PeopleSoft

EnterpriseOne 8.93 Collaborative Portal PeopleBook

May 2004

EnterpriseOne 8.93
Collaborative Portal PeopleBook
SKU TT893CP0504

Table of Contents

Installing the Collaborative Portal

After you install the WebSphere Portal and related services, you can install the Collaborative Portal. After installation, you can create your own portlets or run vendor-provided portlets in your portal.

The installation process is composed of the following steps:

1. Align your WebSphere client- and server-side security settings
2. Run the Collaborative Portal installation program

When you prepare to install Collaborative Portal, gather the following information:

Data	Record Your Values
WebSphere Portal administrator user ID and password	
WebSphere Application Server node name (located in the WebSphere Advanced Administrative Console under Nodes—typically the machine name of the server that is running WebSphere)	
WebSphere Portal Application Server name (the default value is WebSphere Portal)	
WebSphere Portal Virtual Host name (the default value is default_host)	
WebSphere Application Server installation directory	
WebSphere Portal Server installation directory	

Many portlets exist for the Collaborative Portal. These portlets are available on the Update Center. Contact your support representative for information about how to use the Update Center.

Note

If you have downloaded Portlets for an earlier version of the Collaborative Portal, you must check with the Update Center to see if new versions of these Portlets are available for this version of the Collaborative Portal. Use the Portlet Application tool of the Portal Administration Place to install updates of Portlet modules you already have installed.

Prerequisite

- Align your WebSphere client- and server-side security settings.
- Ensure that the WebSphere Portal Server is installed and operating:
  - Verify that you can successfully sign in using your WebSphere Portal administrator user ID and password.
  - Verify that you have a matching version of the WebSphere Portal Server for the version of the Collaborative Portal that you are installing. For example, if you are installing version 4.2.1.01 of the Collaborative Portal, you must install it onto version 4.2.1 of the WebSphere Portal Server. Notice that the first part of the Collaborative Portal version number is the same as the WebSphere Portal Server version.
- Ensure that you can connect to the WebSphere Application Server through the WebSphere Advanced Administration Console.
- Your JAS instance (JAS.ini and JDBJ.ini) must reside on the same machine as the Collaborative Portal because the installation does not allow you to point to a remote machine. If your JAS instance is not local relative to where you intend to install Collaborative Portal, copy your instance to the target server.

► To determine your WebSphere server-side security setting

Depending on your security settings for WebSphere, the install program may not be able to properly deploy and configure one or more WebSphere components. Oftentimes, the server- and client-side security settings are not configured to match. As recommended by IBM (under reference number 1051202), WebSphere client-side security should be enabled if your server-side security is enabled. Similarly, your client-side security should be disabled if your server-side security is disabled.

1. Locate and open the following file with a text editor:

   ```
   <WebSphere Application Server installation
   directory>\properties\sas.server.props
   ```

   For example:

   ```
   c:\WebSphere\AppServer\properties\sas.server.props
   ```

2. Locate the following line in the file:

   ```
   com.ibm.CORBA.securityEnabled=<setting>
   ```

   where `<setting>` is either true (security enabled) or false (security disabled).

3. Close the file.

► To align your WebSphere client-side security setting with a disabled server-side setting

In this scenario, your installation is set to not use WebSphere server-side security.

Note

By following this procedure to disable your client-side security, you are not disabling WebSphere security itself because WebSphere security is enabled by a combination of server-side and client-side settings.

1. Locate and open the following file with a text editor:

   ```
   <WebSphere Application Server installation
   directory>\properties\sas.client.props
   ```

   For example:

   ```
   c:\WebSphere\AppServer\properties\sas.client.props
   ```

2. Edit the sas.client.props file to ensure the following line is set to false:

   ```
   com.ibm.CORBA.securityEnabled=false
   ```

3. Stop and restart your WebSphere services.
4. You may now start the Collaborative Portal install program, and the installation should complete normally.

► To align your WebSphere client-side security setting with pass-through security to match an enabled server-side setting

In this scenario, your installation is set to use WebSphere server-side security. This procedure enables you to set the security to pass-through the user ID and password information to enable proper installation by the Collaborative Portal install program. After you complete this procedure and the Collaborative Portal solution is installed, you may revert to your pre-existing WebSphere security settings.

