



RSA Access Manager Ready Implementation Guide For Portal Servers and Web-Based Applications

Last Modified 6/5/07

1. Partner Information

Partner Name	PeopleSoft
Web Site	www.peoplesoft.com
Product Name	PeopleSoft 8.9
Version & Platform	8.9
Product Description	<p>PeopleSoft 8 pure-internet software enables your enterprise to combine online transactions with rich content—helping customers, suppliers, and employees work together. PeopleSoft 8 is more than products. It embodies PeopleSoft's vision and strategy. It's about working collaboratively. Its about no code on the client. It's about real-time enterprise.</p> <p>PeopleSoft 8 applications are delivered over a standard internet browser for comprehensive business management—making PeopleSoft the only software company to provide real-time business solutions in a pure-internet environment. Innovation of this magnitude is what has made PeopleSoft a leader since 1987..</p>
Product Category	ERP

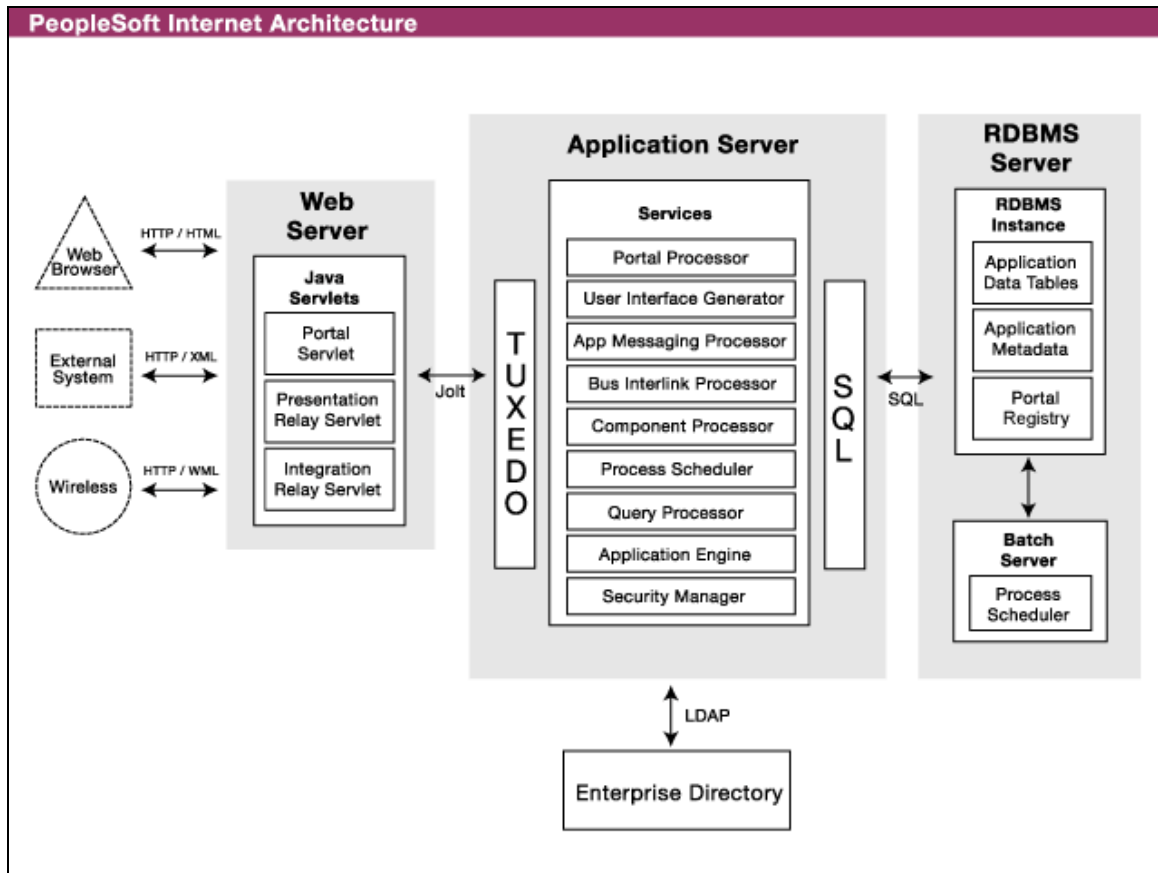
PeopleSoft.

