



Value-Added Module (VAM)

PeopleSoft VAM Deployment Guide

Copyright information

®

©2020. SecureAuth is a registered trademark of SecureAuth Corporation. SecureAuth's Identity Platform software, appliances, and other products and solutions are copyrighted products of SecureAuth Corporation.

Document revision history

Version	Date	Notes
0.1	2017-03-16	Initial draft
1.0	2018-05-25	First draft completed
2.1	2018-09-25	Second version, largely rewritten
2.2	2019-01-11	Fixes, enhancements, deployment changes
2.2.1	2019-04-10	Fixes, enhancements, deployment changes
2.2.1.1	2019-05-06	Enhancement, Login UserID Capitalization is configurable
2.3	2019-09-20	Enhancement, AES 128 Encryption/Decryption algorithm
2.3.1	2020-02-18	Reformat, edits

For information on support for this module, contact your SecureAuth support or sales representative:

Email: support@secureauth.com
insidesales@secureauth.com
 Phone: +1-949-777-6959 +1-866- 859-1526
<https://www.secureauth.com/support>
 Website: <https://www.secureauth.com/contact>

ii

Contents

Introduction	1
Prerequisites	1
Deploy and configure PeopleSoft.....	1
Import a project file	2
Create the Anonymous Login user profile	7
Update web profile	10
Define algorithm chains	14
Define algorithm keysets	17
Define encryption profiles.....	20
Test encryption profiles	23
Set up Signon PeopleCode	24
Deploy and configure the SecureAuth appliance.....	27
Set up the SecureAuth realm	27
Deploy the custom PeopleSoft signin.html page	28
Validate the sign-in workflow	29
Perform deep linking.....	31
Troubleshooting	31
References and release notes	32
Reference	33
Release notes	33
Version 2.2.1 – 04/10/2019	33
Version 2.2 – 11/23/2018	33
Version 2.1 – 10/22/2018	33

Version 2.0 – 09/25/2018	33
Upgrade information.....	34

Introduction

This document describes how to deploy and configure the PeopleSoft Value-Added Module (VAM) on a SecureAuth® Identity Platform appliance. Adding the PeopleSoft VAM in your environment will enable authentication and authorization of applications running on PeopleSoft.

All SecureAuth multi-factor authentication (MFA) and Adaptive Authentication capabilities are supported.

The SecureAuth® Identity Platform, released as version 19.07, was formerly called SecureAuth IdP.

Prerequisites

The PeopleSoft VAM and documentation are compatible with the following systems:

- PeopleSoft 9.2 and PeopleTools 8.57.07 and later, running on Oracle Linux Server 6.6
 - PeopleSoft must be installed and operational
 - PeopleTools must be configured to support a two-tier connection to complete all required deployment steps. A three-tier connection cannot be used.
- SecureAuth IdP version 9.1 and later; SecureAuth® Identity Platform version 19.07 and later
- Oracle Database 12c (however, all versions compatible with PeopleTools are supported)

The following systems were used to develop and test this VAM:

- PeopleSoft 9.1.
- PeopleTools 8.57
- Tested with PeopleSoft Fluid user interface

Deploy and configure PeopleSoft

Use this document to install, deploy, and configure the VAM by completing the following workflow:

- Import a project file into the PeopleSoft system to support encryption of the username between SecureAuth and PeopleSoft, and to install PeopleCode.
- Create a user profile in PeopleSoft, if needed.
- Update the web profile to accept the new user profile.

- Obtain the encryption key and version used by PeopleSoft for use between systems.
- Configure a SecureAuth realm to validate a credential and redirect the user to the PeopleSoft server for seamless login.

Import a project file

The project file you will import is called PROJECT_SA2FA.