1. Locate and open the following file with a text editor:

   ```
   <WebSphere Application Server installation
   directory>\properties\sas.client.props
   ```

   For example:

   ```
   c:\WebSphere\AppServer\properties\sas.client.props
   ```

2. Edit the sas.client.props file to comment out the following lines:

   ```
   #com.ibm.CORBA.securityEnabled=<your_setting>

   #com.ibm.CORBA.loginSource=<your_setting>

   #com.ibm.CORBA.loginUserid=<your_setting>

   #com.ibm.CORBA.loginPassword=<your setting>
   ```

You must search throughout the sas.client.props file to find each of these settings because they might not appear near each other.

3. Ensure that the following lines are set as shown below:

```
com.ibm.CORBA.securityEnabled=true

com.ibm.CORBA.loginSource=properties

com.ibm.CORBA.loginUserid=<username>

com.ibm.CORBA.loginPassword=<password>
```

4. where <*username*> and <*password*> are the credentials you are asked to specify when signing in to the WebSphere Advanced Administration Console. Typically, these are the credentials for the wpsbind user.

   These settings enable the Collaborative Portal install program to operate in silent mode, which is necessary for successful completion of the install. If these settings are not used, then WebSphere security prompts for user ID and passwords, which causes the installation to fail.

5. Stop and restart your WebSphere services.
6. After the WebSphere services have finished starting, attempt to launch the WebSphere Advanced Administration Console.

   If your settings are correct, the WebSphere Advanced Administration Console opens without error.

   You can now start the Collaborative Portal install program, and the installation should complete normally.

Note

Once the installation is complete, you can revert your settings to their original values. That is, you can uncomment your original settings and comment out or delete the temporary settings required for the Collaborative Portal install program.

► To run the Collaborative Portal installation program

1. Place the Collaborative Portal CD into your CD drive.
2. Run the setup program applicable to your platform.

   For example, if your platform is AIX, you should run `setupaix.bin`.

   The install program starts.

3. On Welcome, click Next.

   The install program asks where to install the Collaborative Portal directory.

4. On Directory Name, enter the location where you want to store installation logs and click Next.

   The install program reminds you that you must have your WebSphere security configured to allow the install program to function properly.

5. Choose the “WebSphere Security is properly configured” option and click Next.

   The install program reminds you that the WebSphere Application Server Admin Server must be running. If you can sign in to the WebSphere Portal, then this server is running.

6. Select the "WebSphere Admin Server is currently running" option and click Next.
7. On WebSphere Configuration – Application Server and Portal Server, complete the form based on the information you gathered about how WebSphere is configured for your system.
8. Click Next.
9. On WebSphere Configuration - JSP Cache, verify that the path for the default JSP cache directory is correct for your installation of WebSphere and click Next.

   The system derives this default JSP cache directory from the information you provided previously.

10. On WebSphere Configuration – Connection Information, specify the user ID and password of a Portal administrator user and click Next.

    The system derives default values for the Portal Server URLs from the information you provided previously.

11. Optionally, on Inherited Trust Configuration, enter the Secret Enterprise Key to use for Inherited Trust and click Next.

    Portlets that use Inherited Trust require this value to function properly. The value that appears initially is a default value. You can change this value later if you do not know what value to enter now.

    The system displays an installation summary.

12. On the next form, complete the following fields:

    - JAS.INI File

      Enter the location of your jde.ini file.

    - JDBJ.INI File

      Enter the location of your jdbj.ini.ini file.

Note

You cannot point to a remote server, so an instance of these files must reside on the Collaborative Server machine.

---

13. Click Next.

    The install program performs a series of automated install steps, which include stopping and starting WebSphere, as well as installing various modules. You must allow time for this process to complete without interaction. If new command windows appear, do not close them.

    In addition to this process, the install program places the following jar files in the ..\WebSphere\AppServer\lib\ext folder:

    - jnet.jar
    - jcert.jar
    - jsse.jar
    - inheritedtrust.jar
    - MAFFoundation.jar

    The program also creates a new file, e1access.ini, in the ..\WebSphere\AppServer\properties folder.

