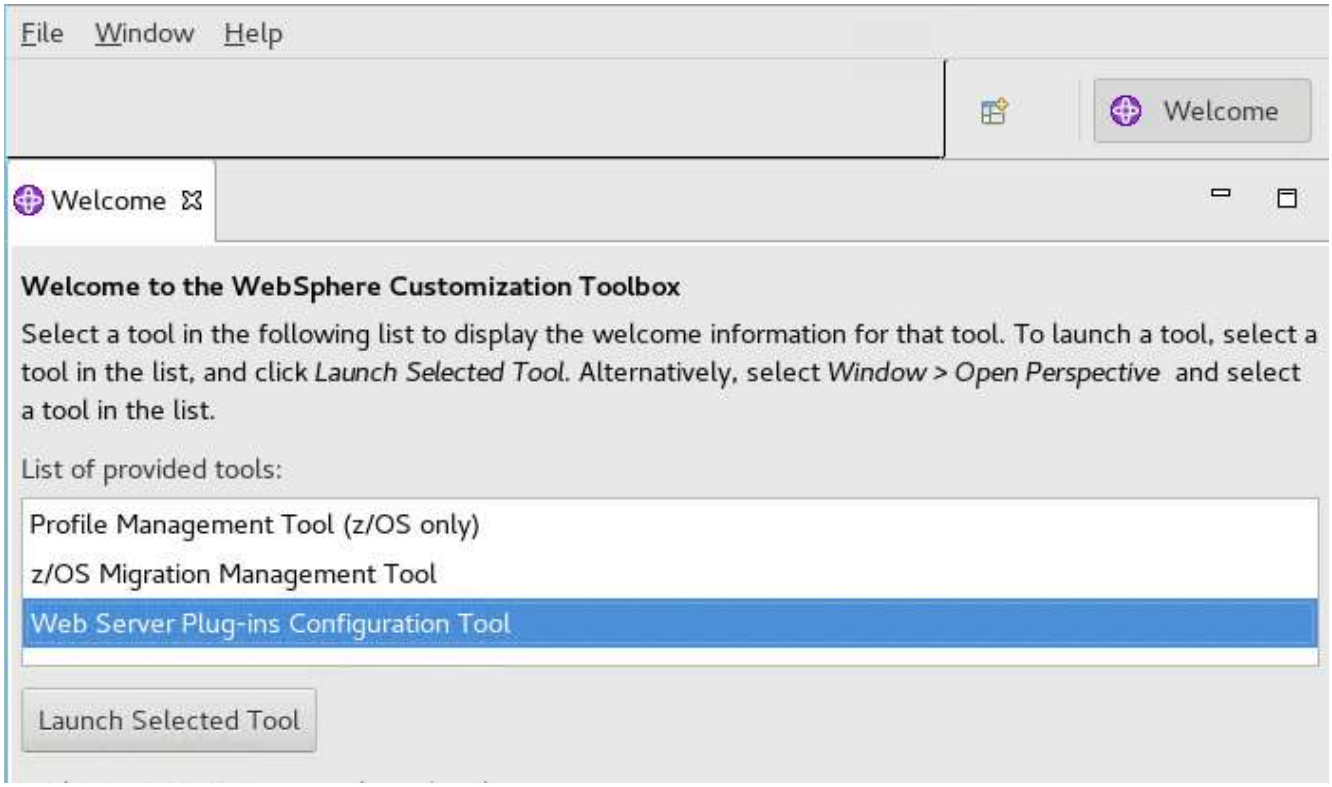
22. On the summary screen, ensure everything is correct and click Install to begin the installation.



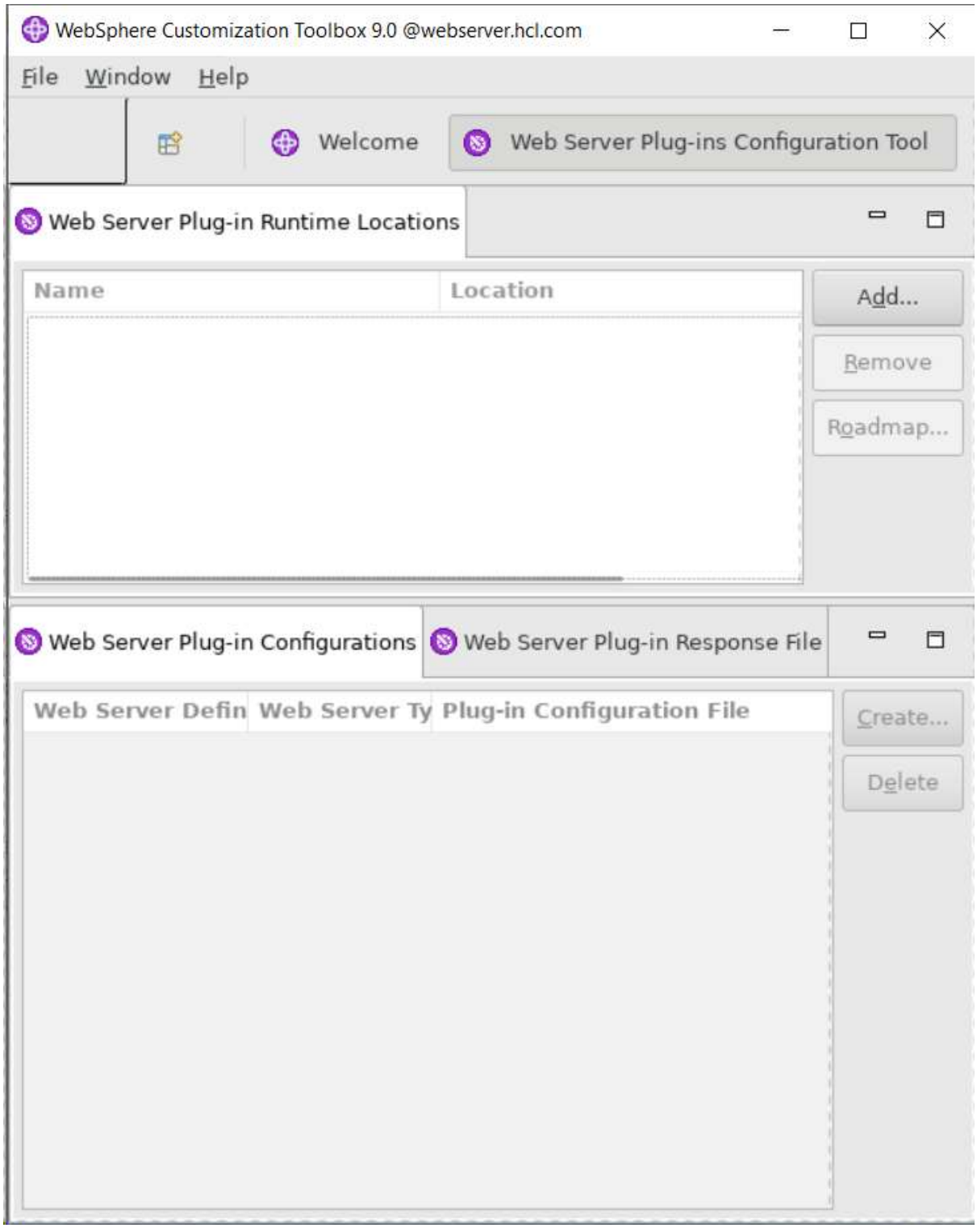
23. Once the installation finishes, select the radio button for WebSphere Customization Toolbox and click Next:



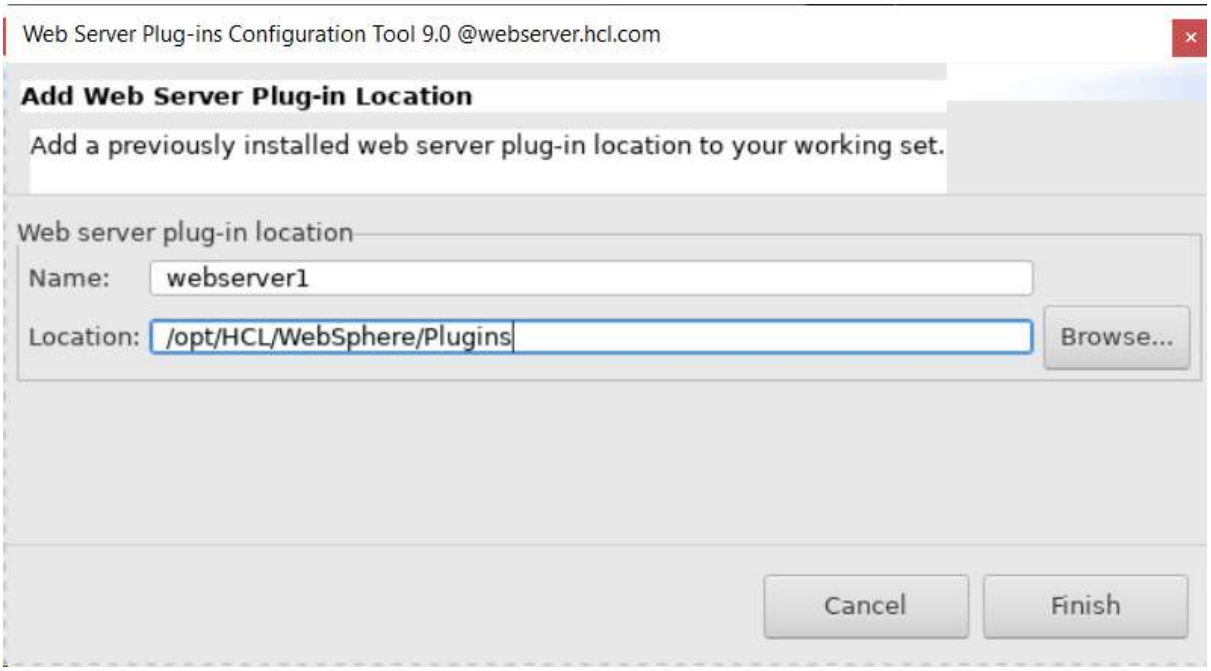
24. When WebSphere Customization Toolbox loads, select **'Web Server Plug-ins Configuration Tool'** and click **'Launch Selected Tool**:



25. In the ‘Web Server Plugin Runtime Location’ window, click ‘**Add…**’.

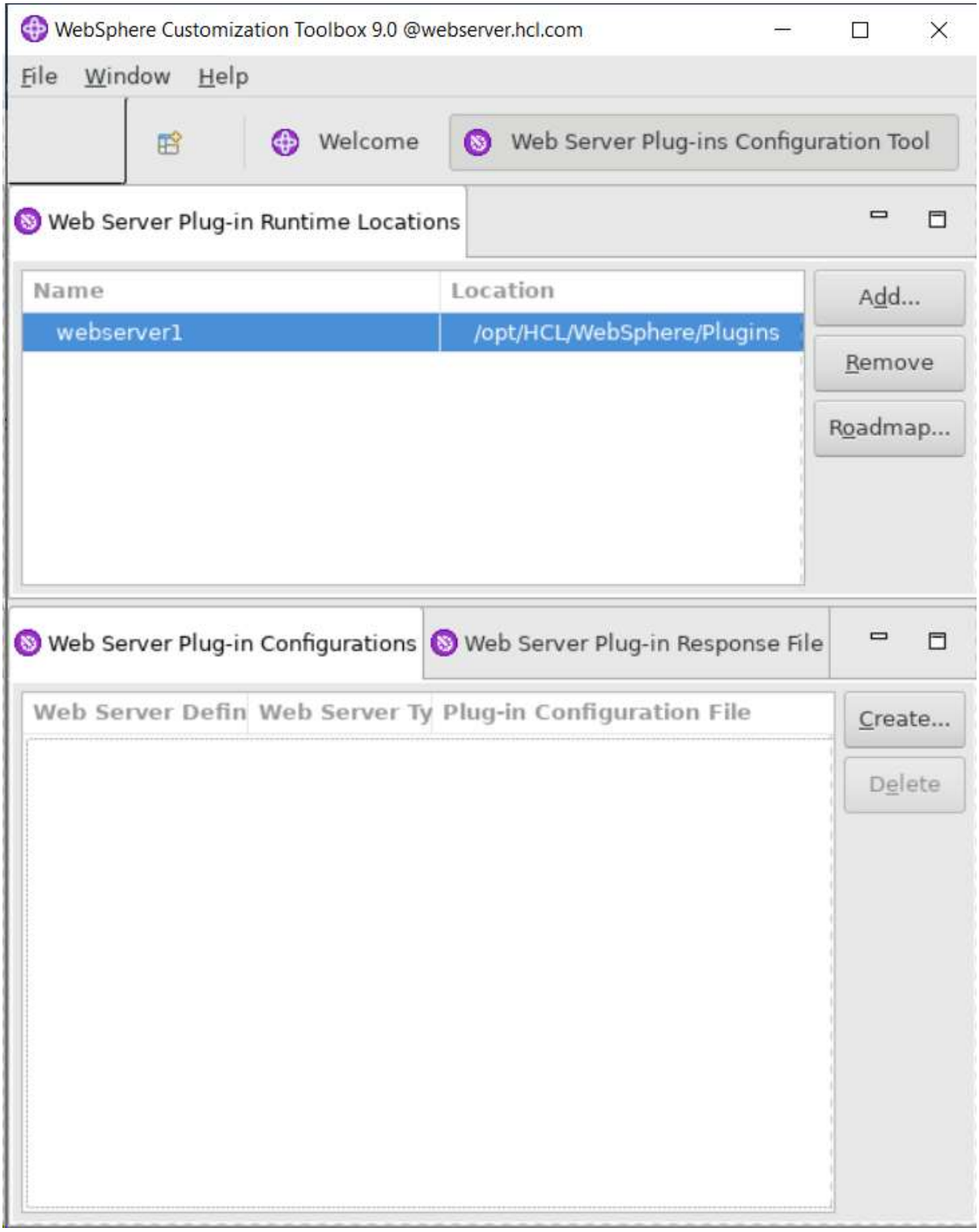


26. Provide a Web Server name and the location of the WebSphere Plug-ins directory. This guide recommends **webserver1** for the name and uses the default directory location specified during installation **/opt/HCL/WebSphere/Plugins**