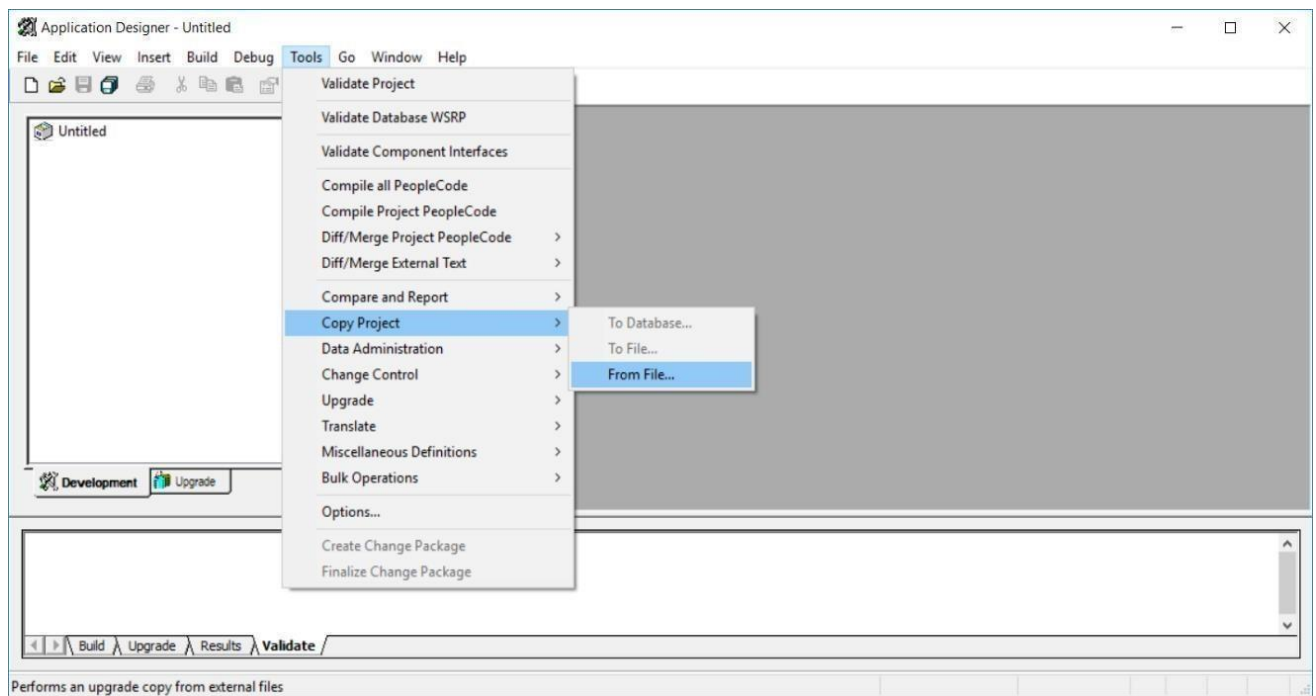
Before starting this task, the PeopleTools Application Designer must be configured to connect to the PeopleSoft database using 2-tier. An application server connection cannot be used for database modifications.

The project contains the following:

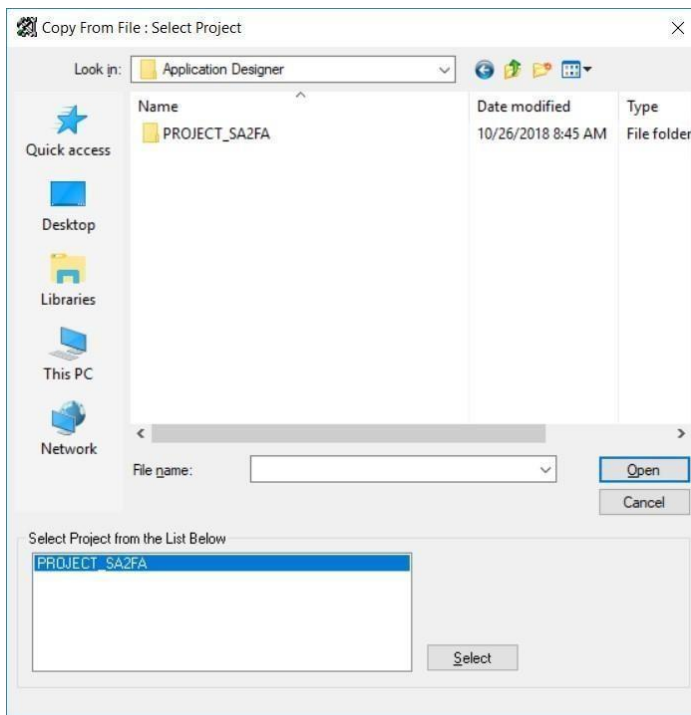
- Record SA_SIGNON.SA_AUTH
This record contains the function Validate_User() used during the login process when an end user is passed by an appliance realm to PeopleSoft.
- Record SA_CONFIGTABLE.SA_CONFIGKEY, SA_CONFIGVALUE
- SQL Query SA_GETCONFIGVALUE
- Fields SA_CONFIGKEY, SA_CONFIGVALUE