    When finished running the install process, the system notifies you.

14. Click Finish to exit the install program.
15. Change ..\WebSphere\AppServer\properties\e1access.ini so that the system puts the all of the log files in a valid location.

```
############################################################
# LOGS -- Copied from application server jas.ini
############################################################
[LOGS]
Debug=FALSE
;Debug=TRUE
log=Z:\WebSphere\AppServer\installedApps\EA_JDE_3.ear\webclient.war\logs\jas.log
```

16. If you are using Oracle, you must also change ..\WebSphere\AppServer\properties\e1access.ini so that tns points to your tnsnames.ora file.

```
############################################################
# JDBj-ORACLE -- Copied from application server jdbj.ini
############################################################
[JDBj-ORACLE]
tns=Z:\OneWorld_S3_APPL\webclient\web\tnsnames.ora
```

17. Copy the JDBC drivers you used to access the system to the ..\WebSphere\AppServer\lib\ext folder.

See Also

- *Configuring Inherited Trust* in *Collaborative Portal Installation and Configuration Guide*

Configuring Inherited Trust

Portlets can connect to back-end applications, many of which require a signin. To prevent the user from having to sign in to the back-end application after having already been authenticated by the Collaborative Portal, you can use an inherited trust system so that the signin to the back-end application is transparent to the user.

The back-end application must be set up with the same user IDs that are used to access the Collaborative Portal. The inherited trust solution provides a secure authentication routine between the Collaborative Portal and the back-end system without sending the user's password over the network. Although the user ID must be consistent between the two applications, the passwords do not need to be the same.

Secret Enterprise Key

A secret enterprise key makes inherited trust signins secure. Both the Collaborative Portal and applications that use inherited trust (such as CRM) must know this key; if it is changed in one place, it must be changed in all others. If an application is aware of this key, trust is established.

To specify this key on the Collaborative Portal, use the init-parameter called `secretEnterpriseKey` in the web.xml file located in the inherited trust enterprise application. (This file is located in the \WebSphere\AppServer\installedApps\jdeinheritedtrust.ear\InheritedTrust.war\WEB-INF directory.)

```
  <web-app id="WebApp_1">
   <display-name>Inherited_Trust</display-name>
   <servlet id="Servlet_2">
     <servlet-name>InheritedTrustServlet</servlet-name>
     <servlet-class>com.jdedwards.portal.InheritedTrustManagerServlet</servlet-
class>
     <init-param id="InitParam_1">
      <param-name>secretEnterpriseKey</param-name>
      <param-value>mysecretkey</param-value>
     </init-param>
   </servlet>
   <servlet-mapping id="ServletMapping_1">
     <servlet-name>InheritedTrustServlet</servlet-name>
     <url-pattern>/servlet/com.jdedwards.portal.InheritedTrustManagerServlet</url-
pattern>
   </servlet-mapping>
   <servlet-mapping id="ServletMapping_2">
     <servlet-name>InheritedTrustServlet</servlet-name>
     <url-
pattern>/servlet/com.jdedwards.oneworld.owportal.InheritedTrustManagerServlet</url-
pattern>
   </servlet-mapping>
```

Specifying the value of the `secretEnterpriseKey` in this manner prevents it from being accessed via other servlets that might attempt to retrieve this value for malicious use.

▶ To configure Multiple Application Framework (MAF) security

Portlets can launch multiple EnterpriseOne applications using the Multiple Application Framework. With Multiple Application Framework security, the user is not required to log in each time a new application launches. However, to achieve single signon to the EnterpriseOne application, you must configure MAF security properly on both the Collaborative Portal server and the EnterpriseOne JAS server.

1. Set up an Inherited Trust secret key on the Collaborative Portal.
2. On the EnterpriseOne JAS server, ensure that mafsecurity.jar and inheritedtrust.jar reside in the WEB-INF/lib directory.