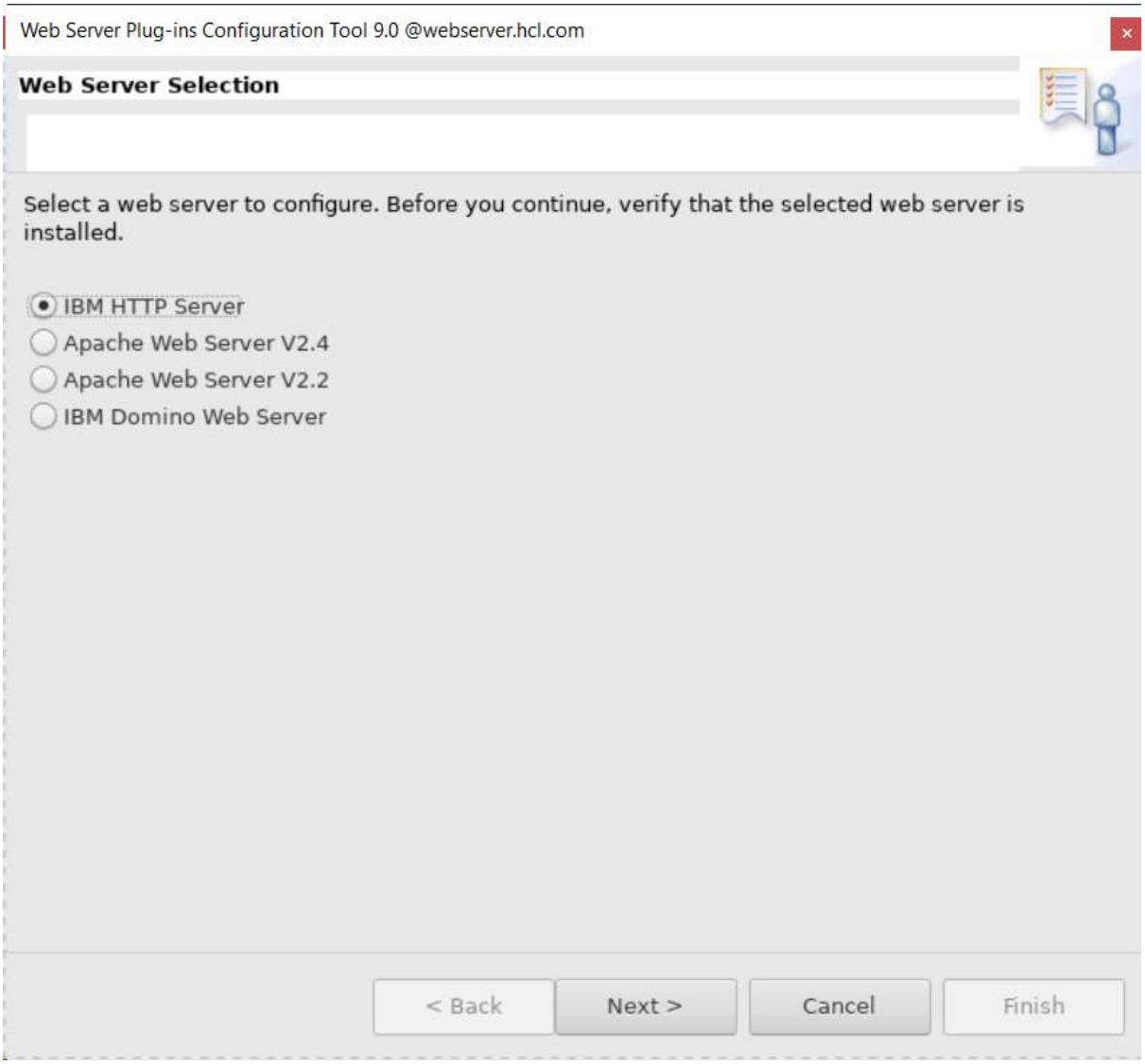


27. Click Finish.

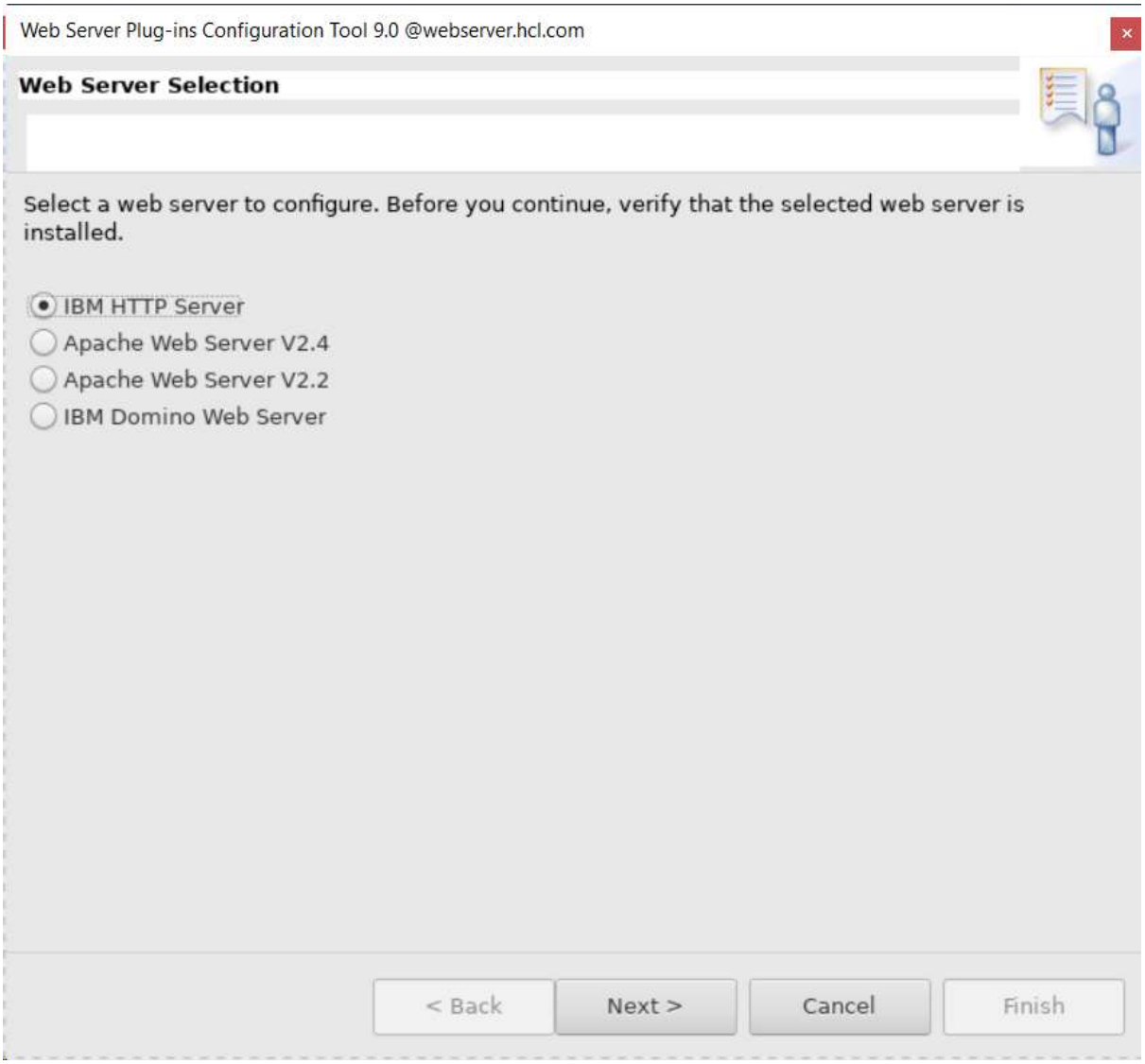
28. You will now see the **webserver1** name defined in the top window titled Web Server Plug-in Runtime Locations. In the bottom window titled Web Server Plugin Configurations click **Create**.



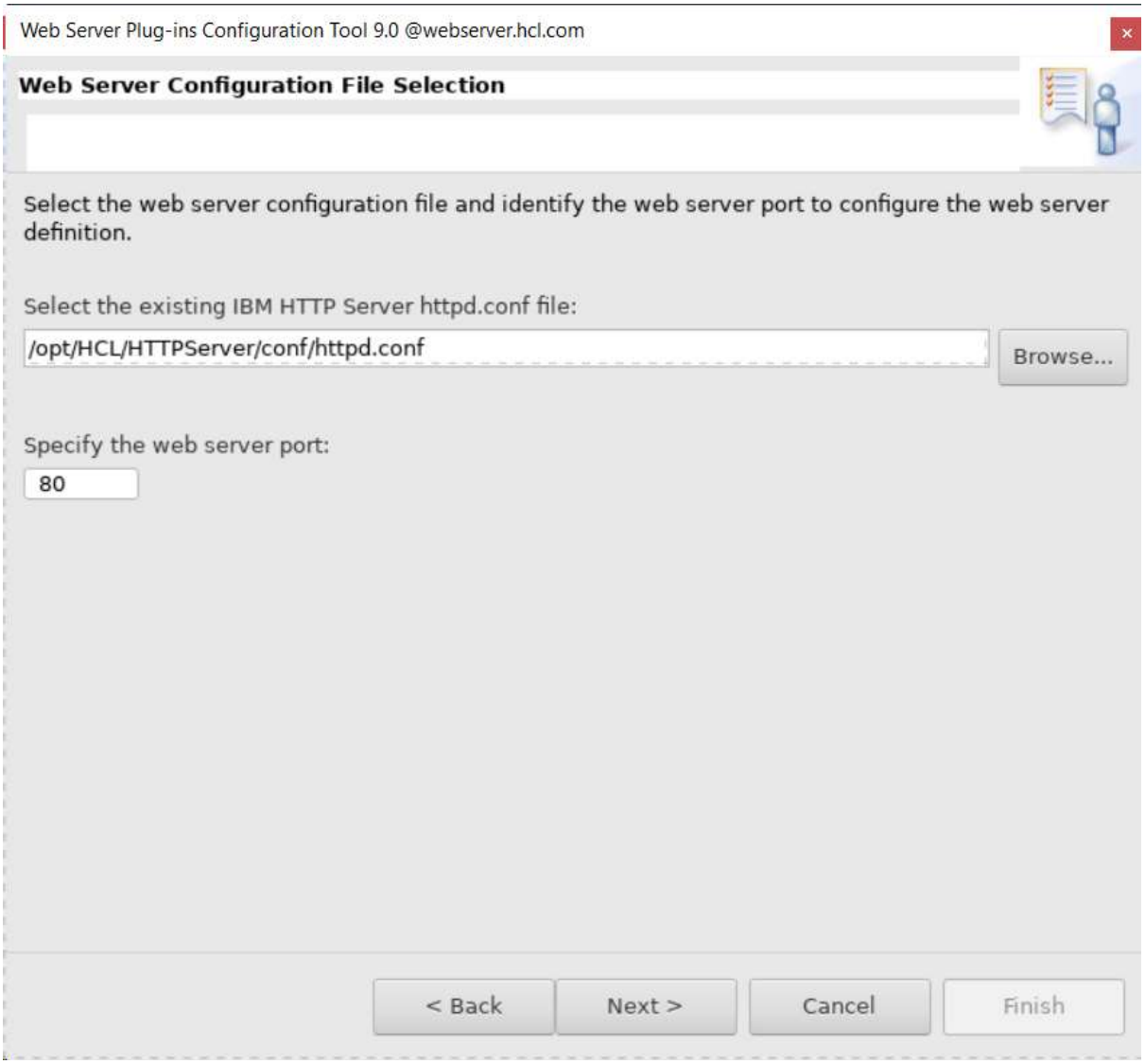
29. Select your Web Server type and click Next. This guide uses IBM HTTP Server.



30. Select the architecture of the installed target web server. This guide uses **64 bit.** **C**lick **Next**.

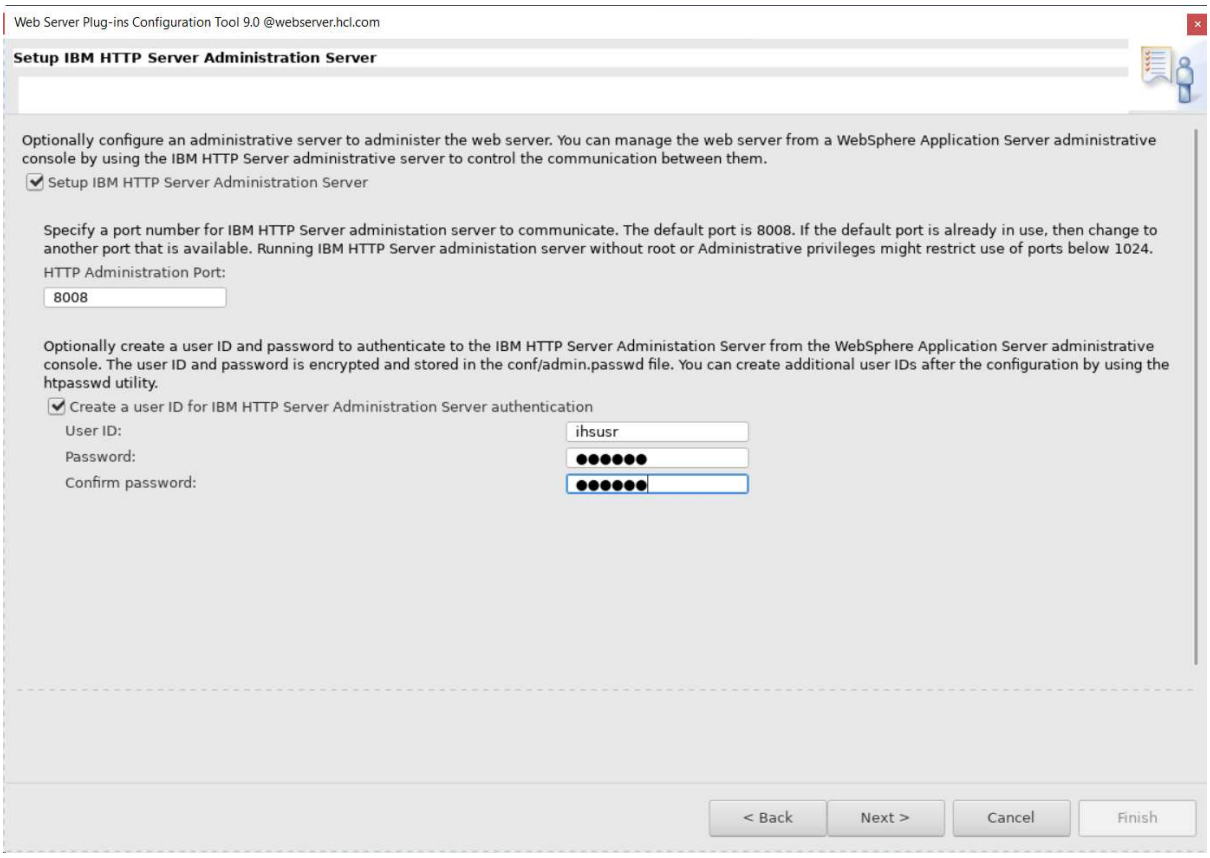


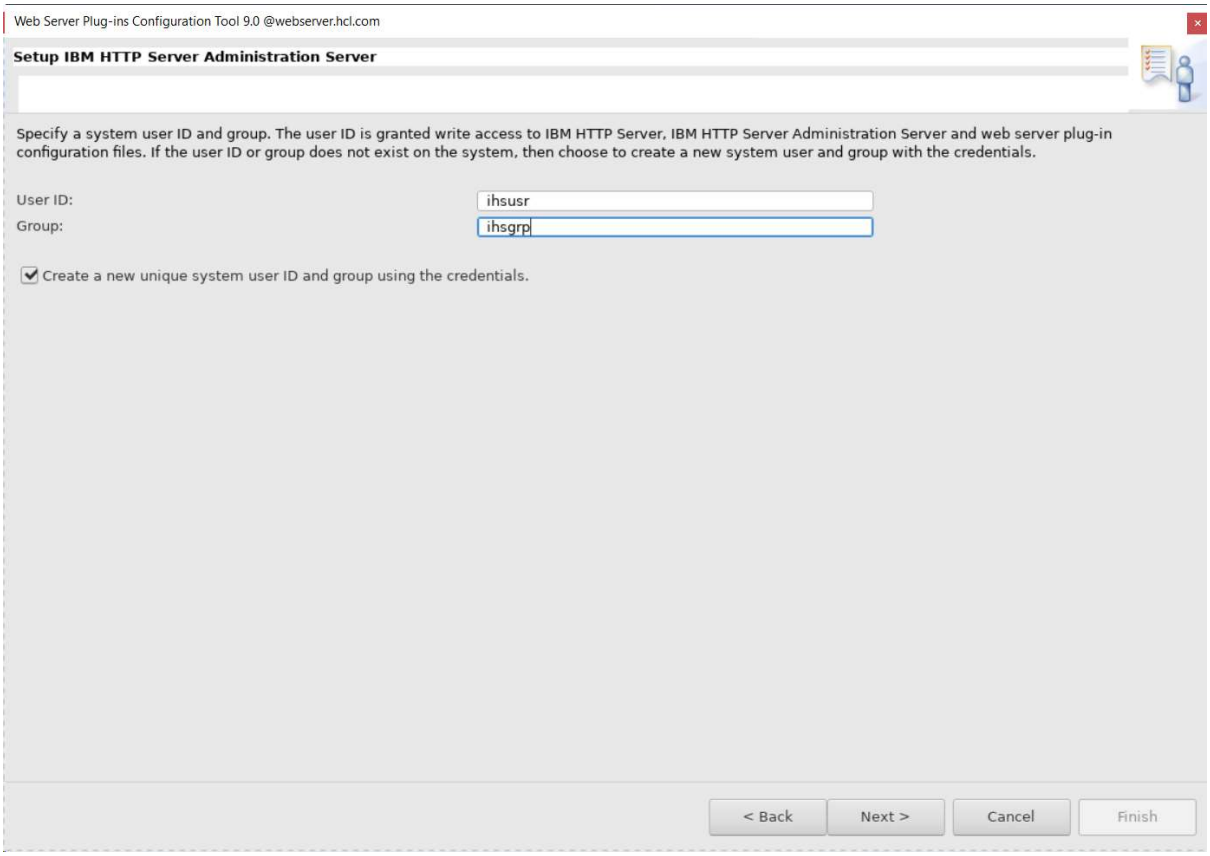
31. Specify the location of the httpd.conf file and the port you chose during installation. This guide uses the prepopulated defaults of **/opt/HCL/HTTPServer/conf/httpd.conf** for the directory and **80** for the port. Click **Next**.



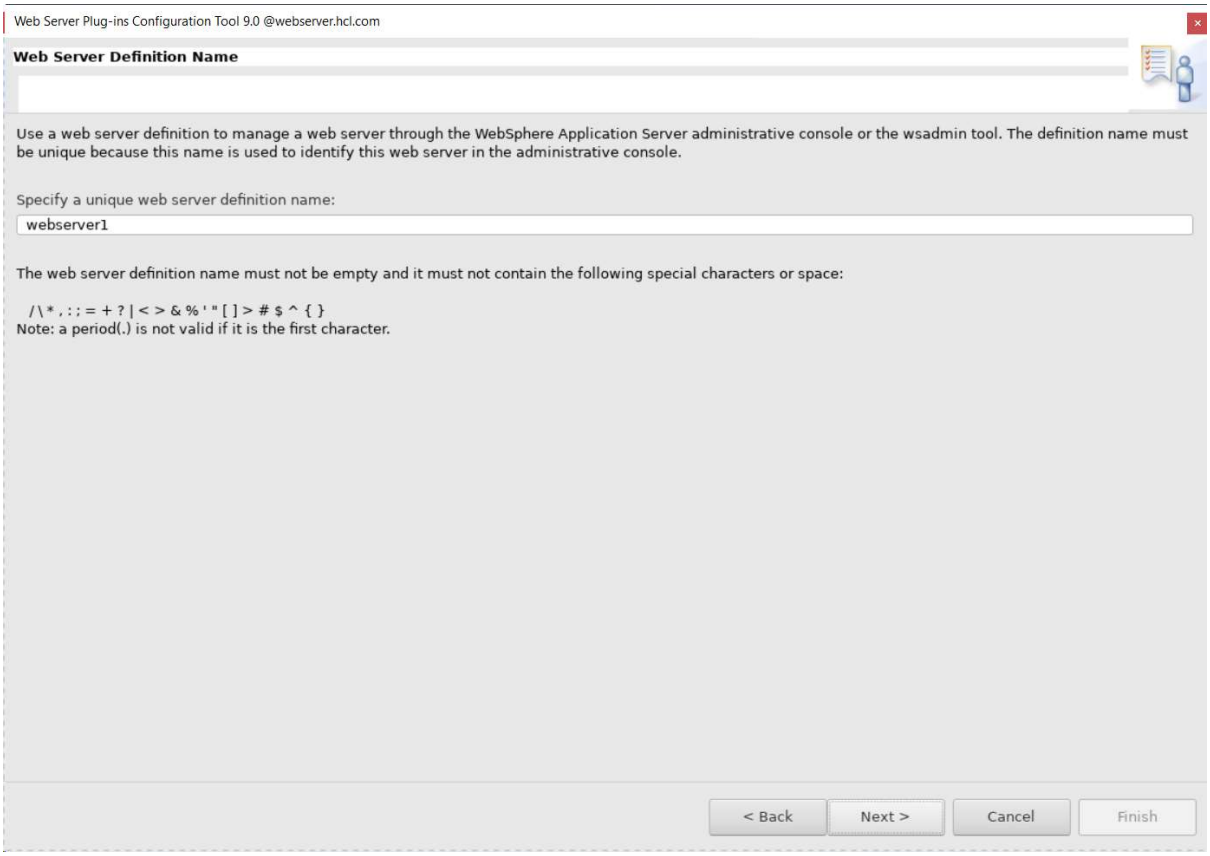
32. Select to Setup IBM HTTP Server Administration Server.

