This documentation and any related computer software help programs (hereinafter referred to as the "Documentation") is for the end user's informational purposes only and is subject to change or withdrawal by CA at any time.

This Documentation may not be copied, transferred, reproduced, disclosed, modified or duplicated, in whole or in part, without the prior written consent of CA. This Documentation is confidential and proprietary information of CA and protected by the copyright laws of the United States and international treaties.

Notwithstanding the foregoing, licensed users may print a reasonable number of copies of the Documentation for their own internal use, and may make one copy of the related software as reasonably required for back-up and disaster recovery purposes, provided that all CA copyright notices and legends are affixed to each reproduced copy. Only authorized employees, consultants, or agents of the user who are bound by the provisions of the license for the product are permitted to have access to such copies.

The right to print copies of the Documentation and to make a copy of the related software is limited to the period during which the applicable license for the product remains in full force and effect. Should the license terminate for any reason, it shall be the user's responsibility to certify in writing to CA that all copies and partial copies of the Documentation have been returned to CA or destroyed.

EXCEPT AS OTHERWISE STATED IN THE APPLICABLE LICENSE AGREEMENT, TO THE EXTENT PERMITTED BY APPLICABLE LAW, CA PROVIDES THIS DOCUMENTATION "AS IS" WITHOUT WARRANTY OF ANY KIND, INCLUDING WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NONINFRINGEMENT. IN NO EVENT WILL CA BE LIABLE TO THE END USER OR ANY THIRD PARTY FOR ANY LOSS OR DAMAGE, DIRECT OR INDIRECT, FROM THE USE OF THIS DOCUMENTATION, INCLUDING WITHOUT LIMITATION, LOST PROFITS, BUSINESS INTERRUPTION, GOODWILL, OR LOST DATA, EVEN IF CA IS EXPRESSLY ADVISED OF SUCH LOSS OR DAMAGE.

The use of any product referenced in the Documentation is governed by the end user's applicable license agreement.

The manufacturer of this Documentation is CA.

Provided with "Restricted Rights." Use, duplication or disclosure by the United States Government is subject to the restrictions set forth in FAR Sections 12.212, 52.227-14, and 52.227-19(c)(1) - (2) and DFARS Section 252.227-7014(b)(3), as applicable, or their successors.

All trademarks, trade names, service marks, and logos referenced herein belong to their respective companies.

Copyright © 2007 CA. All rights reserved.
CA Product References

This document references the following CA products:
- CA™ SiteMinder®

Contact Technical Support

For online technical assistance and a complete list of locations, primary service hours, and telephone numbers, contact Technical Support at http://ca.com/support.
Chapter 1: Overview and Architecture

This section contains the following topics:

- **Background** (see page 7)
- **Increased Security with Tier 2 Integration** (see page 8)
- **Architecture** (see page 9)

**Background**

In an effort to meet the requirements of customers and enable more widespread use of applications, many leading ERP vendors, including PeopleSoft, have developed web-based versions of their applications or web-based front ends for their applications. These web-based front ends provide:

- A standard look-and-feel for employees
- User authentication
- Basic security (such as login by username and password)
- Single signon (SSO) capability for some of these front ends

SiteMinder lets you create a centrally managed environment, providing a secure, personalized user experience across all web applications. Through published interfaces, SiteMinder can authenticate users to PeopleSoft. This integration enables the PeopleSoft 8 web-based infrastructure and applications to coexist with other portals and web applications, while offering the maximum user experience and benefit.
Increased Security with Tier 2 Integration

Successful approaches to centrally managed security have typically included the use of a standard CA Web Agent on a web server and a small piece of PeopleCode that enables PeopleSoft to trust the contents of an HTTP header inserted by eTrust SiteMinder. Such designs depend upon a level of trust of the web server, a compromise of which could be used to gain elevated access to the system. eTrust SiteMinder labels these designs Tier 1 because the point of trust is entirely within the first tier—the web server. In environments where the application server and web server are located entirely on a trusted network, where security requirements are low to moderate, this design is adequate.

In Tier 2 implementation, the point of trust moves away from the web server and into a more trusted host—in this case the PeopleSoft application server. In Tier 2 integrations, the application that implements the application logic and security is given the ability to call SiteMinder APIs to communicate with a Policy server, to validate the information that is presented from the web agent.