   This directory is typically located in the following spot in the directory structure:

   X:\WebSphere\AppServer\installedApps\PeopleSoft\JAS\EA_JAS_80.ear\webclient.war\WEB-INF\lib

   Typically, you will find inheritedtrust.jar in X:\WebSphere\AppServer\installedApps\PeopleSoft\JAS\EA_JAS_80.ear\webclient.war\owportal, so you will need to move it.

3. Move inheritedtrust.jar from X:\WebSphere\AppServer\installedApps\PeopleSoft\JAS\EA_JAS_80.ear\webclient.war\owportal to the WEB-INF/lib directory.
4. On the EnterpriseOne JAS server open web.xml and add the following code to the file, where *mykey* is the Inherited Trust secret key you set up in step 1.

   The Inherited Trust secret key must match exactly because it is case-sensitive.

   This <servlet> entry must be added before any <servlet_mapping> tags to ensure well-formed XML.

```
<servlet>
      <servlet-name>
com.jdedwards.maf.security.RemoteSecurityAdapterServlet</servlet-name>
      <servlet-
class>com.jdedwards.maf.security.RemoteSecurityAdapterServlet</servlet-class>
      <init-param>
          <param-name>secretEnterpriseKey</param-name>
          <param-value>mykey</param-value>
      </init-param>
      <load-on-startup>5</load-on-startup>
  </servlet>
```

5. Add the following two entries to the [SECURITY] section of the jas.ini on the EnterpriseOne JAS server.

```
 [SECURITY]

DBUser=xxx

DBPassword=xxx
```

The DBUser and DBPassword entries are the same entries found in your enterprise server JDE.INI. The security server uses these two entries to access the security tables.

Rebranding the Collaborative Portal

After installing the Collaborative Portal, you might want to make modifications to address your company's branding needs.

► To specify a different logo for the signin screen

1. Open the following file in a text editor:

   ```
   <WebSphere Portal Server installation
   directory>\app\wps.ear\wps.war\screens\html\Login.jsp
   ```

   For example:

   ```
   c:\WebSphere\PortalServer\app\wps.ear\wps.war\screens\html\Login.
   jsp
   ```

2. Make a backup of this file in the event that you wish to revert to a pristine version.
3. Locate the following line and then specify the URL of the image you wish to display on your signin screen:

   ```
   String companyLogoImageURL = "";
   ```

   For example:

   ```
   String companyLogoImageURL = "http://server/logo.gif";
   ```

4. Save and close the file.

   Your changes will take effect immediately.

► To specify an additional disclaimer for the signin screen

1. Open the following file in a text editor:

   ```
   <WebSphere Portal Server installation
   directory>\app\wps.ear\wps.war\screens\html\Login.jsp
   ```

   For example:

   ```
   c:\WebSphere\PortalServer\app\wps.ear\wps.war\screens\html\Login.
   jsp
   ```

2. Make a backup of this file.
3. Locate the following line and specify your disclaimer with the following element:

   ```
   String companyDisclaimerHTML = "";
   ```

   For example:

   ```
   String companyDisclaimerHTML = "By signing in, you agree to the
   <a href=\"http://server/path-to/privacypolicy.html\">privacy
   policy</a>.";
   ```

Note

This element is Java code; therefore, quotation marks must be escaped by specifying a back-slash character before them, as shown above.

4. Save the file.

   Your changes will take effect immediately.

► To specify a title for the Web browser

1. Open the following file in a text editor:

   ```
   <WebSphere Portal Server installation
   directory>\app\wps.ear\wps.war\themes\html\jdehead.jsp
   ```

   For example:

   ```
   c:\WebSphere\PortalServer\app\wps.ear\wps.war\themes\html\jdehead
   .jsp
   ```

2. Make a backup of this file in the event that you wish to revert to a pristine version.
3. Locate the following line:

   ```
   <jdewebgui:pagehead>
   ```

   and change it to:

   ```
   <jdewebgui:pagehead addtitle="false">
   ```

4. Insert the following line above the line you just changed:

   ```
   <title>My Company&reg;</title>
   ```

   For example:

   ```
   <title>My Company&reg;</title>

   <jdewebgui:pagehead addtitle="false">
   ```

5. Save and close the file.
6. Delete your portal's temporary JSP cache.

► To delete your portal's temporary JSP cache

Many JSP files are dependent upon other JSP files. If you change a child JSP but not the parent, you will not see your changes. You must either change the modification date of all the parent JSP files in the hierarchy until you get to the root, or simply delete the JSP cache altogether. Use this task to delete Portal JSP cache (such as if you want to see Portal theme and skin changes).