Create userid/ group and password as per the orgnization policy-

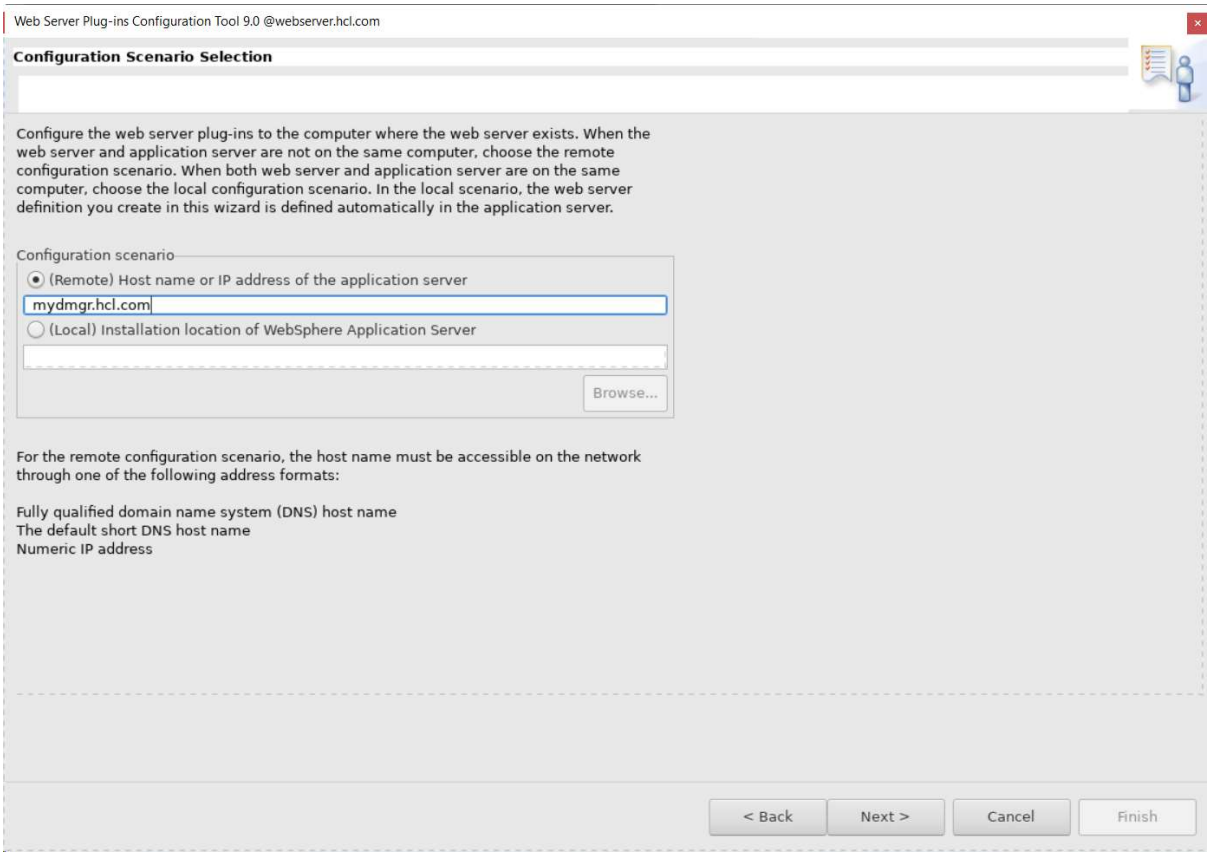



Web Server Plug-ins Configuration Tool 9.0 @webserver.hcl.com
Setup IBM HTTP Server Administration Server
Specify a system user ID and group. The user ID is granted write access to IBM HTTP Server, IBM HTTP Server Administration Server and web server plug-in configuration files. If the user ID or group does not exist on the system, then choose to create a new system user and group with the credentials.
User ID:
ihsusr
Group:
ihsgrp
Create a new unique system user ID and group using the credentials.
< Back
Next >
Cancel
Finish

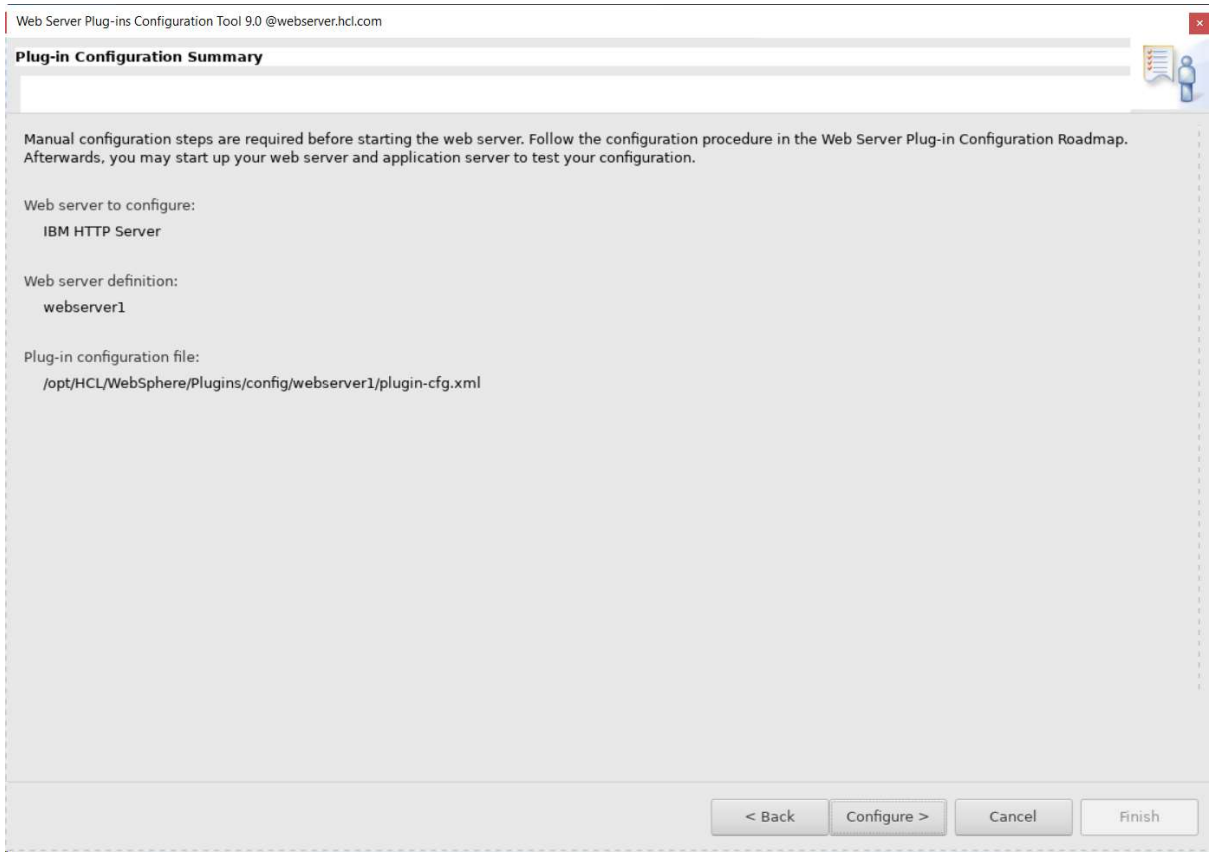
33. Specify the name of your webserver you created previously. This guide uses **webserver1.** Click **Next**.



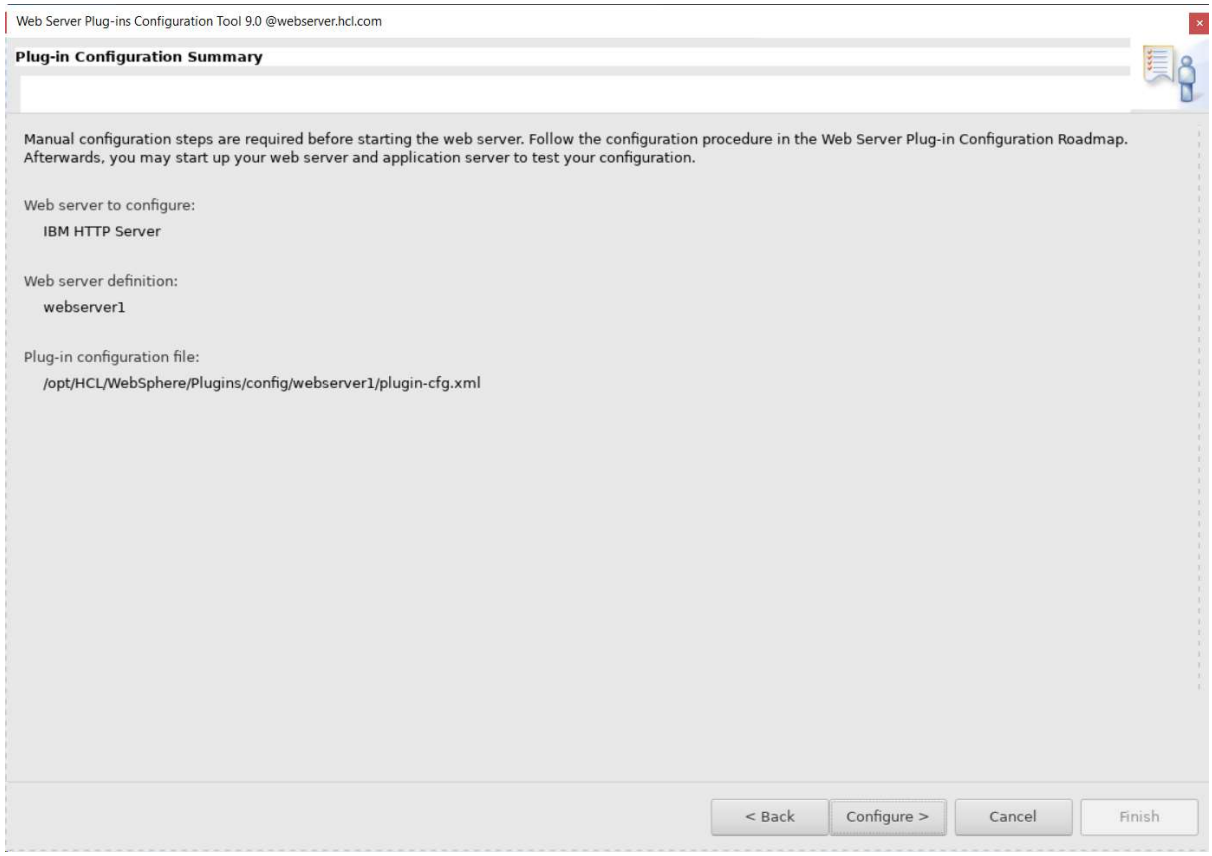
34. On this next screen enter the hostname of your Deployment Manager and click **Next**.



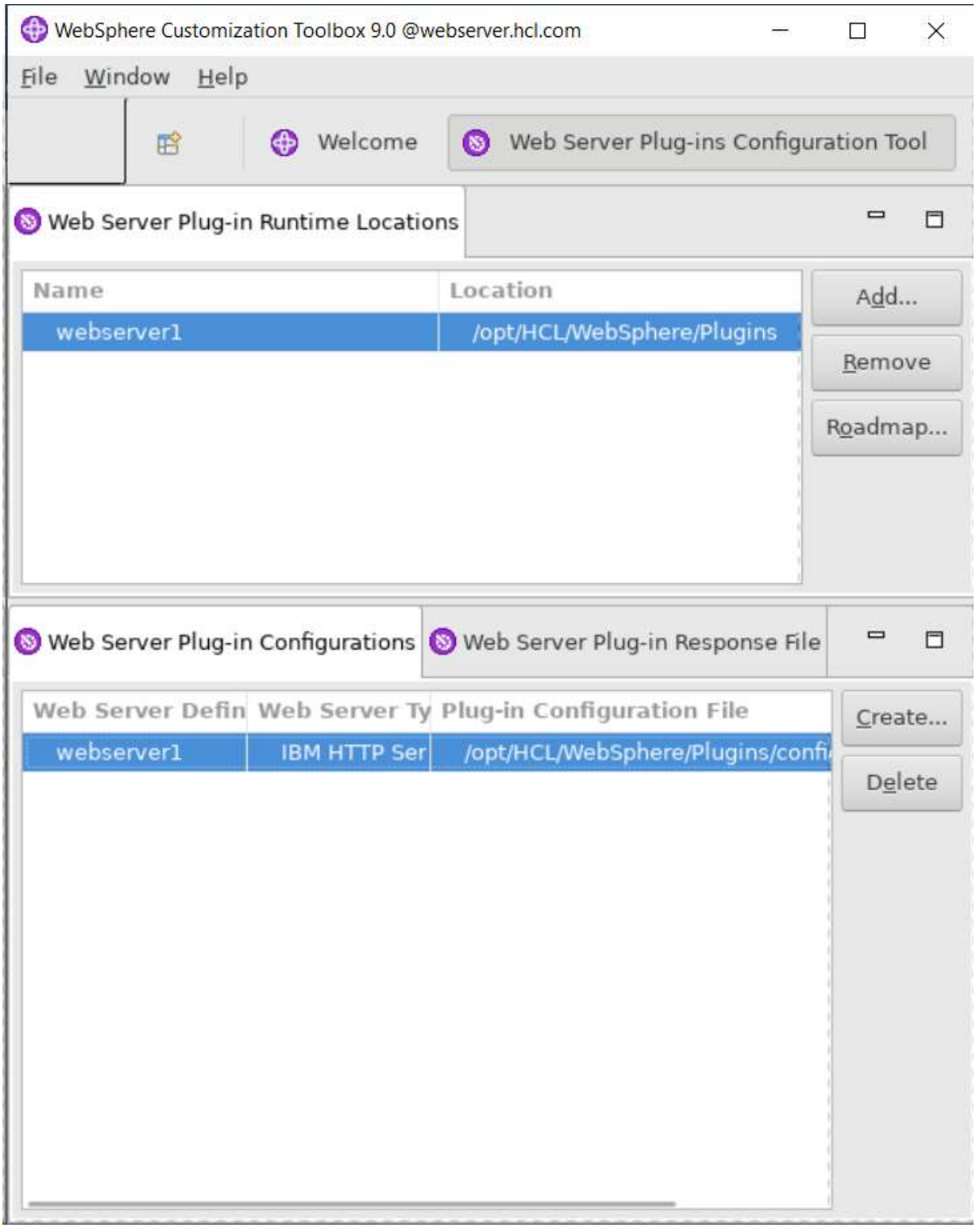
35. Click **Configure** to configure the plug-in.



36. When the process completes, deselect **Launch the plug-in configuration roadmap**. Click **Finish**.



37. Once Configured you will see the result



38. Copy the following file from your IHS web server:

    /opt/HCL/WebSphere/Plugins/bin/configurewebserver1.sh

    To your Deployment Manager server in the following location:

    /opt/HCL/WebSphere/AppServer/bin

39. Switch to the Deployment Manager server. Run the following :

    chmod 777 /opt/HCL/WebSphere/AppServer/bin/configurewebserver1.sh

40. Run the following command from the /opt/HCL/WebSphere/AppServer/bin directory
    ./configurewebserver1.sh -profileName dmgr01

    NOTE: Please ensure Deployment Manager services are running (dmgr) before running the above command

    Output of the command

```
[root@mydmgr bin]# ./configurewebserver1.sh -profileName dmgr01
Using the profile dmgr01
Realm/Cell Name: <default>
Username: WASAdminInLDAP
Password: WASPswdInLDAP
WASX7209I: Connected to process "dmgr" on node dmgrNode01 using SOAP connector;  The type of process is: DeploymentManager
WASX7303I: The following options are passed to the scripting environment and are available as arguments that are stored in the argv variable: "[webse
rver1, IHS, /opt/HCL/HTTPServer, /opt/HCL/HTTPServer/conf/httpd.conf, 80, MAP_ALL, /opt/HCL/WebSphere/Plugins, unmanaged, webserver.hcl.com-node, web
server.hcl.com, linux, 8008, ihsusr, ihsusr]"

Input parameters:

   Web server name            - webserver1
   Web server type            - IHS
   Web server install location - /opt/HCL/HTTPServer
   Web server config location  - /opt/HCL/HTTPServer/conf/httpd.conf
   Web server port            - 80
   Map Applications           - MAP_ALL
   Plugin install location    - /opt/HCL/WebSphere/Plugins
   Web server node type       - unmanaged
   Web server node name       - webserver.hcl.com-node
   Web server host name       - webserver.hcl.com
   Web server operating system - linux
   IHS Admin port             - 8008
   IHS Admin user ID          - ihsusr
   IHS Admin password         - ihsusr
   IHS service name           - ""

Creating the unmanaged node webserver.hcl.com-node .
Unmanged node webserver.hcl.com-node is created.

Creating the web server definition for webserver1 on node webserver.hcl.com-node.
```

    Successful message output

```
Processing the application wps_scheduler.
Get the current target mapping for the application wps_scheduler.
Computed the current target mapping for the application wps_scheduler.
Start updating the target mappings for the application wps_scheduler.
ADMA5075I: Editing of application wps_scheduler started.
ADMA5058I: Application and module versions are validated with versions of deployment targets.
ADMA5005I: The application wps_scheduler is configured in the WebSphere Application Server repository.
ADMA5005I: The application wps_scheduler is configured in the WebSphere Application Server repository.
ADMA5005I: The application wps_scheduler is configured in the WebSphere Application Server repository.
ADMA5005I: The application wps_scheduler is configured in the WebSphere Application Server repository.
ADMA5113I: Activation plan created successfully.
ADMA5011I: The cleanup of the temp directory for application wps_scheduler is complete.
ADMA5076I: Application wps_scheduler edited successfully. The application or its web modules may require a restart when a save is performed.
Target mapping is updated for the application wps_scheduler.

Start saving the configuration.

Configuration save is complete.
```

    NOTE: This activity will take time as this will configure webserver for each portal Application.