2. Contact Information

	Sales contact	Support Contact
Web	www.peoplesoft.com	www.peoplesoft.com/corp/en/support/
Phone	800.380.SOFT	800.4PPLSFT
Web	www.company.com	www.company.com

3. Solution Summary

Feature	Details
Use UserID for SSO	Yes
Use UserID for Personalization	Yes
Recognize Authentication Type	No
API-level Authorization Support (RuntimeAPI)	No
User Management (AdminAPI)	YES via LDAP PROFILESYNCH



4. Integration Overview

To achieve Single-Sign-On with PeopleSoft, the RSA Access Manager Agent is installed on a web server platform supported by PeopleSoft. If BEA Weblogic is used, BEA must be setup to proxy a web server supported by an RSA Access Manager Agent. The agent is then configured to protect all PeopleSoft related pages. PeopleSoft establishes the identity of the user by parsing the HTTP Headers and using the 'ct-remote-user' variable to serve personalized content. PeopleSoft also supports User Management via the PeopleCode function 'LDAP PROFILESYNCH', which will dynamically create a user in the PeopleSoft database if it exists in RSA Access Manager.

5. Product Requirements

- Please consult the PeopleSoft application release notes and upgrade notes for possible support restrictions. Not all Peoplesoft applications support every combination supported on PeopleTools.
- RSA Access Manager must be installed.
- An RSA Access Manager Web Server Agent must be installed on a web server proxy to the PeopleSoft Application Server. For example, If PeopleSoft is installed on IBM WebSphere on Windows, then Microsoft IIS may be configured as a proxy to WebSphere, and the RSA Access Manager IIS Agent can be installed on IIS. In this way, all PeopleTools traffic will pass through IIS and the Access Manager Agent. Please consult RSA Access Manager documentation for supported web servers. Please consult the appropriate web server and application server documentation for instructions on configuring web server proxies.

Integration Modules

File Name	Destination
RSA Access Manager Agent	User Defined
RSA_Access Manager Signon PeopleCode Function	Signon PeopleCode record

6. Product Configuration

This section provides instructions for integrating the People Soft with RSA Access Manager. This document is not intended to suggest optimum installations or configurations. It is assumed that the reader has both working knowledge of the two products to perform the tasks outlined in this section and access to the documentation for both in order to install the required software components. All products/components need to be installed and working prior to this integration. Perform the necessary tests to confirm that this is true before proceeding.

PeopleSoft 8.9 is an Enterprise Resource Planning (ERP) software package which provides automation of tasks in certain areas such as finance and human resources. A summary of the needed configuration steps in order for RSA Access Manager to authenticate PeopleSoft users are as follows:

- A. Create a PeopleSoft user "default user"
- B. Turn off PeopleSoft sign-on page
- C. Implement RSA Access Manager specific Signon PeopleCode
- D. Activate RSA Access Manager specific Signon PeopleCode
- E. RSA Access Manager configuration
- F. Logout Screens
- G. Logon Screens

Important: You must have working knowledge of both RSA Access Manager 6.0, PeopleSoft 8.9 and PeopleTools 8.47 to perform the tasks outlined in this guide. All products need to be installed and working prior to this integration. Perform the necessary tests to confirm that this is true before continuing.