Many web-based applications use an independent session management scheme, frequently through the use of a cookie. Therefore, SiteMinder’s replay prevention and session management logic may be bypassed. The possibility that the SiteMinder and application sessions could lose synchronization with each other is one of the main security problems when integrating applications that maintain their own sessions. Tier 2 integration includes a component to prevent such session synchronization issues. The SessionLinker web server plug-in monitors the SiteMinder Session ID header and PeopleSoft session cookies. When the two sessions diverge, action is taken to prevent the application from operating until a new session within PeopleSoft is established. The default action is to destroy the PeopleSoft session, causing PeopleSoft to create a new session with the correct user information.
The following illustration shows a typical environment.

A description of the numbers in the preceding illustration follows:

1. The user connects to a SiteMinder Agent-enabled web server.
2. The embedded SiteMinder Web Agent communicates with the SiteMinder Policy server and attempts to authenticate and authorize the request for access to PeopleSoft web application resources.
3. The Policy server verifies access permissions and returns PeopleSoft username back to the Web Agent for use in PeopleSoft.
4. The web server passes user security context to an Optional Application Server for transmittal to the PeopleSoft application server.
5. The application server transmits the request to the PeopleSoft application server. Credentials (user security context information) for the DEFAULT_USER variable are carried to PeopleSoft. The application server begins a session by invoking Signon PeopleCode.

**Note:** The DEFAULT_USER account has no access to the system with or without SiteMinder's approval; if someone were to obtain and attempt to use that account without SiteMinder, no access would be granted and no data would be available.
6. Signon PeopleCode retrieves the existing SiteMinder session information and calls the Tier 2 Validation Library to validate the information.

7. The Validation Library (SmPSLoginLib) calls the Policy server with existing session information.

8. The Policy server returns authorization information to the Validation Library.

9. The Validation Library returns the result to PeopleCode, which sets the PeopleSoft security context to that of the user.

Because PeopleSoft deployments vary, the preceding illustration may not reflect any particular customer’s actual environment. For example, the Optional Application Server might not be present. However, the diagram is representative of most typical deployments.
Chapter 2: Pre-Installation Steps

This section contains the following topics:

- System Requirements (see page 11)
- Determining User Attributes of PeopleSoft Username (see page 12)

System Requirements

The minimum requirements for using the SiteMinder Agent for PeopleSoft are the following:

- SiteMinder Policy server v5.5
- A web server with a SiteMinder Web Agent 5QMRx installed
- PeopleTools 8.19
- PeopleSoft components for web access—typically a WebLogic/WebSphere Application Server, the PeopleSoft servlets and support libraries
- Any necessary components to enable the Web Agent’s web server to serve as a gateway to the PeopleSoft application suite

More information:

http://ca.com/support
Determining User Attributes of PeopleSoft Username

As a pre-installation step, determine the user attributes of the PeopleSoft username.

A user attribute within the directory should contain the user’s existing PeopleSoft username. PeopleSoft’s existing concept of a user remains intact in SiteMinder Agent for PeopleSoft. The existing roles, access permissions, and other user data remain untouched. SiteMinder retrieves a user attribute from the user directory and inserts that value as an HTTP header. Signon PeopleCode retrieves this data, and after verification, provides it to PeopleSoft as the user’s identity.

Because the Signon PeopleCode may be customized, the behavior can be significantly altered. For example, the mapping of a SiteMinder username to a PeopleSoft username could be created in a database table within PeopleSoft. PeopleCode could use that table to retrieve the user’s actual username at signon and alter the call to SetAuthenticationResult to use the new value.
Chapter 3: Installation

This section contains the following topics:

Installing the ERP Agent for PeopleSoft (see page 13)
Configuring SessionLinker (see page 16)
Setting Up SiteMinder 5.x (see page 17)
Setting Up a SiteMinder Response (see page 17)
Create a DEFAULT_USER Account in PeopleSoft (see page 18)
How to Enable the DEFAULT_USER on the Web Server (see page 18)
Install the Validation Library on the PeopleSoft Application Server (see page 19)
Install PeopleCode to PeopleSoft Application Designer (see page 20)
Register PeopleCode for Authentication (see page 21)
Test the Installation (see page 22)
Disabling Existing Account Passwords (see page 22)
Replacing the signon.html File (see page 23)

Installing the ERP Agent for PeopleSoft

Installation is performed using the InstallAnywhere software developed by the Macrovision Corporation.