1. Log in to the PeopleSoft database using the PeopleTools Application Designer.

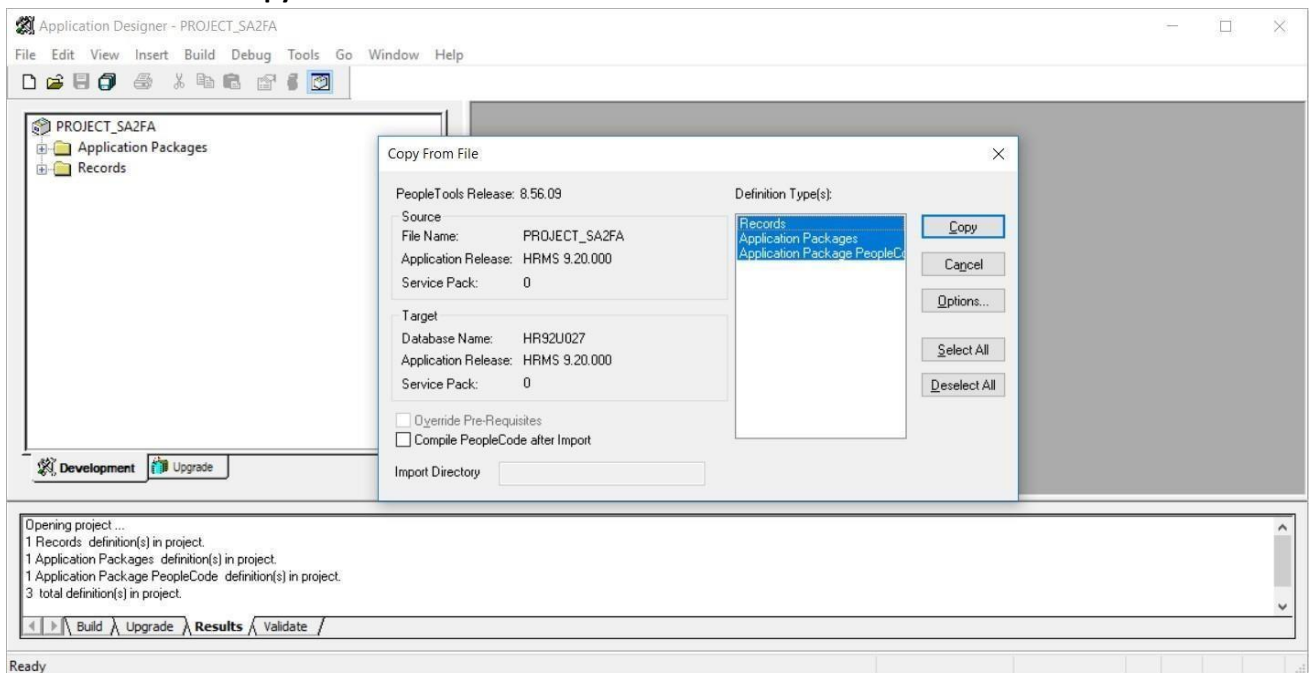
2. Open the Copy from Files dialog box. Select **Tools > Copy Project > From File**



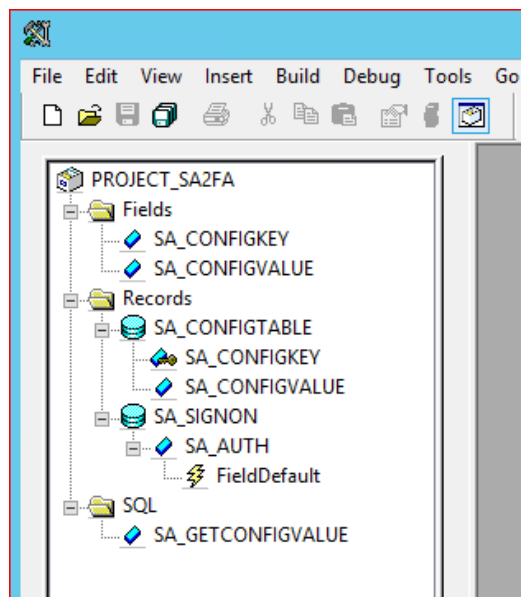
3. Navigate to the location where you extracted the PeopleSoft VAM and open the **\PeopleSoft\Application Designer** subfolder, shown in the following image.
4. Click **PROJECT_SA2FA** and then click the **Select** button.