Below is a step-by-step example of what occurs once PeopleSoft has been configured to trust authentication performed at the web server level via the RSA Access Manager Web Server Agent:

Step	Component	Description
1	Browser	User clicks on a link to the PeopleSoft application: http://servername/ps/ps/?cmd=start
2	Web Server	The RSA Access Manager Web Server Agent intercepts the request for the URL, authenticates the user, and adds the UserID to the HTTP header.
3	Servlet	The PeopleSoft servlet receives the HTTP request, which includes the UserID in a header and connects to the application server using the User ID and Password set in the "Public Users" credentials in the current Web Profile. See below for details.
4	Application Server	The Application server authenticates the connection from the web server by checking the aforementioned user ID and password. The user ID and password must be valid in order for the connection to succeed and for Signon PeopleCode to execute.
5	Signon PeopleCode	When Signon PeopleCode runs, it grabs the "real" UserID from the HTTP request and calls the PeopleCode built-in SetAuthenticationResult and passes the user ID, and "true" for AuthResult. The PeopleCode program always passes "true" for AuthResult because the application server is "trusting" the authentication logic of the Access Manager web server plugin. The PIA session is set to the user ID of whatever you pass into SetAuthenticationResult. For example, SetAuthenticationResult(True, "mrennie", "", False); In this case, the system sets the session to "mrennie". The user can access all the pages to which mrennie has access.

A. Create a PeopleSoft user "default user"

This user ID only requires the permission to log into the HRMS application. PeopleSoft recommends creating a long and difficult-to-guess password. For this example only, "PASSWORD" is used for simplicity's sake. **Note that the user ID and password are case sensitive, and must be set in uppercase.**

- *User ID* = DEFAULT_USER
- *Password* = PASSWORD

B. Turn off PeopleSoft sign-on page

Log into the HRMS system and navigate to *PeopleTools* → *Web Profile* → *Web Profile Configuration* → *<Profile>* → *Security*, where *<Profile>* is the current environment's Web Profile. Check the Allow Public Access checkbox, set *User ID* and *Password* to the values set in Step A, and click *Save*.

<input type="checkbox"/> PIA use HTTP Same Server ?	SSL
<input checked="" type="checkbox"/> Allow Unregistered Content ?	<input type="checkbox"/> Secured Access Only ? <input checked="" type="checkbox"/> Secure Cookie with SSL ?
Authenticated Users	
Inactivity Warning: <input type="text" value="1,080"/> Seconds ?	HTTP Session Inactivity: <input type="text" value="0"/> Seconds ?
Inactivity Logout: <input type="text" value="1,200"/> Seconds ?	
Timeout Warning Script: WEBLIB_TIMEOUT.PT_TIMEOUTWARNING.FieldFormula.IScript_TIMEOUTWARNING	<input type="button" value="Override"/> ?
Public Users	
<input checked="" type="checkbox"/> Allow Public Access ?	User ID: <input type="text" value="DEFAULT_USER"/> ?
	Password: <input type="text" value="*****"/> ?
	HTTP Session Inactivity: <input type="text" value="1,200"/> Seconds ?
Web Server Jolt Settings	
Disconnect Timeout: <input type="text" value="0"/> Seconds ?	XML Link
Send Timeout: <input type="text" value="50"/> Seconds ?	User ID: <input type="text" value="VP1"/> ?
Receive Timeout: <input type="text" value="600"/> Seconds ?	Password: <input type="text" value="***"/> ?
	<input checked="" type="checkbox"/> XML Link Use HTTP Same Server ?

Note: The user is never actually signed on as *DEFAULT_USER*. The *DEFAULT_USER* ID is just a temporary value used to initiate a secure connection to the application server. The application server then determines the real user ID using Signon PeopleCode.

C. Implement RSA Access Manager specific Signon PeopleCode

The following is sample PeopleCode to be used for RSA Access Manager interoperability. This code can reside in its own record or within one already present. For testing purposes here, it was added to an existing record called 'FUNCLIB_LDAP'. The sample code was cut/pasted into the record via the PeopleSoft Application Designer (*Start* → *Programs* → *PeopleTools Installation* → *Application Designer*). When logging into Application Designer, note that the user must have permission to modify the 'FUNCLIC_LDAP' record.