Delete the contents of the following directory:

```
<WebSphere Application Server installation
directory>\temp\nodename\servername\appname
```

where

nodename is the WebSphere application server node name

servername is the WebSphere Portal application server name

appname is the WebSphere Portal application name

For example:

```
c:\WebSphere\AppServer\temp\portal1\WebSphere_Portal\WPS_Enterpri
se_Application
```

The cache will be regenerated automatically, as needed. Preserving a backup of this content is unnecessary.

► **To change a theme's logo to your company's logo**

1. Locate the directory for the theme you wish to change. For instance, the default theme is located at a path similar to:

   ```
   c:\WebSphere\PortalServer\app\wps.ear\wps.war\themes\html
   ```

   For example, the PurpleDropdowns theme is located at a path similar to:

   ```
   c:\WebSphere\PortalServer\app\wps.ear\wps.war\themes\html\PurpleD
   ropdowns
   ```

2. Open the appropriate webgui.css file.

   The theme folder might contain a file named webgui.css. If it does not, this theme uses the webgui.css from the default theme.

3. Locate the following section:

```
.pagelogo {
background-repeat: no-repeat;
background-image: url('http://server/jdewebgui/images/jdelogo-onwhite.gif');
width: 125px;
height: 39px;
}
```

4. Modify the background-image, width, and height settings where width and height are the exact pixel dimensions of the image associated with the URL you specified in the "background-image" setting.

   The URL must also be fully qualified; it must not be relative.

Note

Not all themes are designed to display a page logo (such as the Corporate theme).

► To create a new HTML theme

It is recommended that you copy and modify an existing theme rather than creating a completely new one. However, if you do not want to use this approach, refer to the IBM WebSphere Portal Server InfoCenter documentation for details. This task outlines additional steps to the InfoCenter documentation.

1. If you want to change the colors and logo image of the default theme, place a webgui.css file in your theme's folder.

   This file defines many style attributes that should not be changed. It is recommended that you do not make changes to this file other than modifying the colors and the image URLs.

   If you are satisfied with the colors and logo image of the default theme, proceed to the next step.

2. Add a DIV tag around all visible HTML you have set to appear above the Portlet layout grid.

   This DIV tag must have an ID attribute of "jdeowpTopBarDiv". For example:

```
<DIV ID="jdeowpTopBarDiv">
...
</DIV>
```

3. Add the script handle Onload(); to the ONLOAD attribute of your BODY tag.

   For example, if the ONLOAD attribute is not defined, it will now look like:

   ```
   <BODY ... ONLOAD="javascript:handleOnload();" ... >
   ```

   otherwise, your BODY tag will look like:

   ```
   <BODY ... ONLOAD="javascript:handleOnload();someFunc();" ... >
   ```

4. Sign in to the Collaborative Portal as an administrator user.
5. Use the Portal Administration > Portal Settings > Themes and Skins form to add your new theme. Refer to the IBM WebSphere Portal Server InfoCenter documentation for further details.

Note

In many cases when you make changes to a theme that has already been configured, you will not be able to see your changes until you delete your portal's temporary JSP cache.

► To create a new HTML theme from an existing theme

The easiest way to create a new theme is to duplicate the theme folder of an existing theme.

1. Locate the directory for your HTML themes. For example:

   ```
   c:\WebSphere\PortalServer\app\wps.ear\wps.war\themes\html
   ```

2. This directory contains a folder named PurpleDropdowns. Duplicate this folder (and its contents) and name it MyTheme (or whatever you would like to name your theme).
3. Open the MyTheme folder.