Installer can be run in the following modes:

- GUI mode for Windows or UNIX platforms
- Console mode for UNIX platforms
Run InstallAnywhere in GUI Mode

Perform the following procedure to run InstallAnywhere in GUI mode.

To run InstallAnywhere in GUI mode

1. Access the executable file in the installation media, and click it. A window appears, with the caption InstallAnywhere is preparing to Install..., and a progress bar shows you the progress of the operation. When InstallAnywhere is loaded, the CA Siteminder ERP Agents v5.6 SP3 Introduction window appears.

   **Note:** It is recommended that you quit all programs before continuing with the installation.

2. Click Next. The License Agreement window appears. Read it.

3. Check the "I accept the terms of the License Agreement" check box, and click Next. The Important Information window appears.

4. Read the INSTALLATION NOTES and the DOCUMENTATION NOTES, and click Next. The Select an ERP Agent to Install window appears.

5. Check the radio button next to PeopleSoft Agent, and click Next. The Finding Installed Software window appears.

   Elements of the PeopleSoft agent must be installed on the following servers:
   - PeopleSoft application server
   - Web server, where the Web Agent has been installed.
   - Policy server

   **Note:** Depending on your configuration, whether the servers are located on the same or on different machines, you will need to run Installer once, twice or three times.

6. Mark the check box(es) next to the relevant software, and click Next. The Choose Install Folder window appears.

7. You must specify the location where you want the PeopleSoft Agent to be installed. A default folder C:\Program Files\CA\erpconn is indicated. You may accept the default folder or click Choose, browse to the required folder and click OK. Click Next. The Pre-Installation Summary window appears.

8. Review your selections, and click Previous to change any of your choices or click Install. The installation takes place. When the installation is complete, the Install Complete window appears; a message indicates that the installation is finished. When errors occur, a relevant message is issued. You can view the installation log for details.

   **Note:** The log indicates the following:
   - Whether the installation succeeded or failed
The number of successes
- The number on non-fatal errors
- The number of fatal errors

9. Click Done to exit InstallAnywhere.

Run InstallAnywhere in Console Mode

Perform the following procedure to run InstallAnywhere in console mode.

**To run InstallAnywhere in console mode**

1. Run the executable installer file from the command line, using the following command:
   ```
   executable name -i console
   ```
   When InstallAnywhere is loaded, the CA Siteminder ERP Agents v5.6 SP3 Introduction window appears.
   
   **Note:** It is recommended that you quit all programs before continuing with the installation.

2. Press Enter to continue. The License Agreement window appears. Read it, pressing Enter as necessary to view the entire license agreement. At the end of the text, the "I accept the terms of the License Agreement" text appears.

3. Enter Y if you accept, and want to continue Installing the ERP Agent, and press Enter to continue. The Important Information window appears.

4. Read the INSTALLATION NOTES and the DOCUMENTATION NOTES, pressing Enter as many times as needed to get to the end of the text. The Select an ERP Agent to Install window appears. The options vary according to your platform. For example, on Windows, the options are as follows:

   1- SAP Web Application Server Agent
   2- PeopleSoft Agent
   3- Siebel Agent
   4- SAP ITS Agent

   You are prompted to ENTER THE NUMBER FOR YOUR CHOICE OR PRESS <ENTER> TO ACCEPT THE DEFAULT, WHICH IS MARKED BY AN ARROW.
5. Enter the number that corresponds to PeopleSoft Agent, and press Enter. The Finding Installed Software window appears.

Elements of the PeopleSoft agent must be installed on the following servers:

1- PeopleSoft application server
2- Web server, where the Web Agent has been installed.
3- Policy server

Note: Depending on your configuration, whether the servers are located on the same or on different machines, you will need to run Installer once, twice or three times.

You are prompted to ENTER A COMMA-SEPARATED LIST OF NUMBERS REPRESENTING THE DESIRED CHOICES OR PRESS <ENTER> TO ACCEPT THE DEFAULT, which is marked by an arrow.