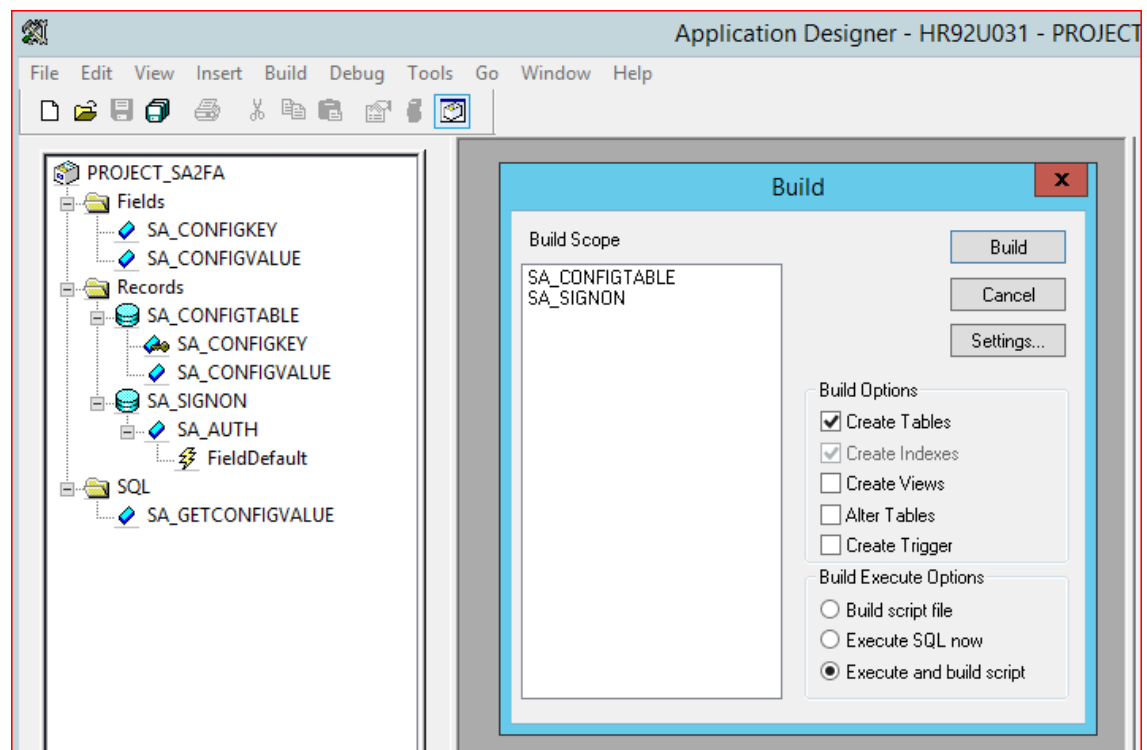
5. Click **Select All** then click **Copy**.



The following image shows the Project after the import.



6. Build the project.



7. Recompile the PeopleCode by clicking **Save**.

PeopleCode is now imported to the PeopleSoft system.

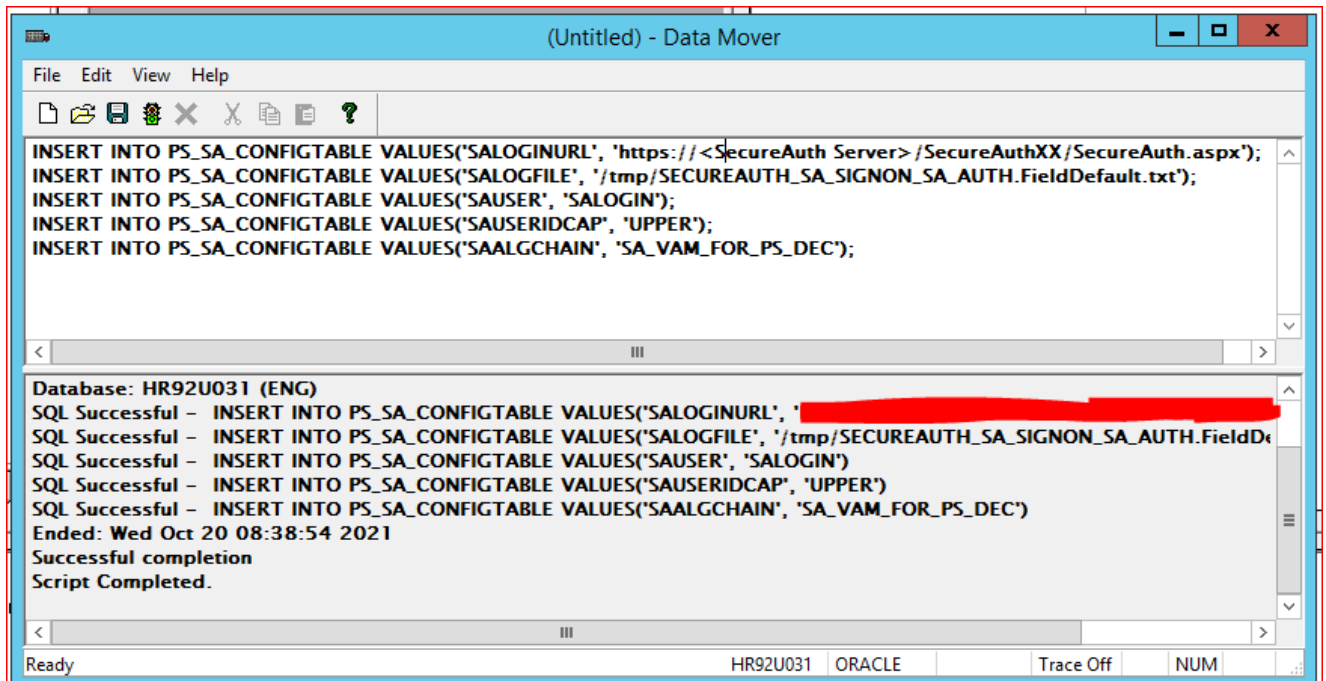
8. Run T-SQL Script to update the following configurable settings for the VAM.