Signon PeopleCode

Signon

Invoke as user signing in

Invoke as User ID: Password:

Signon PeopleCode

[Customize](#) | [Find](#) | [View All](#) |

*Sequence	Enabled	*Record	*Field Name	Event Name	Function Name
1	<input type="checkbox"/>	FUNCLIB_PWDCNTL	PWDCNTL	FieldChange	Password_Controls
2	<input type="checkbox"/>	FUNCLIB_LDAP	LDAPAUTH	FieldDefault	WWW_AUTHENTICATION
3	<input type="checkbox"/>	FUNCLIB_LDAP	LDAPAUTH	FieldDefault	LDAP_AUTHENTICATION
4	<input type="checkbox"/>	FUNCLIB_LDAP	LDAPAUTH	FieldDefault	SSO_AUTHENTICATION
5	<input type="checkbox"/>	FUNCLIB_LDAP	LDAPAUTH	FieldDefault	LDAP_PROFILESYNCH
6	<input checked="" type="checkbox"/>	FUNCLIB_LDAP	LDAPAUTH	FieldDefault	RSA_CLEARTRUST

E. RSA Access Manager configuration

- Install RSA Access Manager web server agent on the web server used to proxy the PeopleSoft Application Server.
- From the RSA Access Manager Entitlements Manager, create users identical to those within PeopleSoft.
- From the RSA Access Manager Entitlements Manager, protect the appropriate resource. The certification testing used /ps/*.
- From the RSA Access Manager Entitlements Manager, create the appropriate rules and entitlements.

F. Logout Screens

Note that the standard PeopleSoft Logout link must be modified or disabled. The following example sets the Logout link to point to a HTML page that will close the browser, thus destroying both PeopleSoft and RSA Access Manager sessions.

1. Navigate to %PEOPLETOOLS_PORTAL_HOME%\WEB-INF\psftdocs\ps and make a backup copy of signin.html.
2. Copy the following code to a file named signin.html, and replace the new file with the original file in Step 1.

```
<html>
  <head>
    <body>
      <SCRIPT LANGUAGE="JavaScript">
        window.opener = top;
        window.close();
      </SCRIPT>
    </body>
  </html>
```

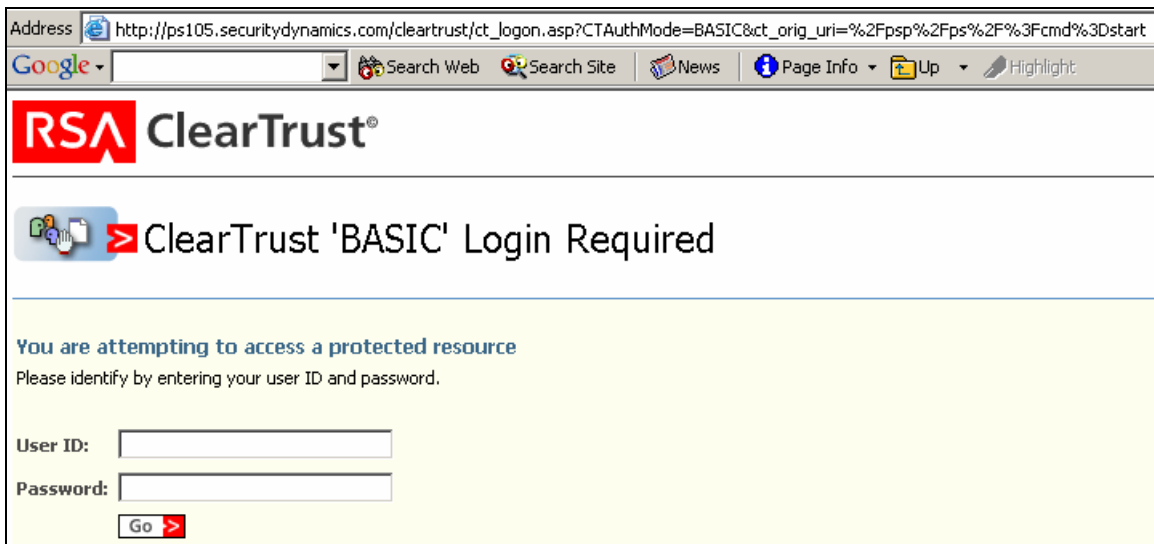
3. Restart the servers.