6. Enter your selection, for example, 1,3. The Choose Install Folder appears.

7. You must specify the location where you want the PeopleSoft Agent to be installed. A default folder, Path to your home directory/CA/erpconn, is indicated. You may accept the default folder and press Enter or enter the full path to the required folder. The Pre-Installation Summary window appears.

8. Review your selections, and press Enter to Install. The installation takes place, and a progress bar appears. When the installation is complete, a confirmation message is issued. When errors occur, a relevant message is issued. You can view the installation log for details.

Note: The log indicates the following:

- Whether the installation succeeded or failed
- The number of successes
- The number on non-fatal errors
- The number of fatal errors

9. Press Enter to exit InstallAnywhere.

---

**Configuring SessionLinker**

When you run the installation process for the agent for PeopleSoft, on the web server and/or the Policy server, SessionLinker is also installed. For more information, see *eTrust SiteMinder Agent - SessionLinker Guide*. 
Setting Up SiteMinder 5.x

SiteMinder v5 Web Agents use the Trusted Host model for authenticating themselves. The SiteMinder Agent for PeopleSoft continues to use the agent name and Shared Secret model used in Version 4 and earlier web agents.

When creating an agent for Signon PeopleCode, make sure the Support 4.x agents check box is selected. This check box is available on the dialog box used for creation of an Agent object by the Policy server Admin UI.

Setting Up a SiteMinder Response

Within SiteMinder, create a set of relevant objects to protect the PeopleSoft application. For example, when using WebLogic and IIS, one possible configuration might include the following:

- A realm protector /servlets/iclientservlet.wls/ (For PeopleSoft 8.4x, the realm to be protected can be /psp/). If the web server is not IIS, omit .wls for PeopleSoft 8.1x; for example: /servlets/iclientservlet/.

- A rule for *

- An HTTP header response named PSUSERNAME containing the user’s PeopleSoft Username.

  **Note:** The name of the HTTP header cannot be changed. Changing the name of this header requires changes to both the PeopleCode and the SmPSLoginLib library.

- Configure the SessionLinker response mentioning the PeopleSoft cookie, PS_TOKEN and the WebLogic/WebSphere session cookie. For more information, see *eTrust SiteMinder Agent - SessionLinker Guide*.

  **Note:** The exact value of the WebLogic/WebSphere session cookie name should be the value for the portalServletSessionCookieName parameter in the configuration.properties file of the PIA installation. (For PeopleSoft 8.45 through 8.48 the corresponding filename is config_prop.)

- A policy that grants access to an appropriate set of users and that links the rule described in this section to the correct SiteMinder response.

  For example, if the variable name is PSUSERNAME and the attribute name is PeoplesoftUsername, SiteMinder protects the entire PeopleSoft environment and returns the user’s PeopleSoft username as an HTTP header, named HTTP_PSUSERNAME.
Create a DEFAULT_USER Account in PeopleSoft

The sole purpose of the default user account is for initial communication between PeopleSoft web server and PeopleSoft application server. The default user account enables execution of the Signon PeopleCode, which in turn enables the SiteMinder integration and retrieves the SiteMinder headers, verifies their content, and starts a session. For security reasons, configure this account so that it has no access to the system.

To create the DEFAULT_USER account
1. Invoke PeopleSoft, and navigate to User Profiles.
2. Select Add a New Value, and create a user.
3. In the User ID field, enter DEFAULT_USER.
4. In the Password field, enter the password.
5. Click the Add button.
6. On the ID and Roles tabs, make sure the user does not have access to any data in the system (no privileges and no roles).
7. Save your changes, and exit the PeopleSoft application.

How to Enable the DEFAULT_USER on the Web Server

The procedures for enabling the DEFAULT_USER on PeopleTools are different for versions developed prior to 8.45, and for the later versions.

More information:
PeopleTools Versions 8.1x and 8.42 (see page 18)
PeopleTools Versions 8.45 through 8.48 (see page 19)

PeopleTools Versions 8.1x and 8.42

To enable the DEFAULT_USER, make the following changes on the configuration properties file on the WebLogic/WebSphere Server:

- Change byPassSignOn from false to true.
- Set the default user or operator ID to DEFAULT_USER.
- Set the value of the default password to a long string that will be difficult to enter again.