41. After the script completes, login into your Deployment Manager via a web browser and navigate to the Servers > Server Types > Web Servers

    Select check box of ‘webserver1’

    Click the box next to your web server name and click ‘Generate Plug-in’

42. You will see a message like the following:

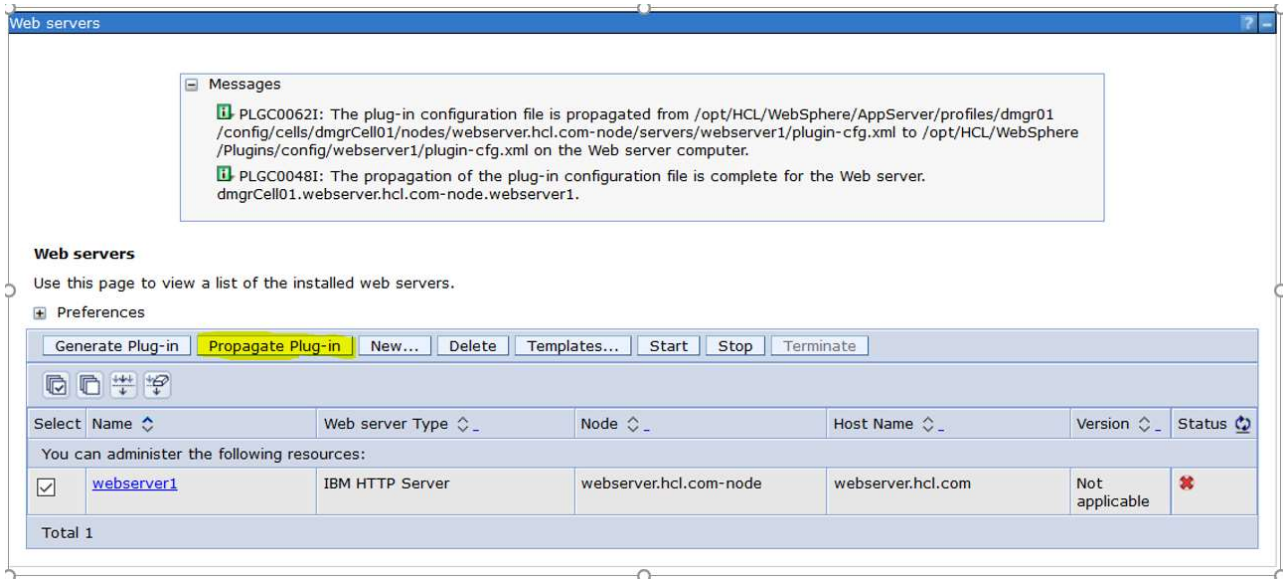
43. Now we need to Propagate the same Plug-in

Select check box of “webserver1”

NOTE: Before starting the propagate, please ensure admin services are running on webserver

```
[root@webserver bin]# ps -ef | grep admin
root      4801     1  0 11:44 ?        00:00:00 /opt/HCL/HTTPServer/bin/httpd -d /opt/HCL/HTTPServer -f conf/admin.conf -k start
root      4802  4801  0 11:44 ?        00:00:00 /opt/HCL/HTTPServer/bin/httpd -d /opt/HCL/HTTPServer -f conf/admin.conf -k start
ihsusr    4803  4801  0 11:44 ?        00:00:00 /opt/HCL/HTTPServer/bin/httpd -d /opt/HCL/HTTPServer -f conf/admin.conf -k start
root      4812  4190  0 11:44 pts/1    00:00:00 grep --color=auto admin
```

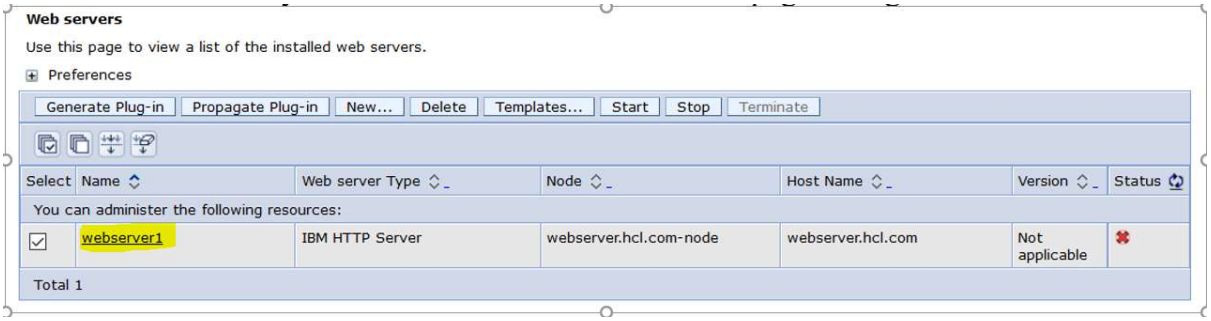
44. Click the box next to your web server name and click ‘Propagate Plug-in’



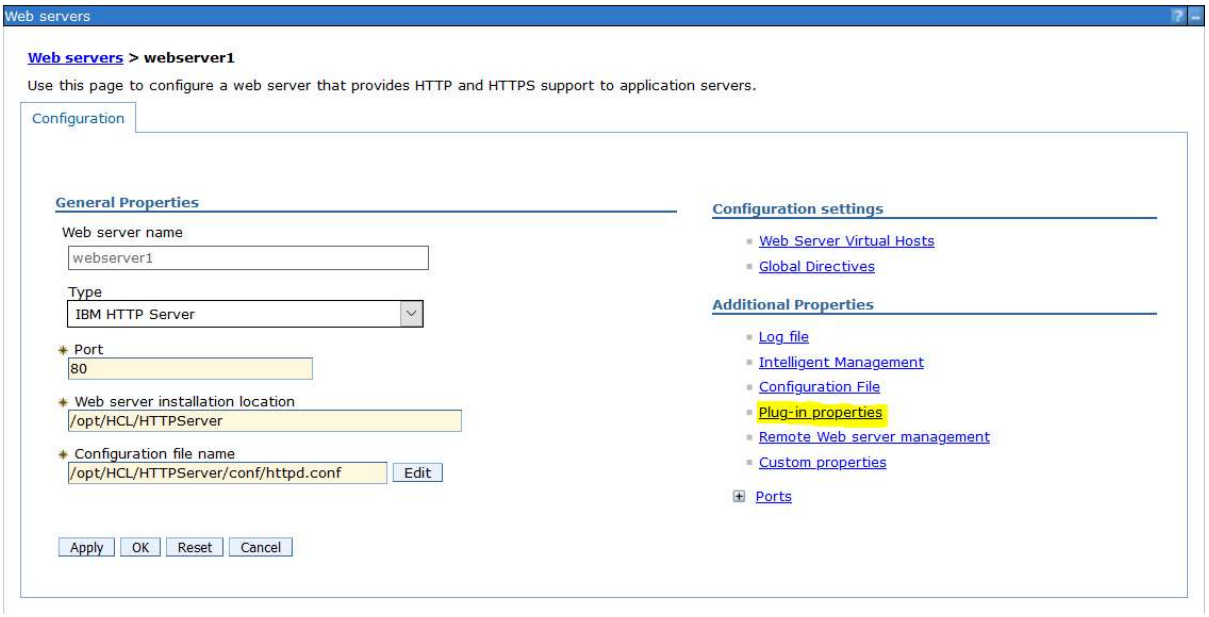
45. Now we need to update the following file as well

plugin-key.kdb
plugin-key.sth

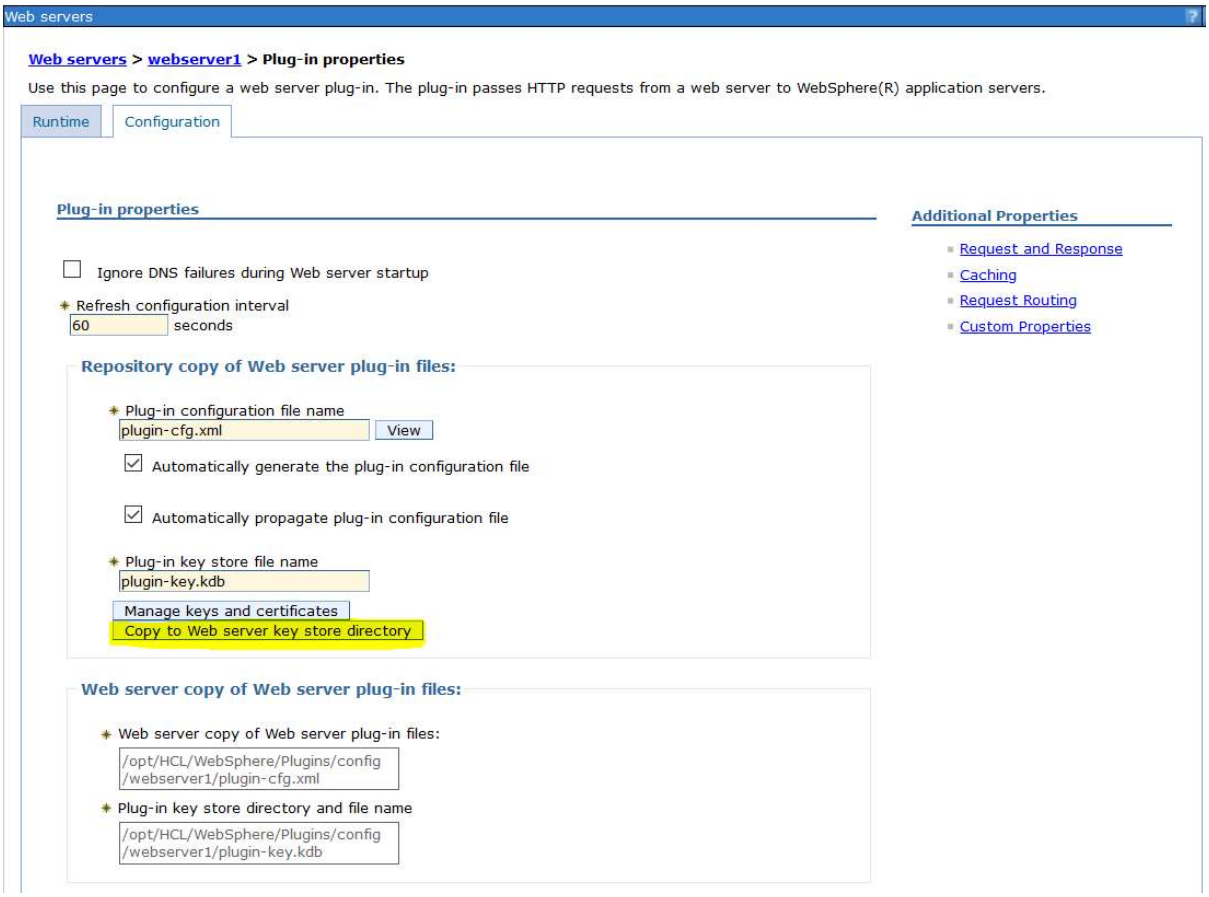
Click on the webserver1



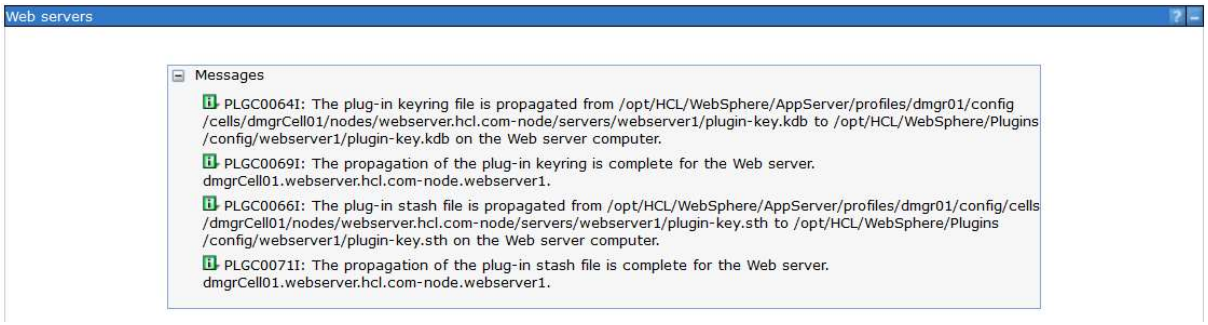
46. Click on Plug-in properties



47. Click on “Copy to Web server key store directory”



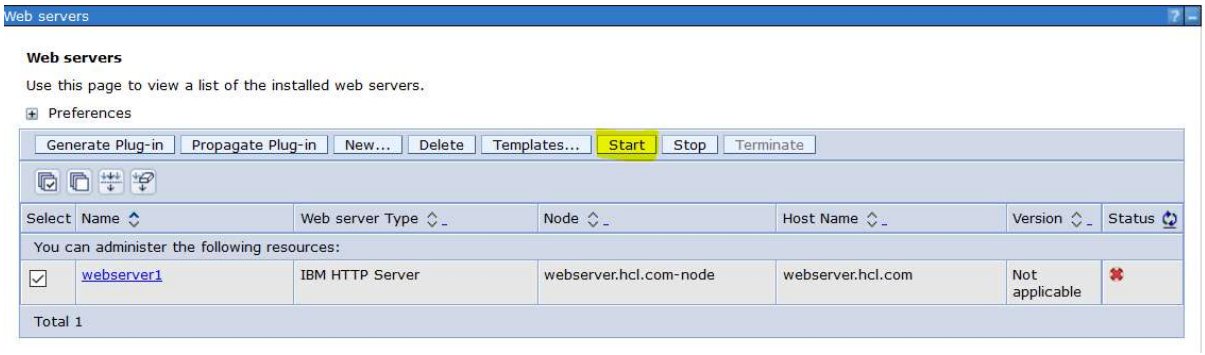
You will see a message similar to the following:

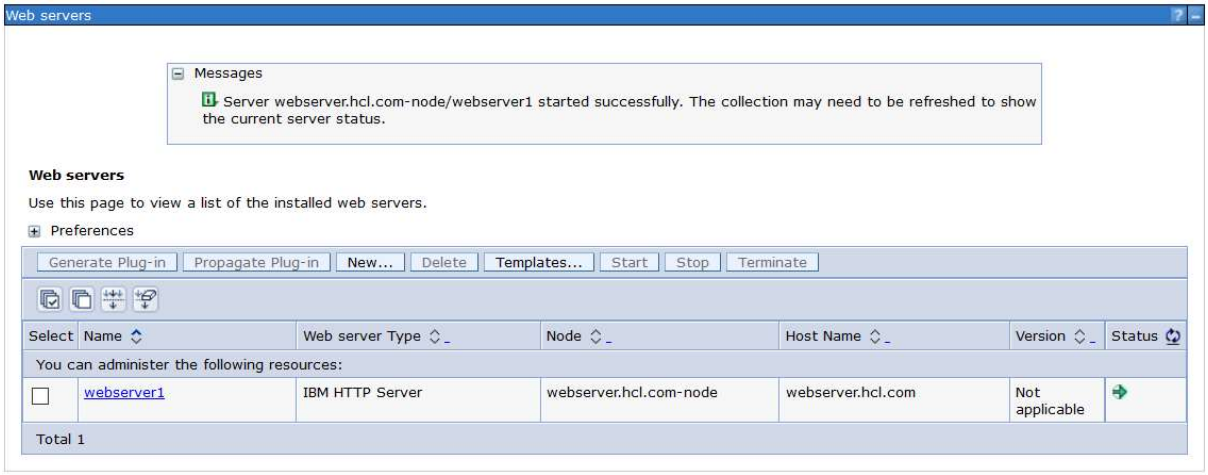


Check on webserver; the following file must be updated in the following directory
/opt/HCL/WebSphere/Plugins/config/webserver1

plugin-key.kdb
plugin-key.sth

48. select the webserver1 and click on **Start**





Check the http services on Webserver machine

```
[root@webserver webserver1]# ps -ef | grep http
root      4801     1  0 11:44 ?        00:00:00 /opt/HCL/HTTPServer/bin/httpd -d /opt/HCL/HTTPServer -f conf/admin.conf -k start
root      4802  4801  0 11:44 ?        00:00:00 /opt/HCL/HTTPServer/bin/httpd -d /opt/HCL/HTTPServer -f conf/admin.conf -k start
ihsusr    4803  4801  0 11:44 ?        00:00:00 /opt/HCL/HTTPServer/bin/httpd -d /opt/HCL/HTTPServer -f conf/admin.conf -k start
ihsusr    4830  4801  0 11:45 ?        00:00:00 /opt/HCL/HTTPServer/bin/httpd -d /opt/HCL/HTTPServer -f conf/admin.conf -k start
root      5112     1  0 12:09 ?        00:00:00 /opt/HCL/HTTPServer/bin/httpd -d /opt/HCL/HTTPServer -k start -f /opt/HCL/HTTPServer/conf/httpd.conf
nobody    5113  5112  0 12:09 ?        00:00:00 /opt/HCL/HTTPServer/bin/httpd -d /opt/HCL/HTTPServer -k start -f /opt/HCL/HTTPServer/conf/httpd.conf
nobody    5114  5112  0 12:09 ?        00:00:00 /opt/HCL/HTTPServer/bin/httpd -d /opt/HCL/HTTPServer -k start -f /opt/HCL/HTTPServer/conf/httpd.conf
nobody    5115  5112  0 12:09 ?        00:00:00 /opt/HCL/HTTPServer/bin/httpd -d /opt/HCL/HTTPServer -k start -f /opt/HCL/HTTPServer/conf/httpd.conf
root      5224  4190  0 12:10 pts/1    00:00:00 grep --color=auto http
```