- SALOGINURL: The SecureAuth realm redirect URL
- SALOGFILE: The path and name for the log file
- SAUSER: The anonymous user account. Can be a new or existing user
- SAUSERIDCAP: Accepts "UPPER", "LOWER", "NONE" which indicate how the capitalization of the UserID must be entered.
- SAALGCHAIN: The description algorithm name.

NOTE: UserID in AD or SQL datastores is NOT case sensitive but UserID in PeopleSoft is case sensitive.

Run PeopleSoft DataMover. Open the **PeopleSoft-DataMover-ConfigValues-Script.dms** file, update the script with appropriate values, and run the script.

The **PS_SA_CONFIGTABLE** table, shown in the following image, was created automatically in the Oracle database after the project was built in step 6.

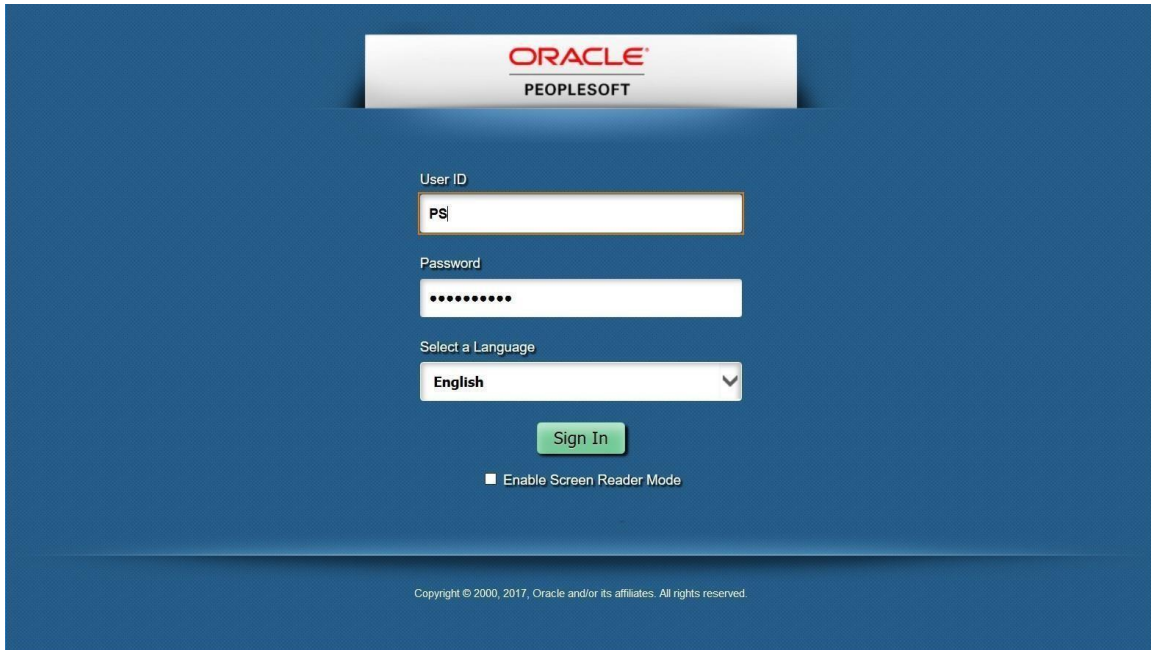


NOTE: **SALOGIN** is used throughout this document as the example name. ID can be any valid username. You will create the ID in the following steps.