Now when a user clicks the Logout link, the browser window will close.

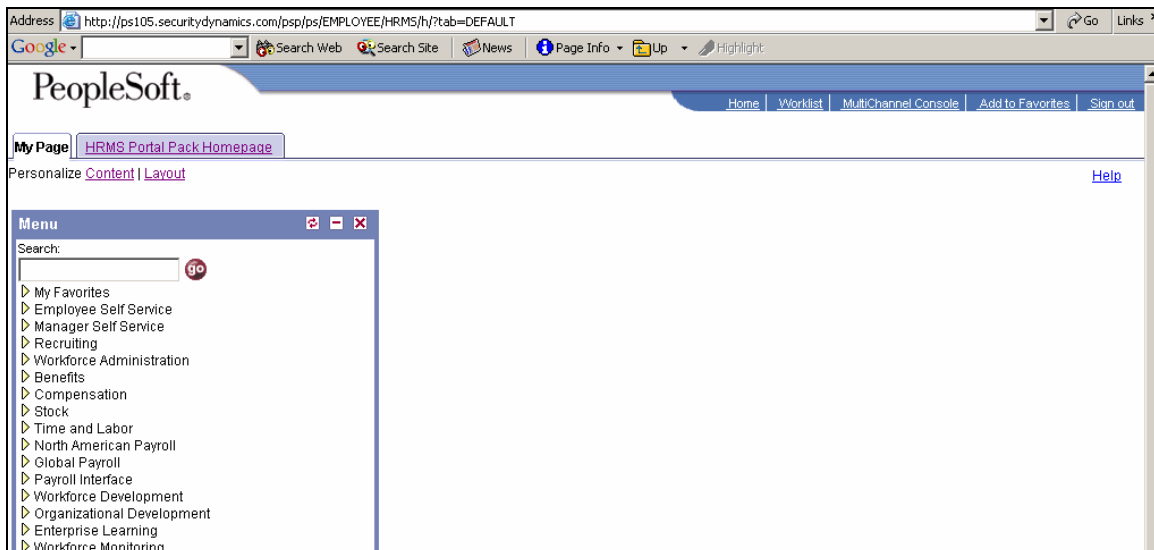
G. Logon Screens

Once the RSA Access Manager IIS Agent has been installed and configured and the appropriate URI has been added as a protected resource in the Entitlements Manager, users will be prompted to authenticate via RSA Access Manager when they select the application link.

`http://servername/ps/ps/?cmd=start`



After the user authenticates, they are presented with their PeopleSoft page.



7. Certification Checklist for Portal Servers and Web-Based Apps

Date Tested: February 23, 2007

Product	Tested Version
RSA Access Manager Server	6.0
RSA Access Manager IIS Agent	4.x
Oracle	8i
PeopleTools	8.47
Iplanet Directory server	5.1
PeopleSoft HRMS	8.9
PeopleSoft Portal	8.9
BEA Weblogic	6.1 sp2
Microsoft Internet Information Server	5.0
BEA Tuxedo	6.5
BEA Jolt	1.2

Test Case	Result
Product Characteristics for SSO Support	
Application/Portal is web-based, and supports access by a standard HTTP-based browser	P
Application/Portal runs on Web Server Platform supported by RSA Access Manager	P
Application/Portal login interface can be modified or replaced	P
Application/Portal can extract user information from RSA Access Manager session cookie	N/A
Application/Portal can extract user information from HTTP Headers	P
Application/Portal can extract authentication type from RSA Access Manager session cookie	N/A
Application/Portal can extract authentication type from HTTP Headers	N/A
Application/Portal can perform SSO with other RSA Access Manager-supported Web Server	P
Login - General	
HTTP basic authentication	N/A
Forms based	P
Forms based w/ URI retention	P
Login – Basic Authentication	
Access Denied for unauthorized user	P
Successful login for authorized user	P
Successful recognition of identity/personalization in 3 rd Party Product	P
Successful recognition of identity/personalization after SSO with other RSA Access Manager-supported Web Server	P
Login –Graded Authentication	
Access Denied for unauthorized user	N/A
Successful login for authorized user	N/A
Successful recognition of identity/personalization in 3 rd Party Product	N/A
Successful recognition of identity/personalization after SSO with other RSA Access Manager-supported Web Server	N/A