   This theme is set to control top-level page navigation by a dropdown control, which means that only sub-level page navigation will be displayed on a left-navigation tree. If you prefer this option, skip to the next step. Otherwise, use the following process to set your theme to display all levels of page navigation on a left-navigation tree.

   a. Open the Default.jsp file in a text editor.
   b. Locate the following line:

      ```
      boolean leftNavUsed = false;
      ```

   c. Change the line to:

      ```
      boolean leftNavUsed = true;
      ```

4. Optionally, alter the webgui.css and jde.css files of your new theme.

   These files define many style attributes that should not be changed. It is recommended that you avoid changing these files other than modifying the colors and the image URLs.

   If you are satisfied with the colors and images of the theme that you copied, proceed to the next step.

5. If desired, use a graphics program to modify the images in the new theme folder.

   Your new theme folder contains many images that are used by the various portlet skins. You can use a graphics program to modify any of these images as you wish, however, you must preserve the file names, image formats, and image dimensions.

6. Sign in to the Collaborative Portal as an administrator user.
7. Use the Portal Administration > Portal Settings > Themes and Skins screen to add your new theme.

   Refer to the IBM WebSphere Portal Server InfoCenter documentation for further details.

Note

In many cases when you make changes to a theme that has already been configured, you will not be able to see your changes. When this happens, simply delete your portal's temporary JSP cache.

An unsupported internal utility known as the Theme Generator can be used to automate some of the more difficult tasks, such as defining the proper color codes and URLs in the webgui.css and jde.css files.

Troubleshooting: Collaborative Portal

Some images appear to be missing

This problem might be specific to a portlet or a problem with your Collaborative Portal install. First, open a browser and visit the signin screen of the Collaborative Portal. Then, attempt to sign in with an invalid user ID and password. This action should produce a signin error.

- If you do not see an error icon toward the top of the error message, a problem exists with the Collaborative Portal install. It is likely that the install program did not successfully install either the ERP Application or that the WebSphere Web Server Plug-in needs to be regenerated. Verify that your WebSphere Security is configured properly and run the Collaborative Portal install program again.
- If you do see the error icon, another family of images might not be working (the install program might affect these images). Open the webgui.css file from the default HTML theme using a text editor program. For example, in Windows, this file is located at:

  `c:\WebSphere\PortalServer\app\wps.ear\wps.war\themes\html\webgui.css`

  Search for the pagelogo section, which might look similar to the following example:

```
.pagelogo {
background-repeat: no-repeat;
background-image: url('http://cp.jdedwards.com:80/jdewebgui/images/jdelogo-
onwhite.gif');
width: 125px;
height: 39px;
}
```

  Examine the URL value for the background image, for example:

  `http://cp.jdedwards.com:80/jdewebgui/images/jdelogo-onwhite.gif`

  Paste this URL in the address bar of your Web browser. If the image you chose does not appear, the URL is incorrect. The text before `/jdewebgui/images/jdelogo-onwhite.gif` is the Portal Server URL Prefix value that was specified in the install program on the WebSphere Configuration – Connection Information install form.

  Determine the corrections you must make to the URL so that the image will load properly. Then, run the Collaborative Portal install program again. Ensure that you specify the correct value in the Portal Server URL Prefix field.

Some pages do not appear to be functioning properly

First, verify that your Web browser meets the minimum technical requirements of the Collaborative Portal.

Note

Some portlets might have additional technical requirements. Please refer to the associated portlet documentation for further information.

If you recently updated your client machine Web browser, it is possible that the browscap.ini file on the Web server is out of date. The browscap.ini file contains the user agent strings for each version of each Web browser. Update this file each time you update your Web browser.

Next, try to isolate your portlet by making it the only one on the page. A portlet bug might be negatively influencing other portlets around it on the same page. This negative influence could be caused by several factors:

- Improperly formatted HTML
- JavaScript problems
- Portlets that override Cascading StyleSheet (CSS) definitions

If possible, avoid using the problem portlets or, instead, install updates to the portlets that are causing the problems.

A portlet from the Update Center fails to install or update

Verify that you specified the version of your Collaborative Portal accurately on the Update Center when you downloaded the portlet. Do not use portlets for an older or a newer version of the Collaborative Portal.

Typically, the Update Center provides a ZIP file containing documentation and a portlet archive file. You must extract the ZIP file first. Ensure that you are selecting the portlet archive file—not the ZIP file—when performing an install or update.