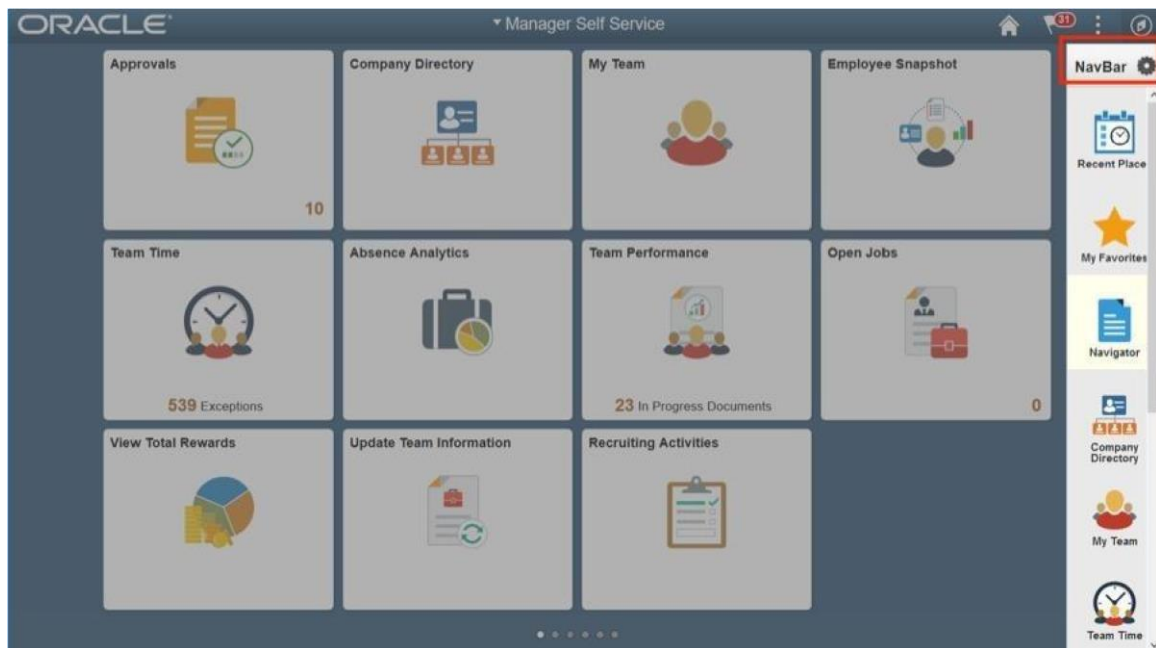
Create the Anonymous Login user profile

Optional: Complete this optional step if an anonymous user is not available for use in the VAM. This is the name of the user that is configured in step 8 for the SAUSER.

1. Log in to PeopleSoft using a web browser.



2. Open User Profiles by clicking the NavBar gear icon at the top right. Select **Navigator > Security > User Profiles > User Profiles**.



- Click the **Add New Value** tab, shown in the following image.



- Enter a username in the **User ID** field. The following example shows **SALOGIN**, but your username will be a unique ID for your organization.
- Add the username by clicking **Add**.

Signon PeopleCode User Profiles

User Profiles

Find an Existing Value Add a New Value

User ID SALOGIN

Add Add (Alt+1)

Find an Existing Value Add a New Value

NOTE: SALOGIN is used throughout this document as the example name. ID can be any valid username. The ID must match the **SAUSER** config value in the PS_SA_CONFIGVALUES table.

6. Enter the password for the new User ID in the **New Password** and **Confirm Password** text fields.

Signon PeopleCode User Profiles

General ID Roles Workflow Audit Links User ID Queries

User ID SALOGIN ☐ Account Locked Out?

Description

Logon Information

Symbolic ID

☐ Password Expired?

User ID Alias

General Attributes

Language English

Currency

Default Mobile Page

Permission Lists

Navigator Homepage Primary

Process Profile Row Security

Save Add Update/Display

General ID Roles Workflow Audit Links User ID Queries

7. Select **None** from the **ID Type** dropdown.

8. Click **Save**.

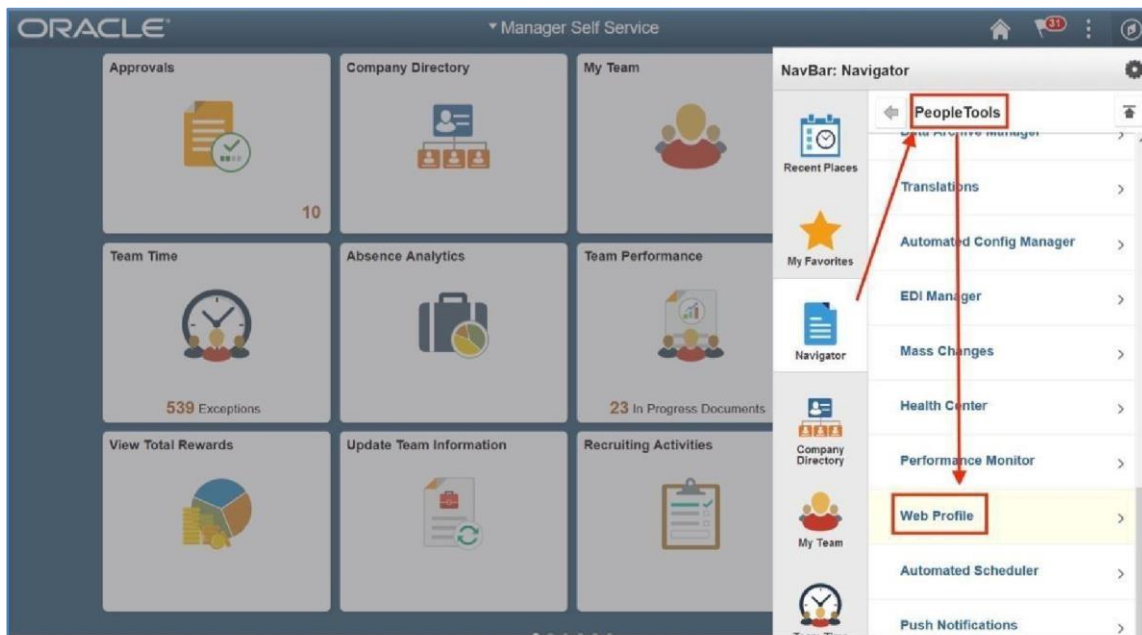
The screenshot shows the 'User Profiles' form in the Signon PeopleCode application. The 'ID Types and Values' section has a table with one row where 'ID Type' is set to 'None'. The 'User Description' section is empty. The 'Save' button is highlighted in orange.