49. Now Switch to web server. Navigate to the <*httpRoot*>/conf directory. Open the httpd.conf file in a text editor

50. Locate the following line in the httpd.conf file.
    #LoadModule rewrite_module modules/mod_rewrite.so

51. Uncomment the line by removing the pound symbol at the beginning of the line.
    LoadModule rewrite_module modules/mod_rewrite.so

52. Locate the following line in the httpd.conf file.
    # Diagnostic log files, uncomment to enable.

53. Insert the following two lines above this line.

    RewriteEngine on
    RedirectMatch ^/$ /wps/portal/

    Example end result:

```
RewriteEngine on
RedirectMatch ^/$ /wps/portal/

# Diagnostic log files, uncomment to enable.
```

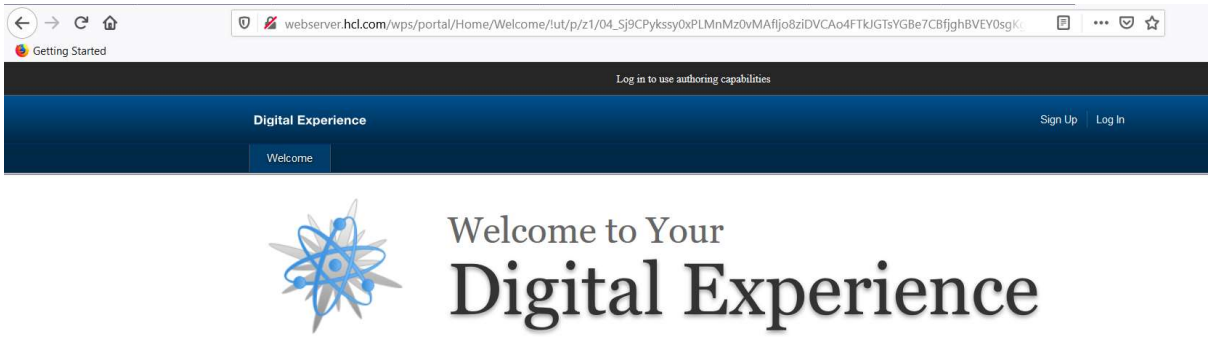
    NOTE: By default accessing your Portal site via http://mywebserver.hcl.com/ will result in an IBM® HTTP Server page being shown instead of your Portal site. This configuration change will ensure accessing http://mywebserver.hcl.com/ will show your Portal site.

54. Save the httpd.conf file.

55. Restart the deployment manager, nodeagents, portal servers, and webserver.

56. Verify that you can access the Portal cluster from the web server address:

    http://mywebserver.hcl.com/



Conclusion

In this guide, you built a two-horizontal node HCL® Portal v9.5 CF17 cluster using an external database and federated LDAP security.

At this point, this guide recommends you upgrade to the latest fixpack of Java, latest fixpack of IBM® WebSphere Application Server, and latest Cumulative Fix (CF) available for HCL® Portal.

At this link you will find the latest Java and WebSphere Application Server fixpacks:

http://www.ibm.com/support/docview.wss?uid=swg27004980

At this link you will find the latest HCL® Portal cumulative fix:

https://support.hcltechsw.com/csm/en?id=kb_article&sysparm_article=KB0013939

Recommended Additional Reading

This guide was intended as a starting point for HCL® Portal administrators building their Portal environments. Additional resources are available to guide you through additional configuration and usage of your Portal environment. Links provided may note different versions of Portal, however, all links are applicable to HCL® Digital Experience (HCL® Portal) v9.0 and v9.5. This guide recommends the following for additional reading:

Building a Proof of Concept Website with Portal:
http://www.redbooks.ibm.com/abstracts/sg248313.html?Open

Portal Administration Guide:
https://www.scribd.com/document/337564239/Portal-85-Admin-Workshop

Portal Performance Tuning Guide:
https://support.hcltechsw.com/csm?id=kb_article&sysparm_article=KB0074411

Portal Security Hardening Guide:
https://support.hcltechsw.com/csm?id=kb_article&sysparm_article=KB0074054

Developing Themes for HCL® Portal:
https://help.hcltechsw.com/digital-experience/9.5/dev-theme/themeopt_themes.html

Creating Pages and Adding Content with Managed Pages:
https://help.hcltechsw.com/digital-experience/8.5/panel_help/h_mp_create_pages.html

HCL® Digital Experience - YouTube videos:
https://www.youtube.com/results?search_query=HCL+Digtial+Experience

HCL® Digital Experience Product Documentation:
https://help.hcltechsw.com/digital-experience/index.html

Appendix A1 - Enabling SSL on the Web Server

Introduction

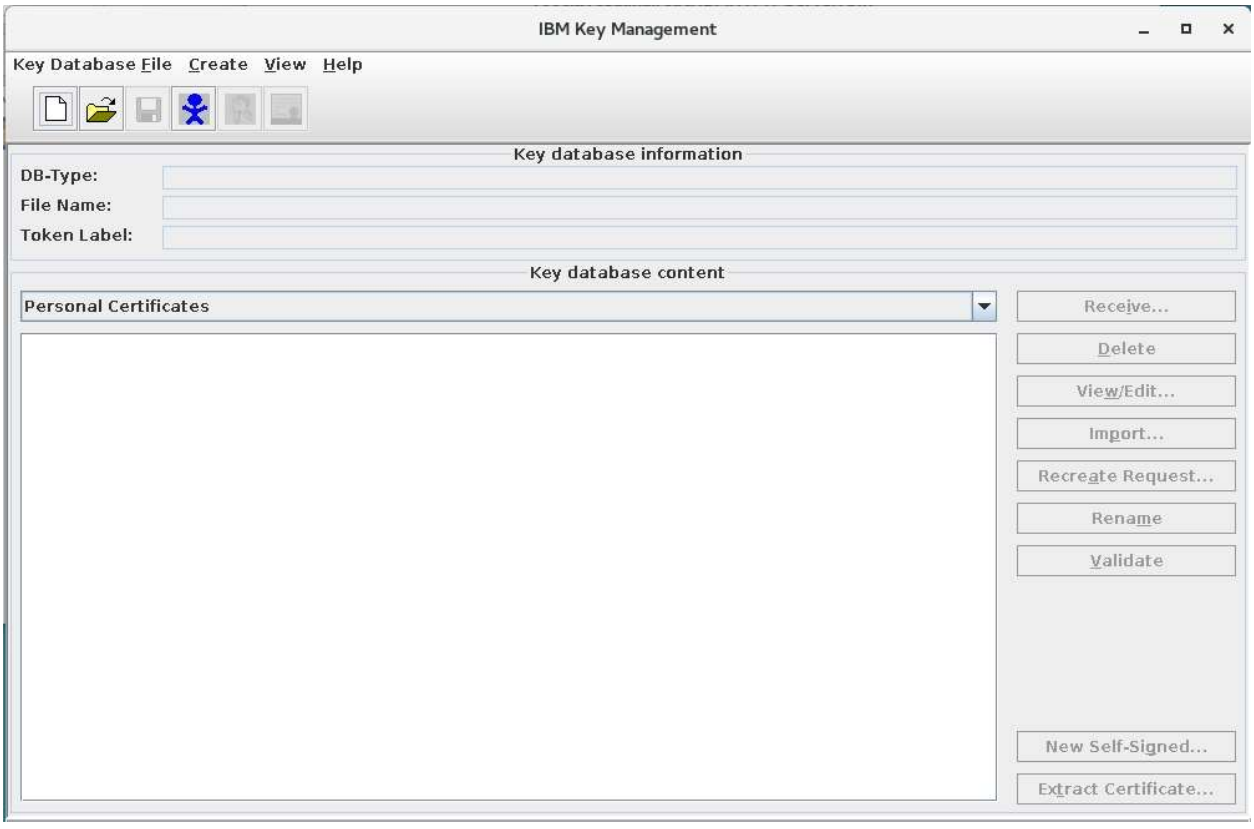
This appendix will guide you through enabling SSL on your IBM® HTTP Server. This appendix also provides instructions for how to configure IBM® HTTP Server with logic that will ensure any visitors to your Portal site will always browse over a secure https:// link and never over an unsecure http:// link. This appendix also provides details on how to enable SSL communications between your Portal servers and web server. Finally, this appendix will provide an example of how to allow visitors to your Portal site to automatically be redirected to the /wps/portal portion of your Portal server.

NOTE: The authors of this guide STRONLGY recommend SSL be enabled on your web server for all Portal sites. However, there are valid arguments to be made where SSL should not be enabled. Hence, the instructions for enabling SSL on the web server are in an appendix of this guide rather than being contained within Chapter 8 of the guide.

1. Navigate to the <HTTPServer>/bin/ikeyman directory of your web server.
2. Launch the IBM® Key Management tool via executing the ikeyman command

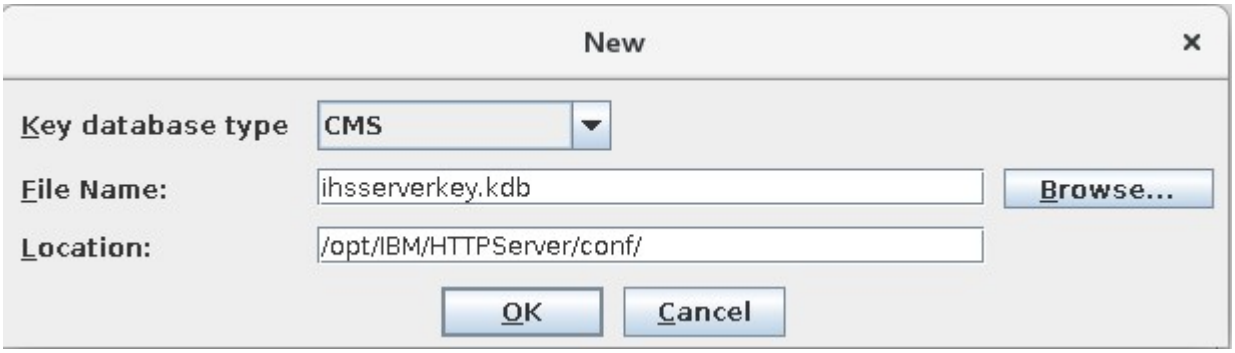
```
[root@          bin]# cd /opt/IBM/HTTPServer/bin/
[root@          bin]# ./ikeyman
```

3. You will see the following screen:



4. Click **Key Database File > New**

5. Select **CMS** for Key Database type. Provide a File Name and Location. Click **OK.**



6. Provide a password for the key file. Retype the same password in the Confirm Password field. Click the checkbox to **Stash password to a file**. Click **OK**.

NOTE: This guide uses a self-signed SSL certificate for demonstration purposes. If you are installing a self-signed SSL certificate, proceed with executing steps #7 - #9 of this Appendix.

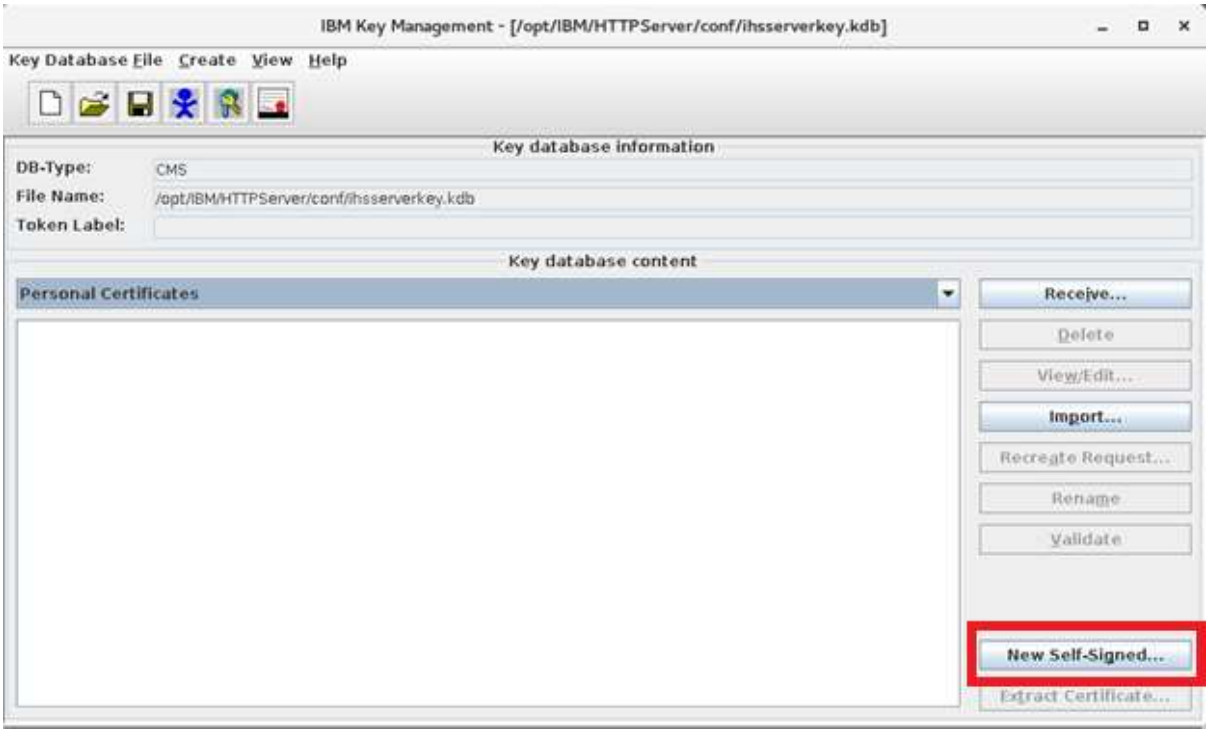
However, many Portal sites will use an SSL certificate issued by their company's Certificate Authority, or, an SSL certificate issued by a trusted third-party Certificate Authority such as Comodo, Symantec, GoDaddy, etc. If you require a certificate issued by your company or by a trusted third-party, see the following document:

https://www.ibm.com/support/docview.wss?uid=swg21006430

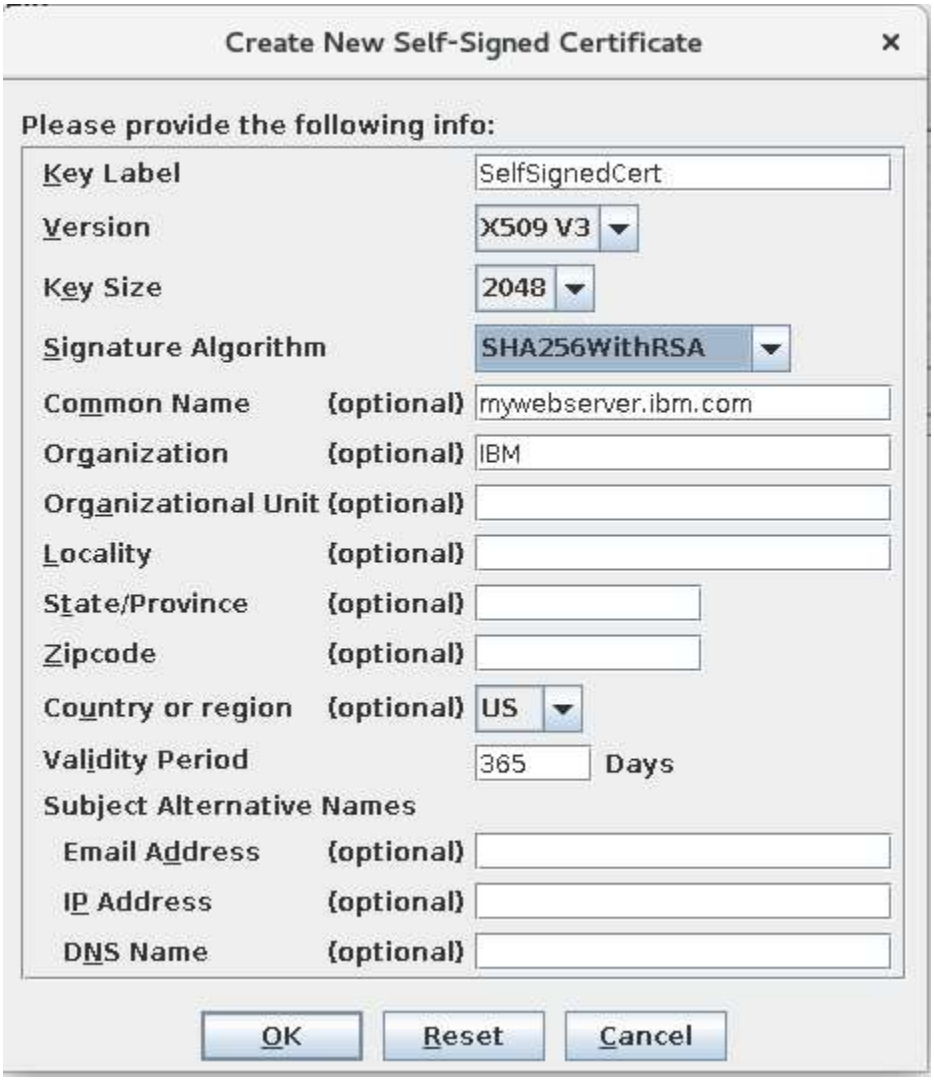
Execute the steps in the sections titled:
How do I create a new "Certificate Request" to send to a CA (for example, Verisign)?
How do I receive the Certificate into the Key Database File (kdb) file after getting it back from the CA?