Restart the WebLogic/WebSphere server to activate these changes.
PeopleTools Versions 8.45 through 8.48

To enable the DEFAULT_USER, modify the following properties on the security page of the web profile configuration:

- Enable the Public Users—Allow public Access property by selecting the check box.
- Set Public Users—User ID property to DEFAULT_USER
- Set Public Users—Password property to a long string that will be difficult to enter again

Restart the WebLogic/WebSphere server to activate these changes.

Install the Validation Library on the PeopleSoft Application Server

The Agent installer writes the Validation Library in the PeopleSoft agent installation folder/bin directory. A 64-bit version of the Validation Library (for use on supported 64-bit UNIX platforms) is installed in the PeopleSoft agent installation folder/bin/64bit directory.

Depending on your platform, the Validation library includes the following files:

- Windows: SMPSLoginLib.dll, LoginLibTester.exe, and smagentapi.dll
- AIX: libSMPSLoginLib.a, LoginLibTester, and libsmagentapi.so
- HPUX: libSMPSLoginLib.sl, LoginLibTester, and libsmagentapi.sl
- Solaris: libSMPSLoginLib.so, LoginLibTester, and libsmagentapi.so
- Linux: libSMPSLoginLib.so, LoginLibTester, and libsmagentapi.so

To install the Validation Library on the PeopleSoft Application Server

Copy the files for your platform to the appropriate location:

- For Windows hosts, to the PeopleSoft Application server folder/bin\server\winx86 subfolder
- For UNIX hosts, to the PeopleSoft Application server folder/bin subfolder
Install PeopleCode to PeopleSoft Application Designer

A file named peoplecode.txt is installed in the PeopleSoft Agent Installation Folder\peoplesoft\PeopleCode folder. The file includes the following:

- Debugging entries, which you can remove before the code is used in a production system
- Declarations for functions included in the Login Library, and a function called SITEMINDER_SSO that makes calls to the library

**To install PeopleCode to PeopleSoft Application Designer**

1. Configure the peoplecode.txt file:
   a. Open peoplecode.txt.
   b. Modify the SITEMINDER_SSO function. Follow the comments (instructions) provided within the function.
   c. Save and close the file.

   **Important:** The changes might affect the site security. CA will not take responsibility for the accuracy or veracity of the PeopleCode if you make changes other than those documented within the existing peoplecode.txt file. For assistance in customizing, contact Customer Support at http://ca.com/support.

2. Start the PeopleSoft Application Designer program.

3. Log in as a privileged user with write permissions to the FUNCLIB_LDAP record.

4. Open the Open Object window and specify the following:
   - Object Type: Record
   - Name: FUNCLIB_LDAP

5. Click Open.

6. Select the LDAP Auth row, click the right mouse button, and select View PeopleCode.

7. Append the contents of the peoplecode.txt file to the end of the existing PeopleCode source code.

8. Click Save and exit from the Application Designer.


**More information:**

[Registering PeopleCode for Authentication](#) (see page 21)
Register PeopleCode for Authentication

Registering PeopleCode enables the SITEMINDER_SSO function.

**To register PeopleCode for authentication**
1. In the PeopleSoft program, navigate to SignOn PeopleCode.
2. Select the Invoke as user signing in radio button.
3. Add a new row and enter the specified information in the following fields:
   - Enabled: checkmark
   - Record: FUNCLIB_LDAP
   - Field Name: LDAPAUTH
   - Event Name: FieldDefault
   - Function Name: SITEMINDER_SSO
   - Exec Auth Fail: Leave blank (no checkmark)
4. Click Save, and log out of PeopleSoft.

**More information:**

Install PeopleCode to PeopleSoft Application Designer (see page 20)
Test the Installation

Access to PeopleSoft through the existing signon.html page should be blocked. Before replacing this page, test the integration (installation).

**To test the installation**

1. Access the PeopleSoft application through the startup page by using the command start. For example, open one of the following URLs:

   For PeopleSoft 8.1x
   
   http://peoplesoft.acme.com/servlets/iclientservlet.wls/peoplesoft8/?cmd=start
   
   For non-IIS web servers, omit the .wls from the above URL.