JGS

*P=Pass or Yes F=Fail N/A=Non-available function

8. Notes

- **BEA proxy to Microsoft IIS:** The proxy needs to be setup so that you can install the RAS Access Manager IIS agent to provide Single Sign On to the PeopleSoft environment running on BEA. See the PeopleSoft and BEA documentation on how to configure this solution. The certification testing used the path based proxy method and the iisproxy.ini file that was created had the following settings.

```
WebLogicHost=ps105.securitydynamics.com  
WebLogicPort=7001  
WIForwardPath=/ps, /cs
```

- **LDAP PROFILESYNCH:** The PeopleCode function 'LDAP PROFILESYNCH', will dynamically create a user in the PeopleSoft database if it exists in Access Manager (via LDAP). This is possible when PeopleCode is modified for the LDAP_PROFILESYNCH function to add the DN info (O, OU, etc) to the userID passed in the HTTP header.

9. Known Issues

- This integration is currently unavailable for environments in which PeopleSoft is running on an Oracle application server.
- Usernames are case sensitive in PeopleSoft, but case insensitive in Access Manager. So, "jsmith", "JSmith" and "JSMITH" would uniquely represent one Access Manager user and three PeopleSoft users. It is therefore a requirement of this integration that each PeopleSoft username is represented by a unique, case insensitive string of characters. To highlight this requirement, the example code converts all incoming usernames to uppercase. In the example, all PeopleSoft users are stored in uppercase. Therefore, if the username "jsmith" is entered for Access Manager authentication, it is converted to "JSMITH" before creating a People session. Please remove the "Upper" function in the following line of code if necessary.

```
SetAuthenticationResult( True, Upper(&userID), "", False);
```

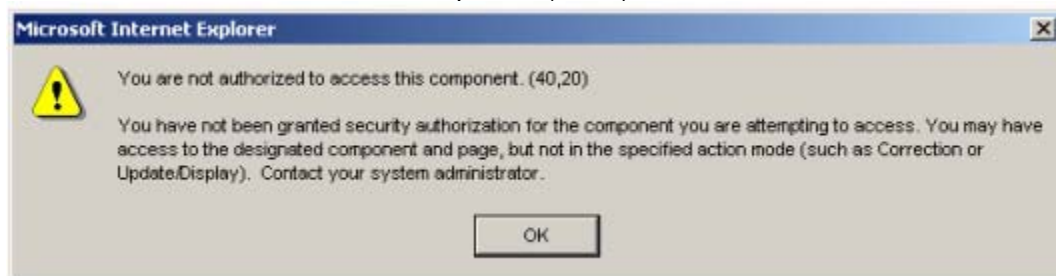
It is recommended that PeopleSoft usernames be restricted to all uppercase or all lowercase letters. This way, the users will have a case insensitive authentication with Access Manager. The code can then be tailored to normalize the id as appropriate (i.e. to convert the id to uppercase as in the example, or to lowercase, if that is how they are stored in PeopleSoft).

- When PeopleSoft 8 uses BEA Weblogic as its application server proxied through IIS webserver, the http header variable that the BEA WebLogic server sees is 'ct-remote-user' and not 'CT_REMOTE_USER'. If this is the case in your configuration, the appropriate line in the PeopleCode will need to be modified:

```
&userID = %Request.GetHeader("ct-remote-user");
```


- There have been instances where users will get the following message even though they have authorization to the component they tried to access.

You are not authorized to access this component (40,20)



To help resolve this issue it is recommended to backup the following files and then change all the lines that contain cmd=login to cmd=start in each file.

```
cookiesrequired.html  
exception.html  
expire.html
```



passwordexpired.html
passwordwarning.html
signin.html
signin.wml
signintrace.html
signon.wml
sslrequired.html