And skip steps #7 - #9 of this Appendix. Resume on step #10.

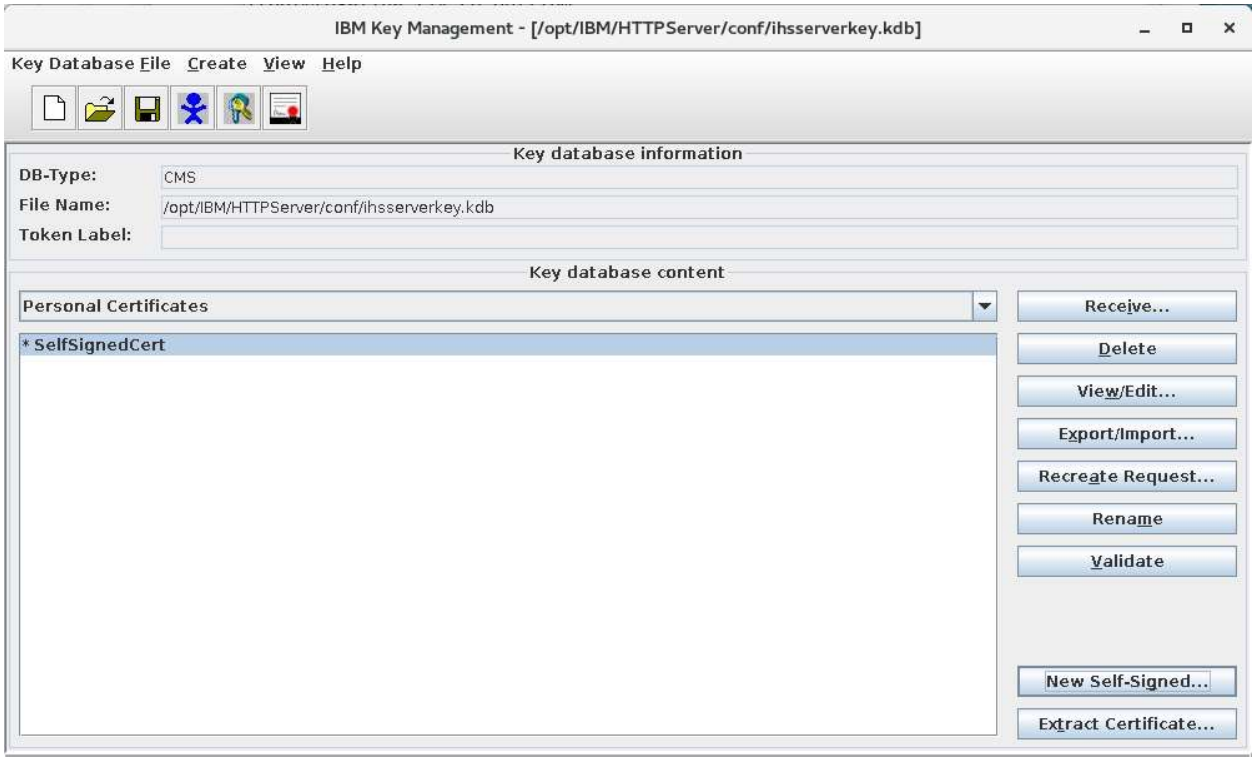
7. Click on **New Self-Signed…** in the lower right of the window.



8. Fill in the **Key Label**, **Key Size**, **Signature Algorithm, Common Name, and Organization fields.** For the Common Name field, use the hostname of the IBM® HTTP Server, mywebserver.ibm.com for this guide. Click **OK.**



9. You will see the following screen.



10. Click **Key Database File > Exit** to close the IBM® Key Management tool.

11. Navigate to the <HTTPServer_root>/conf directory. For this guide: **/opt/IBM/HTTPServer/conf**.

12. Open the httpd.conf file in a text editor.

13. Locate the line in the httpd.conf file which begins with **Example SSL section**

```
# Example SSL configuration
# To enable this support:
#   1) Create a key database with ikeyman or bin/gskcapicmd
#   2) Update the KeyFile directive below to point to that key database
#   3) Uncomment the directives up through the end of the example
#
#LoadModule ibm_ssl_module modules/mod_ibm_ssl.so
#Listen 443
#SSLCheckCertificateExpiration 30
#<VirtualHost *:443>
 #SSLEnable
 #Header always set Strict-Transport-Security "max-age=31536000; includeSubDomains; preload"
#</VirtualHost>
#KeyFile /opt/IBM/HTTPServer/conf/ihsserverkey.kdb
#SSLDisable
# End of example SSL configuration
```

14. Update this section with the following text

```
LoadModule ibm_ssl_module modules/mod_ibm_ssl.so
Listen 443
SSLCheckCertificateExpiration 30
<VirtualHost *:443>
      SSLEnable
      SSLClientAuth None
      Header always set Strict-Transport-Security "max-age=31536000; includeSubDomains; preload"
</VirtualHost>
KeyFile /opt/IBM/HTTPServer/conf/ihsserverkey.kdb
SSLDisable
```

Example end result for this guide:

```
# Example SSL configuration
# To enable this support:
#   1) Create a key database with ikeyman or bin/gskcapicmd
#   2) Update the KeyFile directive below to point to that key database
#   3) Uncomment the directives up through the end of the example
#
LoadModule ibm_ssl_module modules/mod_ibm_ssl.so
Listen 443
SSLCheckCertificateExpiration 30
<VirtualHost *:443>
 SSLEnable
 SSLClientAuth None
 Header always set Strict-Transport-Security "max-age=31536000; includeSubDomains; preload"
</VirtualHost>
KeyFile /opt/IBM/HTTPServer/conf/ihsserverkey.kdb
SSLDisable
# End of example SSL configuration
```

15. In the httpd.conf file - locate the following two lines rule you implemented in Chapter 8.
    RewriteEngine on
    RedirectMatch ^/$ /wps/portal/

16. Update the lines to match the following text:
    RewriteEngine on
    RewriteCond %{SERVER_PORT} =80
    RewriteRule ^(.*) https://%{SERVER_NAME}%{REQUEST_URI} [R,L]
    RedirectMatch ^/$ /wps/portal/

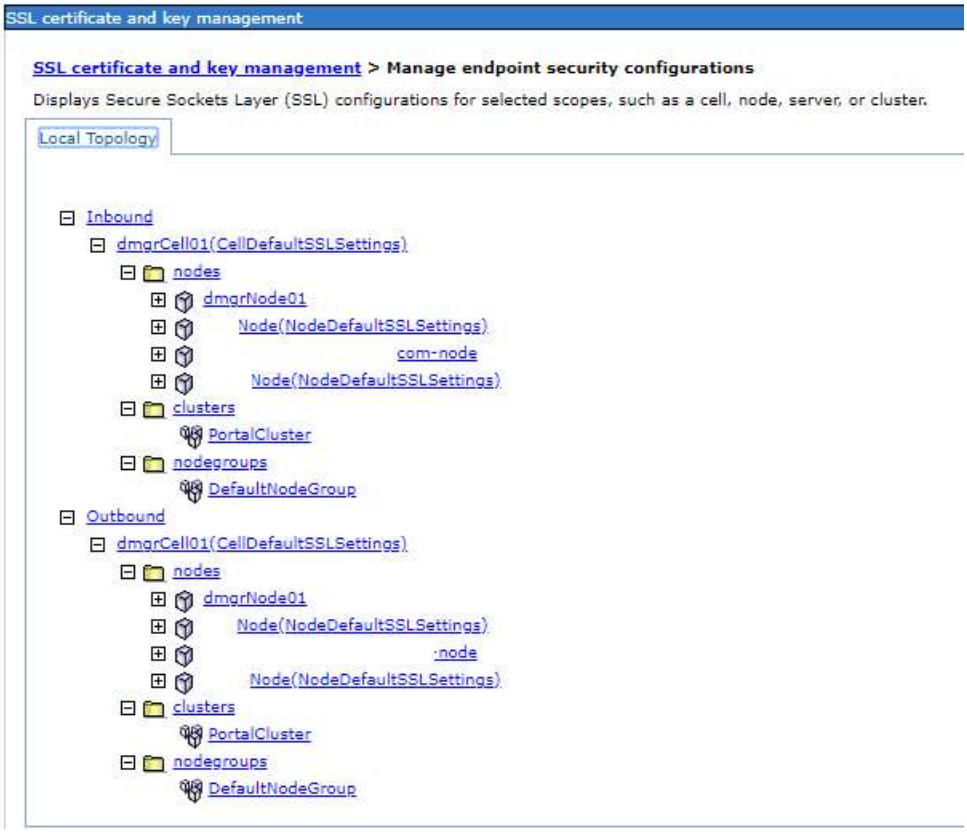
NOTE: For this guide, the end result of the changes in the httpd.conf file looking like the following.

```
LoadModule ibm_ssl_module modules/mod_ibm_ssl.so
Listen 443
SSLCheckCertificateExpiration 30
<VirtualHost *:443>
 SSLEnable
 SSLClientAuth None
 Header always set Strict-Transport-Security "max-age=31536000; includeSubDomains; preload"
</VirtualHost>
KeyFile /opt/IBM/HTTPServer/conf/ihsserverkey.kdb
SSLDisable
# End of example SSL configuration

RewriteEngine on
RewriteCond %{SERVER_PORT} =80
RewriteRule ^(.*) https://%{SERVER_NAME}%{REQUEST_URI} [R,L]
RedirectMatch ^/$ /wps/portal/

# Diagnostic log files, uncomment to enable.
```

17. Save and close the httpd.conf file.

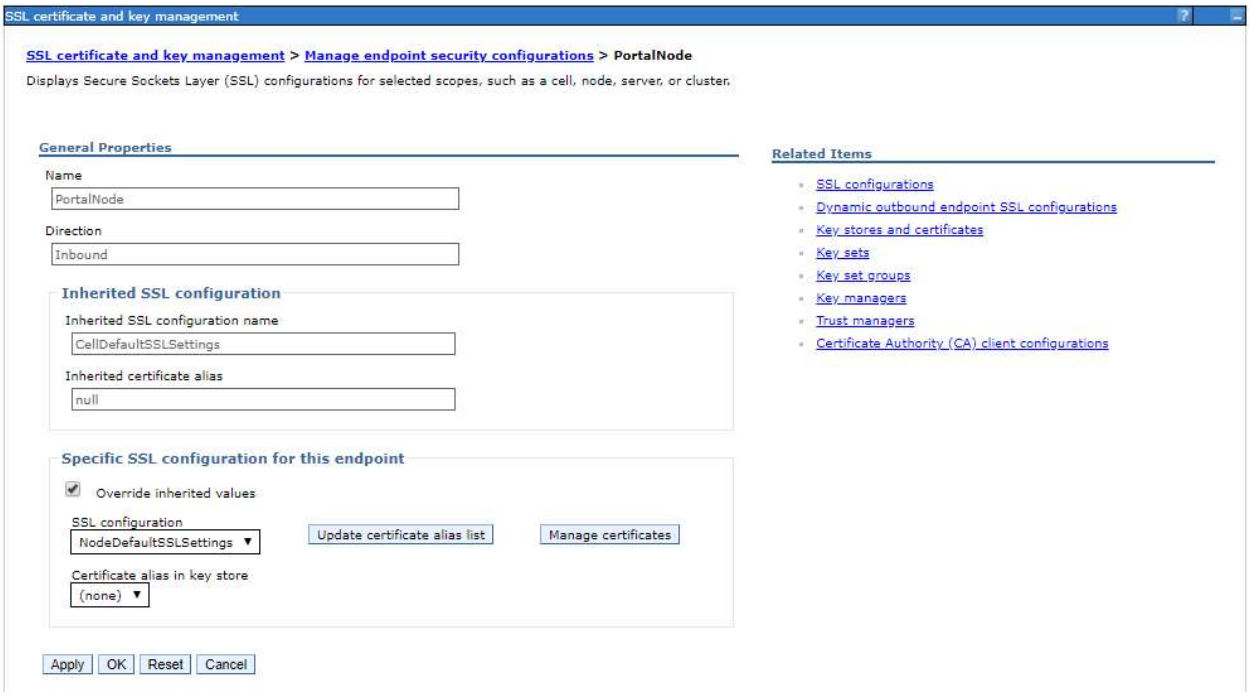
18. Login to the Deployment Manager via a web browser.

19. Navigate to **Security > SSL certificate and key management > Manage endpoint security configurations.** You will see a screen similar to the following:

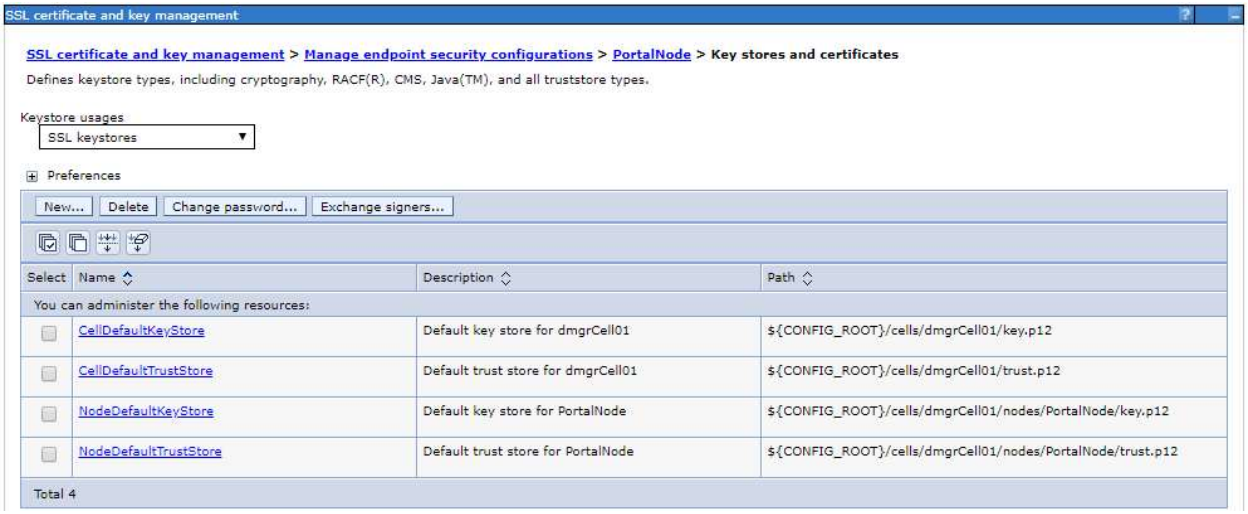


20. Under the heading Inbound, you will have four total entries representing your Deployment Manager node, primary portal node, additional horizontal portal node, and web server node. Click on **NodeDefaultSSLSettings** for **your primary Portal node**.

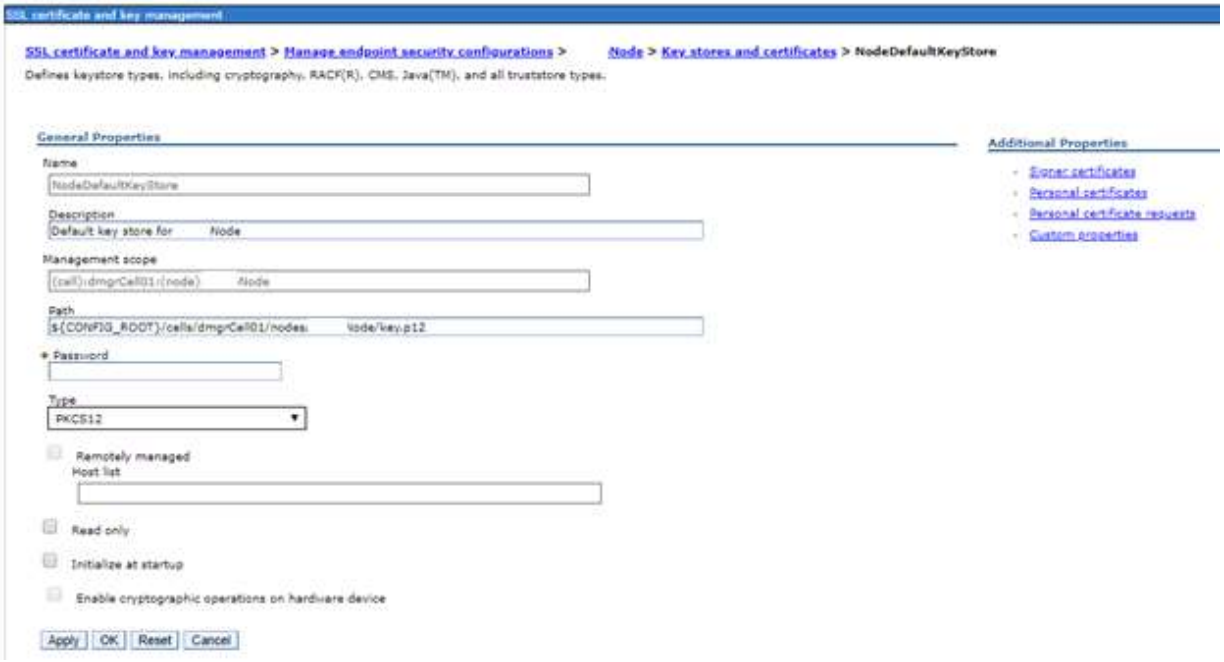
21. You will see the following screen:



22. Click on **Key stores and certificates** on the right side. You will see the following screen:



23. Click on **NodeDefaultKeyStore**. You will see the following screen.



24. Click on **Personal certificates** on the right-hand side. You will see the following screen.

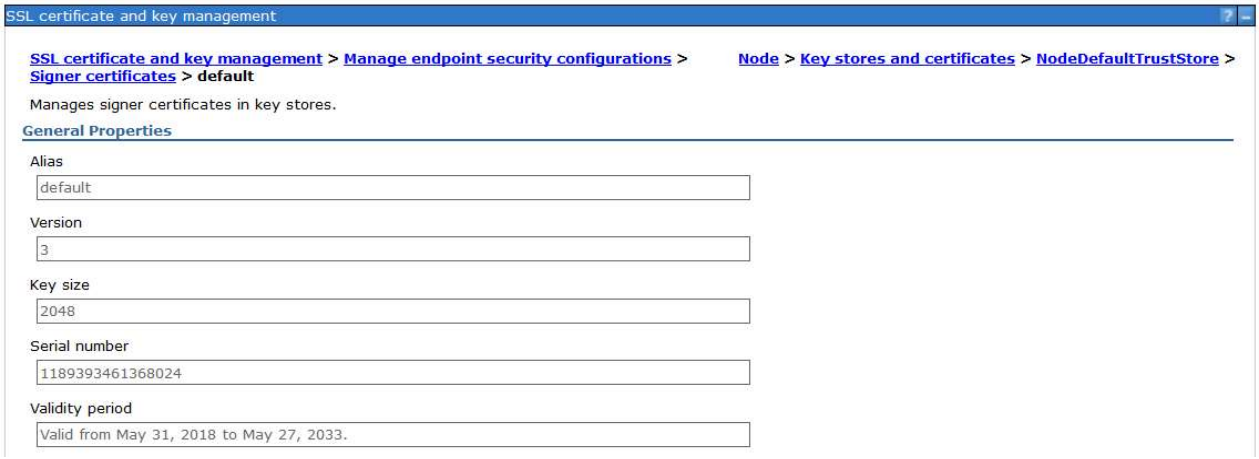
25. The first entry on this screen is a personal certificate. The second entry on this screen is a signer certificate. Record the serial number of the signer certificate - **1189393461368024** for this guide.