   For PeopleSoft 8.4x
   
   http://peoplesoft.acme.com/psp/ps/?cmd=start

2. At the SiteMinder login screen, enter the SiteMinder user credentials.

   After you login to SiteMinder, access to PeopleSoft should immediately be granted.

If, at any time, PeopleSoft prompts for credentials, some portion of the integration is not operating correctly.

**More information:**

[Troubleshooting](#) (see page 25)

Disabling Existing Account Passwords

Because existing accounts are not blocked from logging into PeopleSoft in Tier 2 mode or through some other mechanism, you should lock out passwords for accounts accessing PeopleSoft through the web. See PeopleSoft documentation for assistance in this process.
Replacing the signon.html File

To prevent users from attempting to sign on to PeopleSoft through existing bookmarks, replace the existing signon.html. Installer installs sample signon.html files (signon_81x.html for PeopleSoft 8.1x and signon_84x.html for PeopleSoft 8.4x) in the PeopleSoft Agent Installation folder\peoplesoft\Documentation folder. These files provide the existing warnings and error messages, while removing the username and password prompts.

Replace the existing file with the relevant sample signon file after renaming it signon.html or configure the system to use the new file.
Chapter 4: Troubleshooting and Messages

This section contains the following topics:

- **Verify SiteMinder Policies** (see page 25)
- **Checking the Web Agent Log** (see page 26)
- **Examining PeopleCode Logs** (see page 26)
- **Examining the Library Logs** (see page 29)

## Verify SiteMinder Policies

Perform the following procedure to verify the SiteMinder policies.

**To verify the SiteMinder policies**

1. Start the SiteMinder Test Tool through the Policy server, as follows:
   - Start, Programs, SiteMinder, SiteMinder Test Tool
2. Enter the correct Agent name, Shared Secret, and IP address. Click Connect.
3. Enter the correct resource (For PeopleSoft 8.1x, `/servlets/iclientservlet.wls/peoplesoft8/?cmd=start` and for PeopleSoft 8.4x, `/psp/ps/?cmd=start`), the action GET, and click IsProtected.
   - **Note:** For PeopleSoft 8.1x on non-IIS web servers, omit the .wls from the URL.
4. Enter a valid SiteMinder username and password, and click IsAuthenticated.
5. Click IsAuthorized.

**Note:** If a red indicator appears or the PSUSERNAME and/or NPSSessionLinker responses do not appear in the Attributes box, examine the SiteMinder Policy server configuration and logs. The PSUSERNAME response should hold a valid PeopleSoft username.
Checking the Web Agent Log

If the web browser shows a 500 Server Error page, or if the web browser continuously returns to the login page, check the Web Agent log.

For a solution to these problems see CA eTrust SiteMinder Agent Guide. Further diagnosis is beyond the scope of this document, but an examination of the Web Agent log file might reveal the solution.

Examining PeopleCode Logs

The PeopleCode logs six stages during a successful authentication, as shown in the following table. The stage numbers are not actually called out in the log.

<table>
<thead>
<tr>
<th>Stage</th>
<th>Log Text</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Calling SmSSOSetLogging</td>
<td>PeopleCode is making its first call to the Validation Library (SMPSLoginLib). This is intended as a checkpoint to indicate that PeopleCode has been called, and is attempting to do its work.</td>
</tr>
<tr>
<td>2</td>
<td>Done calling DLL</td>
<td>PeopleCode has succeeded in calling the first DLL entry point, indicating that it has located, loaded, and used the DLL.</td>
</tr>
<tr>
<td>3</td>
<td>Authentication request received for DEFAULT_USER...</td>
<td>A login attempt has occurred for SiteMinder integration, thus the remaining PeopleCode should be run.</td>
</tr>
<tr>
<td>4</td>
<td>Checking user KC0003</td>
<td>PeopleCode is checking the validity of the user who just attempted to log in.</td>
</tr>
<tr>
<td>5</td>
<td>User KC0003 OK with SiteMinder</td>
<td>The Validation Library has indicated that the information provided matches the expected values and that the login attempt should be allowed.</td>
</tr>
</tbody>
</table>
Examining PeopleCode Logs

Not Reaching Stage 1 (No log file)

If no log file is created, check the following:

- Is PeopleCode in the correct record? See the following steps:
  - Step 4 in Installing PeopleCode to the Application Designer (see page 20)
  - Step 3 in Registering PeopleCode for Authentication (see page 21)
- Does PeopleCode open an appropriate log file? If not, check the log file path and make sure it is valid and the folder exists.