9. If you receive a **Warning – Symbolic ID is missing** message, click **OK** to acknowledge and close the alert.

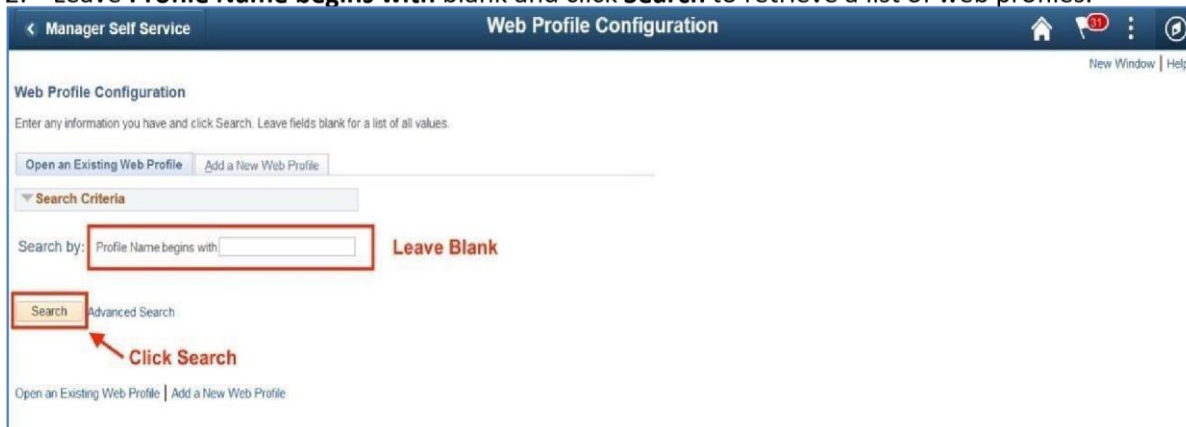
The screenshot shows the 'User Profiles' form with a warning dialog box open. The dialog box title is 'Warning - Symbolic ID is missing.' and it contains the following text: 'A Symbolic ID links a PeopleSoft user with a database-level user. A Symbolic ID is required for the following types of users: Users that make a 2-tier connection using Connect Id / Connect Password authentication. Users who submit jobs via Process Scheduler.' There is a checkbox for 'Do not show this message again' and 'OK' and 'Cancel' buttons. The 'OK' button is highlighted in orange.

Update web profile

1. Open the Web Profile Configuration screen. Select **PeopleTools > Web Profile > Web Profile Configuration**



2. Leave **Profile Name begins with** blank and click **Search** to retrieve a list of web profiles.



3. Select the active web profile.

Manager Self Service **Web Profile Configuration** New Window | Help

Web Profile Configuration

Enter any information you have and click Search. Leave fields blank for a list of all values.

[Open an Existing Web Profile](#) [Add a New Web Profile](#)

Search Criteria

Search by: Profile Name begins with

[Search](#) [Advanced Search](#)

Search Results

View All 1-5 of 5

Profile Name
DEV
KIOSK
PROD
STANDALONE
TEST

[Open an Existing Web Profile](#) [Add a New Web Profile](#)

Select the active profile

NOTE: If you do not know which web profile is active because the location of **configuration properties** (which determines what web profile is used) varies from system to system, you can determine the active web profile by searching **Web Profile History**.

ORACLE **Manager Self Service** New Window | Help

Web Profile

Web Profile Configuration

Web Profile History

Copy Web Profile

Delete Web Profile

Recent Places

My Favorites

Navigator

Company Directory

My Team

Approvals 10

Company Directory

My Team

Team Time 539 Exceptions

Absence Analytics

Team Performance 23 In Progress Documents

View Total Rewards

Update Team Information

Recruiting Activities

4. Click Search.

Manager Self Service **Web Profile History** New Window | Help

Web Profile History

Enter any information you have and click Search. Leave fields blank for a list of all values.