26. At the top of the page click on **Key stores and certificates.** You will screen the following screen.

27. Click on **NodeDefaultTrustStore.** You will see the following screen.

28. Click on **Signer certificates** on the right side. You will see the following screen.

29. Click on the alias named **default**. You will see the following screen.



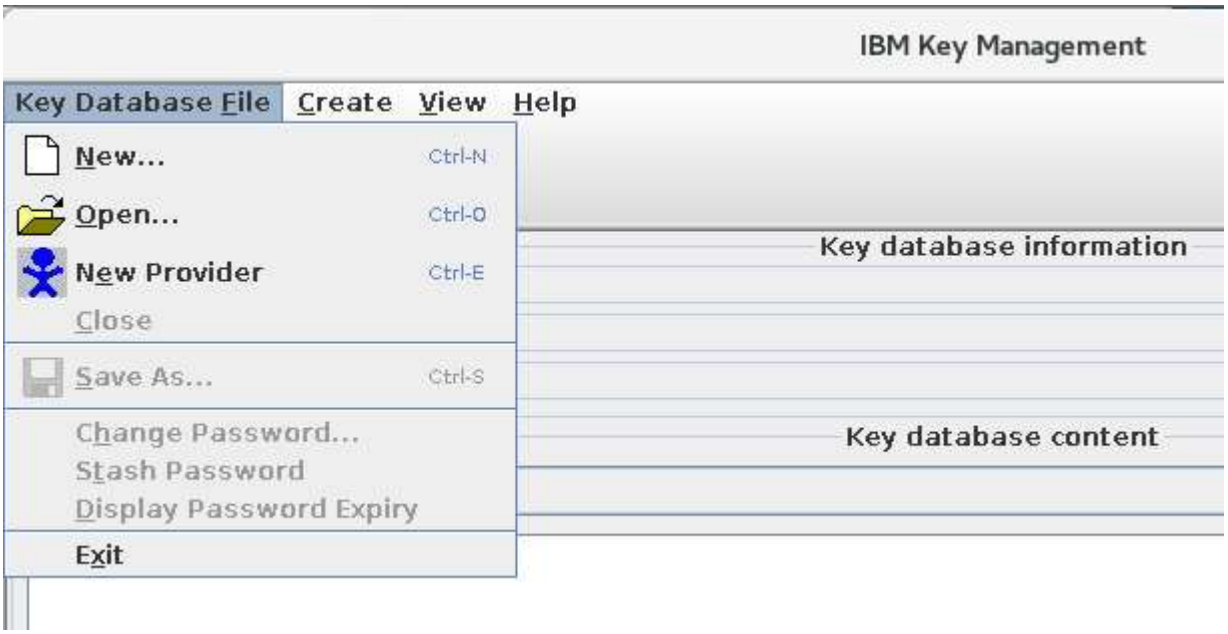
30. Validate the serial number that appears on this screen matches the serial number you previously recorded. If it does not, go back to the **NodeDefaultTrustStore** and choose a different certificate alias name. Inspect each certificate alias until you identify the correct one with the matching serial number. For this guide the alias **default** contained a matching serial number.

31. Click on the **NodeDefaultTrustStore** at the top of the page. Click the checkbox next to the alias you identified with the matching serial number. **default** alias for this guide. Click **Extract**.

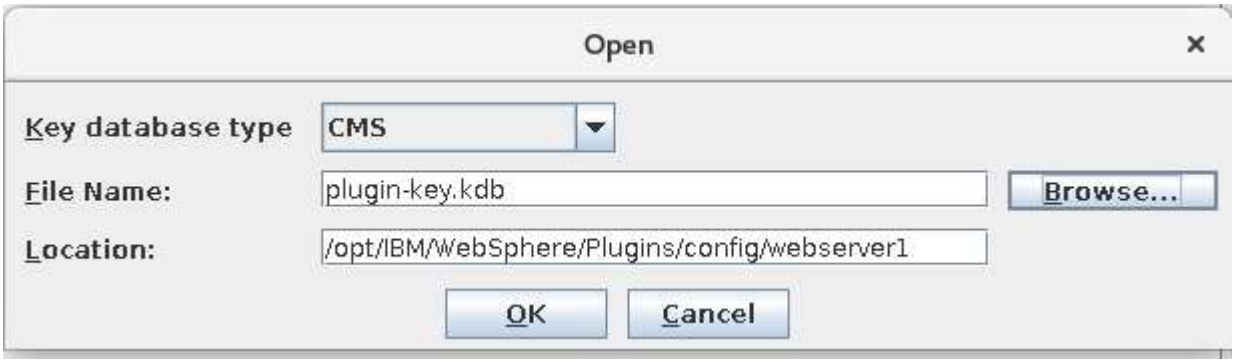
32. Enter a temporary path and filename. Click OK. This will create a file on the Deployment Manager. Copy this file to a temporary location on your IHS server.

33. Navigate to the <*httpRoot*>/bin/ directory of your web server. Launch the IBM® Key Management tool via executing the ikeyman command.

34. Click on **Key Database File > Open…**

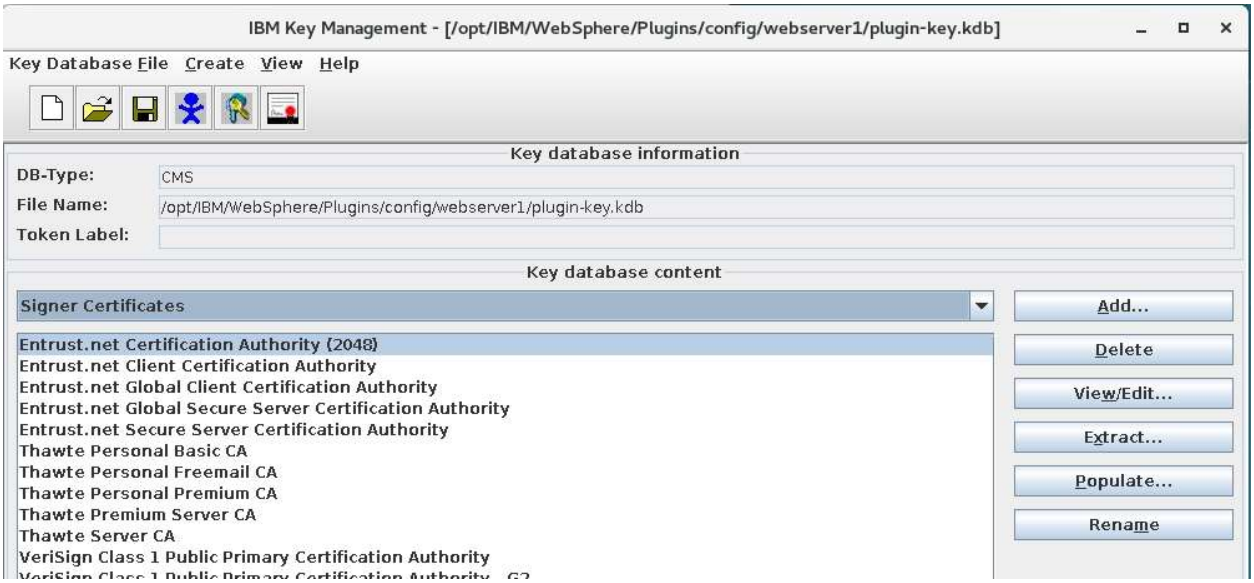


35. Click **Browse…** Navigate to the <*pluginRoot*>/Plugins/config/webserver1 directory and select the plugin-key.kdb file.



36. Click **OK.** You will be prompted for the password of the plugin-key.kdb file. The default password is **WebAS**. Enter the password and click **OK.**

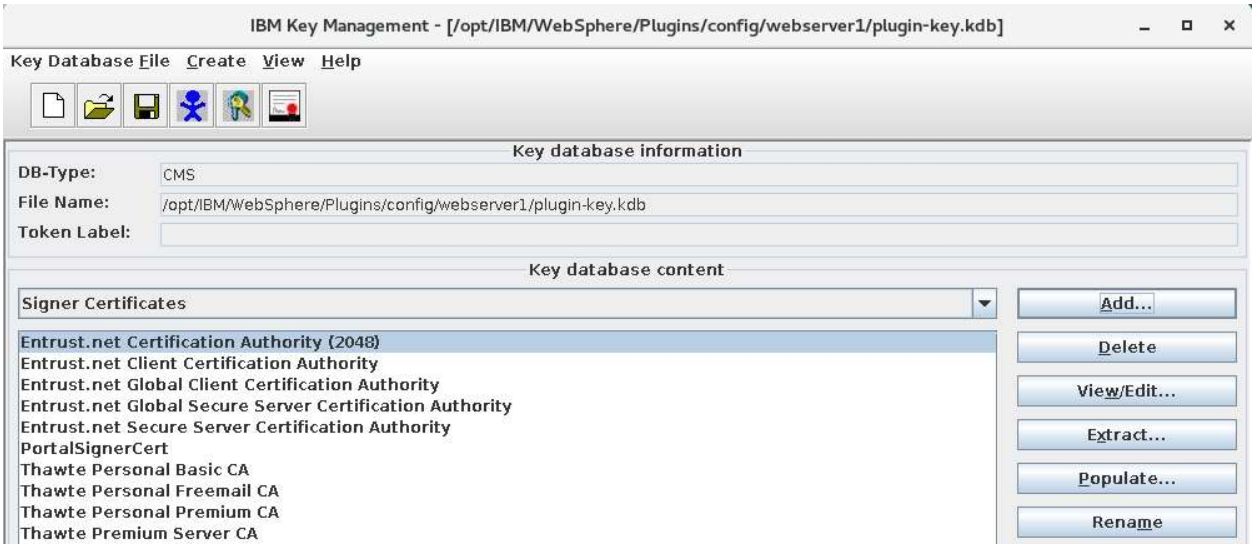
37. Click the drop down box to change from Personal Certificates and select **Signer Certificates.**



38. Click **Add…** Fill in the File Name and location where you copied the extracted certificate file nodeRootSigner.arm on the websever. Click **OK**.

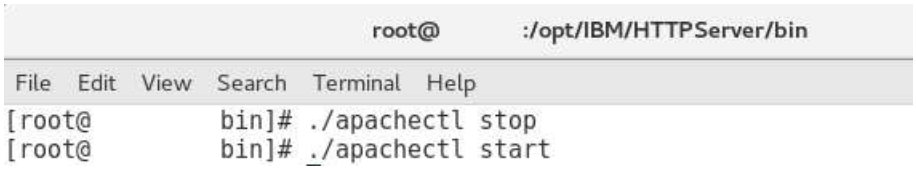
39. Enter a value to label the certificate. This guide recommends **PortalSignerCert.** Click **OK**.

40. You will now see your **PortalSignerCert** in the list of Signed Certificates.



41. Close the ikeyman tool. You will be in the <*httpRoot*>/bin directory.

42. Restart the web server by executing the following two commands:
    ./apachectl stop
    ./apachectl start



43. Validate you are able to access your webserver over https in a web browser:
https://mywebserver.ibm.com/

44. Validate you are able to access your webserver over http in a web browser.
http://mywebserver.ibm.com/

NOTE: The end result in the web browser should be a secure https:// url.

45. SSL is now successfully enabled on your web server. Any visitors to your Portal site who attempt to access over http will automatically be redirected to a secure https:// link.

Appendix A2- Remote Search Installation and Configuration.

HCL® Digital Experience : https://hclsw.co/dx-page This video demonstrates how to set up a remote search server with an HCL® Portal 9.5 CF18 cluster.

Please check below mentioned YouTube video for this topic.

https://www.youtube.com/watch?v=WldILSgwvBI

Appendix A3- Resolving Duplicate Users and Groups

Introduction

If you have been directed to this Appendix by a chapter in the guide, you are in a configuration where you have one or more administration users or groups in your Portal configuration that have the same names as one or more administration users or groups in your LDAP configuration. If you attempt to add your LDAP to the Portal configuration duplicate user names and/or duplicate group names will occur and prevent the Portal server from starting or functioning properly.

In this appendix, you will update the Deployment Manager administration user name, Portal administration user name, and Portal administration group to be different values from those in your LDAP. This change will ensure duplicate user names and/or duplicate group names are not present when you add your LDAP server to the Portal cluster configuration. No changes to your LDAP will be required - all changes will occur on the Deployment Manager.

NOTE: This appendix assumes you have not yet configured an LDAP and you are able to login to your Deployment Manager successfully prior to executing the steps. If you have already added an LDAP and you are unable to login to your Deployment Manager, do not execute the steps in this Appendix. Instead, see the following link for correcting that scenario: https://www.ibm.com/developerworks/community/blogs/PortalL2Thoughts/entry/Fixing_a_common_issue_Duplicate_adminuser_admingroup_names_in_Portal?lang=en

Technical Background

When Portal is installed, you are asked to specify an administration username. This username, and a group named “wpsadmins” are used to initially configure the Deployment Manager and Portal server prior to an LDAP being added.

The full distinguished name of the user and group is as follows:
uid=PortalAdminID,o=defaultWIMFileBasedRealm
cn=wpsadmins,o=defaultWIMFileBasedRealm

The LDAP contains a user and group with similar names, e.g.:

uid=PortalAdminID,cn=users,dc=ibm,dc=com

cn=wpsadmins,cn=groups,dc=ibm,dc=com

When an LDAP is added to the configuration, we now have two users named "wpadmin" when we try to login. HCL® Portal / WebSphere Application Server does not - by design - support and does not attempt to resolve duplicate user names on login with a federated repositories configuration.

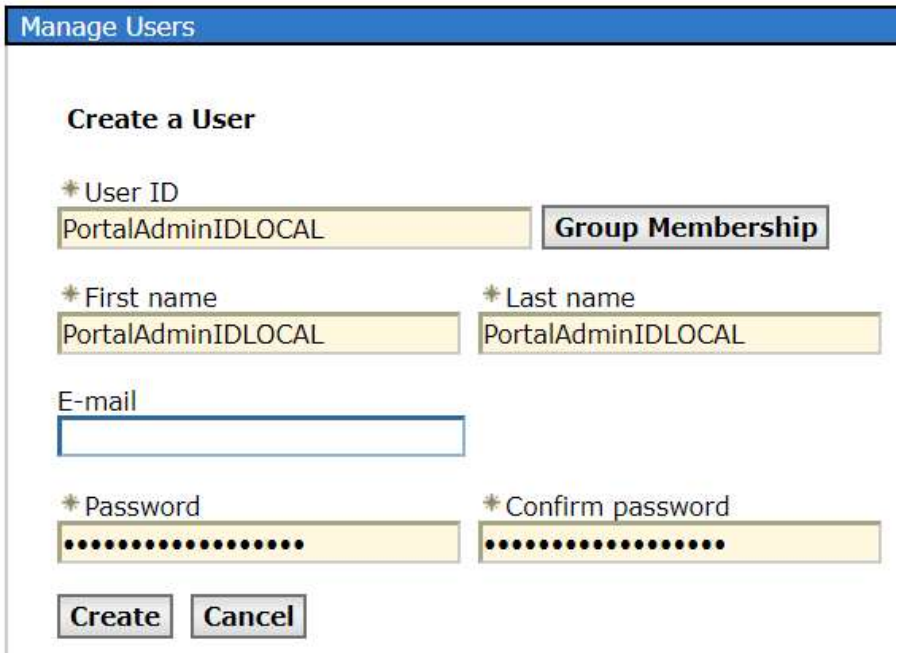
Removing the Duplicates

1. Login to the Deployment Manager with the *dmgrAdminID*.
   https://mydmgr.ibm.com:9043/ibm/console

2. On the left-hand side of the screen, Click **Users and Groups > Manage Users**

3. Click **Create…**

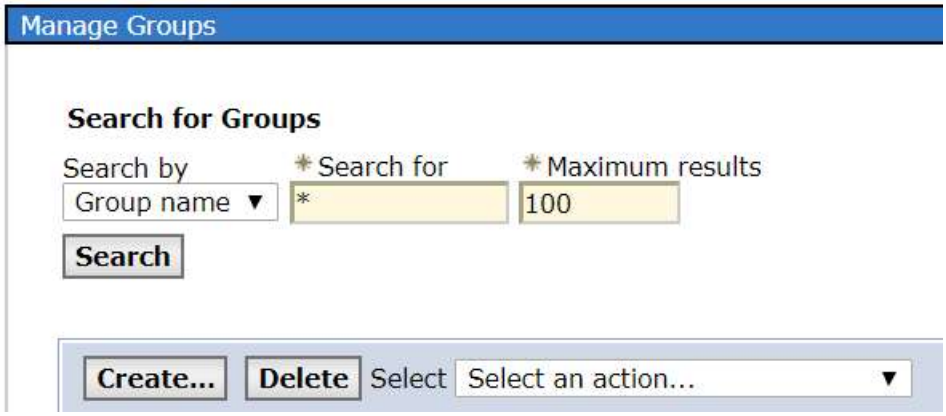
4. Fill in the values on this screen and click **Create**.