Not Reaching Stage 2

Reaching this stage means that PeopleCode is being called when a user logs in. If no further entries appear in the log, the PeopleSoft application server probably cannot locate the Validation Library. Verify that the Validation Library is installed in the correct directory and that you have followed all steps listed in the readme.txt file, which is included in the distribution kit.

More information:

Installing the Validation Library on the Application Server
Not Reaching Stage 3

Stage 3 indicates that an authentication attempt has been received for the user DEFAULT_USER. If the Stage 3 entry does not appear in the log file, make sure the default user is enabled.

More information:

Enabling the DEFAULT_USER on the Web Server (see page 18)

Not Reaching Stage 4

If the text Failed to get header PSUSERNAME appears instead of the text Checking user, the SiteMinder HTTP header response PSUSERNAME does not appear in the HTTP request. Verify the SiteMinder response through the use of the SiteMinder Test Tool and the SiteMinder Web Agent log files.

More information:

Verifying SiteMinder Policies (see page 25)

Not Reaching Stage 5

If the following text appears, Login Library is unable to verify the user’s session information:

User XXX, session ... not acceptable... rejecting

Examine the Login Library log file for any indication of configuration problems.

More information:

Examining the Library Logs (see page 29)

Not Reaching Stage 6

If the PeopleSoft application server does not reach Stage 6, it may have crashed between Login Library’s successful response and the end of the SITEMINDER_SSO function. Examine PeopleCode for a potential cause, which is likely to be something external to any of the PeopleSoft agent binaries.
Examining the Library Logs

PeopleCode contains the function SmSSOSetLogging, which takes two parameters:

- An integer indicating the logging level (from 0 to 4) with higher numbers indicating larger amounts of information
- The path to a log file

Log Levels

The following table shows the log level parameter values along with their meanings and indicators.

<table>
<thead>
<tr>
<th>Level</th>
<th>Log Indicator</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>No indicator; no log file</td>
<td>None; the log file is off</td>
</tr>
<tr>
<td>1</td>
<td>ERR</td>
<td>Errors only; errors in initialization and communication are logged</td>
</tr>
<tr>
<td>2</td>
<td>INF</td>
<td>Informational; at this level information indicating the root cause of the problem is shown. The specific cause of the problem will probably not appear.</td>
</tr>
<tr>
<td>3</td>
<td>DBG</td>
<td>Debug; information not typically useful in production environments.</td>
</tr>
<tr>
<td>4</td>
<td>XXX</td>
<td>Extra; the information shown is intended as an aid in locating problems in the Login Library code itself, and is not intended for non-Computer Associates personnel.</td>
</tr>
</tbody>
</table>
Determine the Level to Set

Perform the following procedure to determine the level to set.

To determine the level to set

1. Set the log level to 2 and examine the logs. The most common problems reported to SiteMinder are the result of errors in the configuration of the Policy server IP agent name and shared secret. At log level 2 many of these errors will appear and the solution will be obvious— for example a typical error is “Failed to connect agent - check shared secret and agent name,” implying that the agent name or shared secret is the likely root cause of the problem.

2. Increase the log level to 3 and examine the logs. When the problem’s cause does not appear under log level 2 and the only error text appearing is “Session not valid - returning –1,” log level 3 will reveal additional information, including the cause.
Appendix A: NPSEncrypt and NPSVersion Tools

This section contains the following topics:

NPSEncrypt Tool (see page 31)
NPSVersion Tool (see page 33)

NPSEncrypt Tool

Sometimes, secret values must be stored in a configuration file. For security purposes, you might want to encrypt and store the encrypted form of these secret values. To do this, use the NPSEncrypt tool. When a setting allows encrypted values to be used, this product decrypts it before use. If the setting is not encrypted, the value entered will be used as is.

The NPSEncrypt utility takes plain text entered on the command line, encrypts it, and prints the result on the screen. The resulting encrypted text can be cut and pasted wherever it is needed.