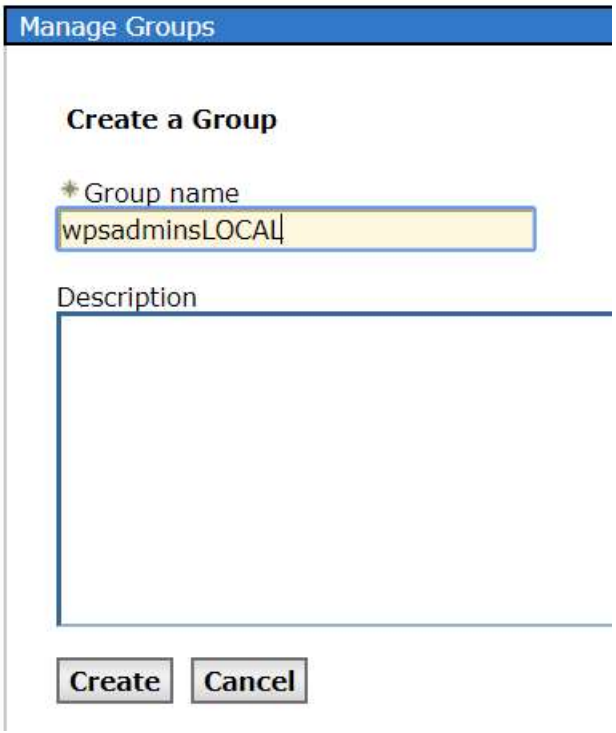
NOTE: The userID you specify will be temporary and will be replaced by your *WASAdminInLDAP* once LDAP configuration is completed. This guide recommends appending the word LOCAL to the end of the userID to distinguish the userID as local to the Portal server. This guide's authors have found most enterprise LDAPs do not contain userIDs with the word LOCAL appended at the end of the userID. Ensure the final result does not conflict with an existing userID in your LDAP.

5. On the left-hand side of the screen, Click **Users and Groups > Manage Groups**

6. Click **Create…**

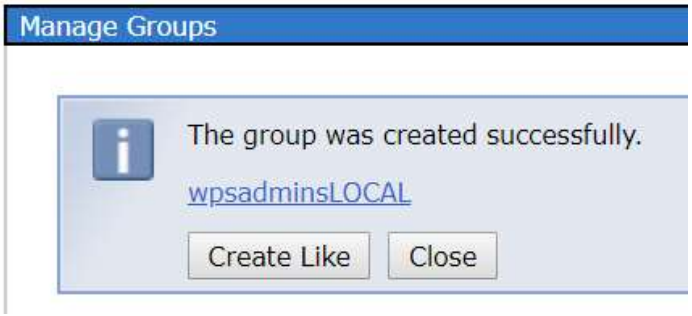


7. Fill in the value on this screen and click **Create**.



NOTE: Similar to the userID, the group you specify will be temporary and will be replaced once LDAP configuration is completed. This guide recommends appending the word LOCAL to the end of the group name to distinguish the group as local to the Portal server. This guide's authors have found most enterprise LDAPs do not contain groups with the word LOCAL appended at the end of the group name. Ensure the final result does not conflict with an existing group name in your LDAP.

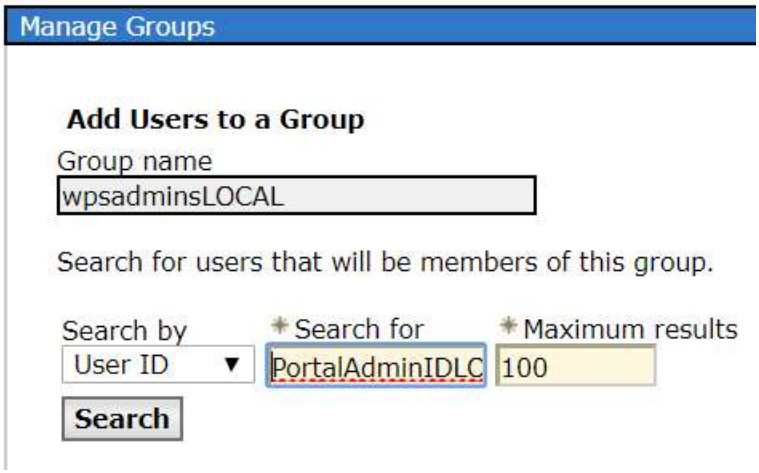
8. Click the **Blue Link** that appears for your group name.



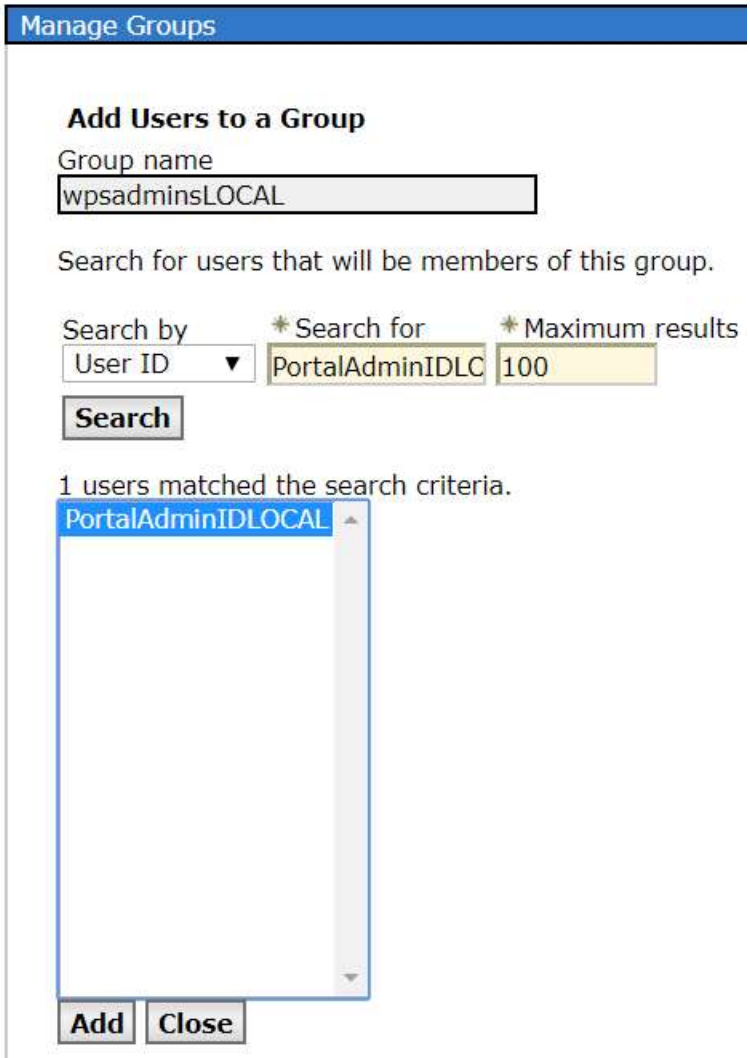
9. Click the blue link for **Members**

10. Click **Add Users…**

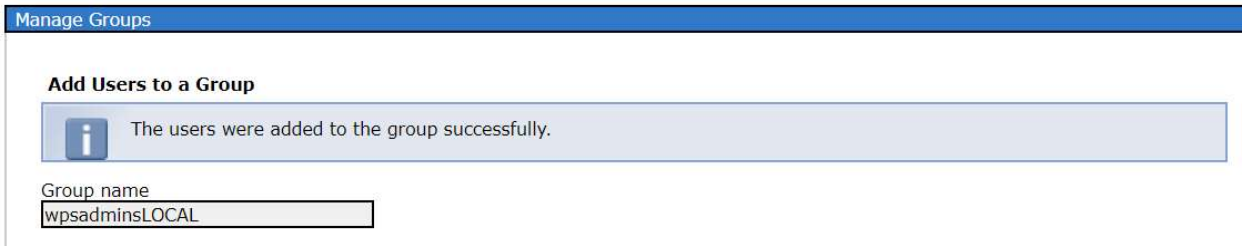
11. Update the Search text to your newly created userID. This guide uses PortalAdminIDLOCAL. Click **Search.**



12. A single result should be returned. Click the result so it is highlighted. Click A**dd.**



13. You will see:



14. Logout of the Deployment Manager.

15. Open a terminal session / command prompt to the primary node of your Portal server. Navigate to the <wp_profile>/ConfigEngine directory.

16. Execute the following command:

    ./ConfigEngine.sh wp-change-was-admin-user
    -DWasPassword= dmgrAdminPswd
    -DnewAdminId=uid=PortalAdminIDLOCAL,o=defaultWIMFileBasedRealm
    -DnewAdminPw=newpassword

```
[root@      ~]# cd /opt/IBM/WebSphere/wp_profile/ConfigEngine/
[root@      ConfigEngine]# ./ConfigEngine.sh wp-change-was-admin-user -DWasPassw
ord=dmgrAdminPswd -DnewAdminId=uid=PortalAdminIDLOCAL,o=defaultWIMFileBasedRealm
 -DnewAdminPw=newpassword
```

    Substitute the values provided with the new userID and password you created in previous steps.

NOTE: HCL Portal stores the WebSphere Application Server administration ID in multiple areas of the configuration. Changing the ID in the Deployment Manager Console via Security > Global Security will not update the configuration in all locations HCL® Portal stores the ID. Ensure you use the configuration task to update the ID.

17. Open a terminal session / command prompt to the primary node of your Deployment Manager. Navigate to the <dmgr_profile>/bin directory.

18. Stop the Deployment Manager via the stopManager.sh command.

```
[root@          ~]# cd /opt/IBM/WebSphere/AppServer/profiles/dmgr01/bin
[root@          bin]# ./stopManager.sh -user dmgrAdminID -password dmgrAdminPswd
```

NOTE: The values currently are still those of the original administration ID and new password. The next command to start the Deployment Manager will pick up the new administration ID and begin using it. All subsequent commands will use the new administration ID and new password.

19. Start the Deployment Manager via the startManager.sh command.

```
[root@          ~]# cd /opt/IBM/WebSphere/AppServer/profiles/dmgr01/bin
[root@          bin]# ./startManager.sh
```

20. Login to the Deployment Manager with your new user ID you created.

    https://mydmgr.ibm.com:9043/ibm/console

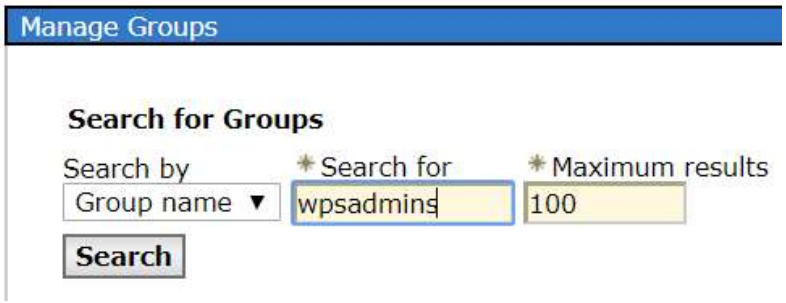
21. On the left-hand side of the screen, Click **Users and Groups > Manage Users**

22. Enter the value *dmgrAdminID* and Click **Search.**

23. Click the checkbox next to the *dmgrAdminID* and Click **Delete**. Click **Delete** on the subsequent screen to confirm the action.

24. On the left-hand side of the screen, Click **Users and Groups > Manage Groups**.

25. Enter the value wpsadmins and Click **Search.**



26. Click the checkbox next to the wpsadmins group and Click **Delete**. Click **Delete** on the subsequent screen to confirm the action.

27. Switch back to the open terminal session / command prompt of the primary node of your Deployment Manager. You should be in the <wp_profile>/ConfigEngine directory.

28. Run the following Portal configuration task:
./ConfigEngine.sh wp-change-portal-admin-user
-DWasPassword=newpassword
-DnewAdminId=uid=PortalAdminIDLOCAL,o=defaultWIMFileBasedRealm
-DnewAdminPw=newpassword
-DnewAdminGroupId=cn=wpsadminsLOCAL,o=defaultWIMFileBasedRealm

```
[root@      ~]# cd /opt/IBM/WebSphere/wp_profile/ConfigEngine/
[root@      ConfigEngine]# ./ConfigEngine.sh wp-change-portal-admin-user -DWasPa
ssword=dmgrAdminPswd -DnewAdminId=uid=PortalAdminIDLOCAL,o=defaultWIMFileBasedRe
alm -DnewAdminPw=newpassword -DnewAdminGroupId=cn=wpsadminsLOCAL,o=defaultWIMFil
eBasedRealm
```

29. Navigate to the <wp_profile>/bin directory on the primary Portal node. Stop the nodeAgent by executing the stopNode.sh command.

```
[root@      ~]# cd /opt/IBM/WebSphere/wp_profile/bin/
[root@      bin]# ./stopNode.sh -user PortalAdminIDLOCAL -password newpassword
```

30. Execute the syncNode.sh command from the <wp_profile>/bin directory.

```
[root@      ~]# cd /opt/IBM/WebSphere/wp_profile/bin/
[root@      bin]# ./syncNode.sh mydmgr.ibm.com 8879 -user PortalAdminIDLOCAL -pa
ssword newpassword
```

31. Execute the startNode.sh command from the <wp_profile>/bin directory.

```
[root@      ~]# cd /opt/IBM/WebSphere/wp_profile/bin/
[root@      bin]# ./startNode.sh
```

NOTE: This guide assumes if you are reading this appendix only the primary node of the Portal server has been configured in the Portal cluster. If you have multiple nodes in your Portal cluster, repeat steps #29-#31 for each node in your cluster to ensure they receive the configuration updates.

32. Execute the stopServer.sh command from the <wp_profile>/bin directory for the Portal server.

```
[root@      ~]# cd /opt/IBM/WebSphere/wp_profile/bin/
[root@      bin]# ./stopServer.sh WebSphere_Portal -user PortalAdminIDLOCAL -pas
sword newpassword
```

33. Execute the startServer.sh command from the <wp_profile>/bin directory for the Portal server.

```
[root@      ~]# cd /opt/IBM/WebSphere/wp_profile/bin/
[root@      bin]# ./startServer.sh WebSphere_Portal
```

NOTE**:** This guide assumes if you are reading this appendix only a single Portal server has been configured in the Portal cluster. If you have multiple servers in your Portal cluster, repeat steps #31-#33 for each server in your cluster.

34. Verify that you can login to your Primary Portal with the new PortalAdminIDLOCAL userID.

    http://myprimaryportal.ibm.com:10039/wps/myportal

At this time, you may proceed with adding the LDAP server to your Portal cluster. The duplicate usernames and duplicate group names have been removed from the configuration and will no longer conflict when the LDAP server is added to the configuration.

Encountering Issues and Receiving Help

If you encounter any failures following the steps in this guide, you may open a case with HCL ® Portal Level 2 support.

To best assist you with any issues you encounter, the L2 Support engineer may request that you run the wpcollector tool.

wpcollector is a command line tool that automates the collection of portal logs and configuration files and optionally assists the customer with sending those files to HCL ® Support, saving valuable time. Using automated log collection early in the PMR life cycle can greatly reduce the number of doc requests that are made by Support.

For more information on wpcollector and how to use it, see the following documentation:

https://support.hcltechsw.com/csm

For questions, error message explanations, and more, try searching or posting a question on Forum. This is an HCL ® run forum to ask and answer technical questions:

https://support.hcltechsw.com/community?id=community_forum&sys_id=02c5dcf01b32f70cc1f9759d1e4bcb43

Questions About This Guide

If you have any questions **specifically regarding the contents of this guide**, the primary editor – Rahul Srivastava - can be reached at: rahulsr@hcl.com

Authors of this Guide

Roopanker Upadhyay, HCL® Portal L2 Support Engineer, for contributions on Portal installation, database transfer, and clustering.

Rahul Srivastava, HCL® Portal L2 Support Engineer, for contributions on LDAP security and web server installation and configuration, Portal Installation, database transfer, and clustering.

Travis Cornwell, HCL® Portal L2 Support Engineer, technical reviewer and editor of all chapters.

Thorsten Reinheimer, HCL® EUTC Support Engineer, technical reviewer and editor of all chapters.

Acknowledgments

Brett Gordon, HCL® Portal L2 Support Manager, for significant technical review and feedback on initial release of this guide.