A product that allows an encrypted value automatically decrypts it when needed.

To encrypt a value, use the command prompt and type the NPSEncrypt command followed by a space and followed by the text to be encrypted:

```
C:\>npsencrypt secret
[NPSEncrypt Version 1.1 - NPSEncrypt Revision 1]
[NDSEnc-B]CKtyevyWkrF24Aj9Ly+xEQ==
```

In this case the encrypted form of secret is:

```
[NDSEnc-B]CKtyevyWkrF24Aj9Ly+xEQ==
```

When you copy and paste, grab the entire line, including [NDSEnc-].
NPSEncrypt will encrypt the same text to many different cipher text values. Use any of the values, for example:

C:\>npsencrypt secret
[NPSEncrypt Version 1.1 - NPSEncrypt Revision 1]
[NDSEnc-C]iQ02KvRN2f4tMwjtgRYQ==
C:\>npsencrypt secret
[NPSEncrypt Version 1.1 - NPSEncrypt Revision 1]
[NDSEnc-C]FWhVC+MiA7aNnA87szw76g==
C:\>npsencrypt secret
[NPSEncrypt Version 1.1 - NPSEncrypt Revision 1]
[NDSEnc-B]PD24A2tz6H+KeDh74zUlg==
NPSVersion Tool

Use the NPSVersion tool to extract version information from many Computer Associates products. To use this tool, type the NPSVersion on a command line followed by a space and the name of the executable whose version information you want, for example:

```
C:\> NPSVersion sessionlinkd
[NPSVersion Version 1.0 - NPSVersion Revision 1]
sessionlinkd - Package: NPSSessionLinker V1.3
sessionlinkd - Component: SessionLinker daemon V1.3.2 (Jul 14 2003 20:26:16)
sessionlinkd - Platform: AIX
C:\>
```

**Package**

Refers to the version of Product, in this case the SessionLinker version 1.3 product.

**Component**

Refers to the actual part of the product that is enclosed within this specific file. It is not uncommon for this version number to be larger than the **Package** version. This is usually due to **Component** having one of more bugs repaired or minor enhancements added that did not require the entire Package to be rebuilt or renumbered.

You may use the NPSVersion tool on one platform to extract information for a product built for any other platform. The actual information displayed might differ in format and content from what is shown above, but the relevant lines when discussing any issues with Support are Package and Component. Each line includes a version number.
Index

A
Architecture • 9

B
Background • 7

C
CA Product References • iii
Checking the Web Agent Log • 26
Configuring SessionLinker • 16
Contact Technical Support • iii
Create a DEFAULT_USER Account in PeopleSoft • 18

D
Determine the Level to Set • 30
Determining User Attributes of PeopleSoft Username • 12
Disabling Existing Account Passwords • 22

E
Examining PeopleCode Logs • 26
Examining the Library Logs • 29

H
How to Enable the DEFAULT_USER on the Web Server • 18

I
Increased Security with Tier 2 Integration • 8
Install PeopleCode to PeopleSoft Application Designer • 20
Install the Validation Library on the PeopleSoft Application Server • 19
Installation • 13
Installing the ERP Agent for PeopleSoft • 13

L
Log Levels • 29

N
Not Reaching Stage 1 (No log file) • 27
Not Reaching Stage 2 • 27
Not Reaching Stage 3 • 28
Not Reaching Stage 4 • 28
Not Reaching Stage 5 • 28
Not Reaching Stage 6 • 28
NPSEncrypt and NPSVersion Tools • 31
NPSEncrypt Tool • 31
NPSVersion Tool • 33

O
Overview and Architecture • 7

P
PeopleTools Versions 8.1x and 8.42 • 18
PeopleTools Versions 8.45 through 8.48 • 19
Pre-Installation Steps • 11

R
Register PeopleCode for Authentication • 21
Replacing the signon.html File • 23
Run InstallAnywhere in Console Mode • 15
Run InstallAnywhere in GUI Mode • 14

S
Setting Up a SiteMinder Response • 17
Setting Up SiteMinder 5.x • 17
System Requirements • 11

T
Test the Installation • 22
Tier 1 • 8
Tier 2 • 8
Troubleshooting and Messages • 25

V
Verify SiteMinder Policies • 25