[Find Existing Web Profile History](#)

Search Criteria

Search by: Web Server Name begins with

☐ Case Sensitive

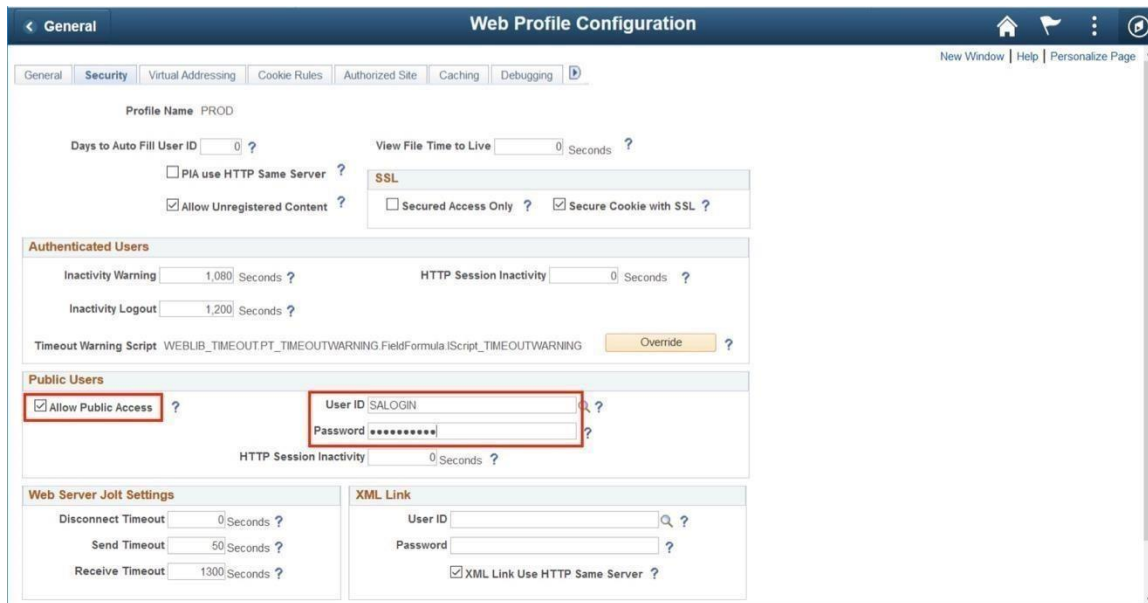
[Search](#) [Advanced Search](#)

The page will refresh with the most recent active profile, shown in the image below.



Note the profile name and return to **Web Profile Configuration** to select the active profile.

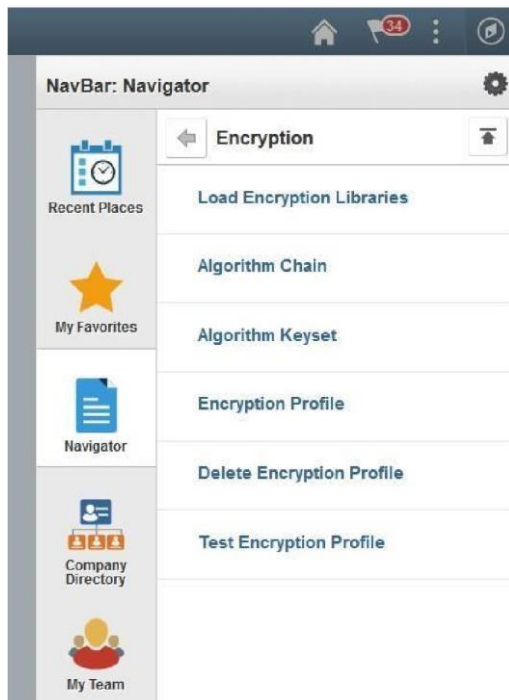
5. In the **Public Users** section, set the **Allow Public Access** checkbox.
6. Type **SALOGIN** in the **User ID** text field.
7. Type the password you previously created for the account into the **Password** text field.
8. Click **Save**.



The image shows the 'Web Profile Configuration' window with the 'Security' tab selected. The 'Profile Name' is 'PROD'. Under 'Authenticated Users', there are fields for 'Inactivity Warning' (1,080 seconds), 'Inactivity Logout' (1,200 seconds), and 'HTTP Session Inactivity' (0 seconds). There is a checkbox for 'Allow Public Access' which is checked. Under 'Public Users', there are fields for 'User ID' (SALOGIN) and 'Password' (masked with asterisks). There are also checkboxes for 'Secured Access Only' and 'Secure Cookie with SSL'. At the bottom, there are 'Web Server Jolt Settings' (Disconnect Timeout, Send Timeout, Receive Timeout) and 'XML Link' settings (User ID, Password, and a checkbox for 'XML Link Use HTTP Same Server').

Define algorithm chains

1. Log in to PeopleSoft and open the Algorithm Chain page. Select **Navigator > PeopleTools > Security > Encryption > Algorithm Chain**.



2. Open Algorithm Chain page

< Manager Self Service

Algorithm Chain

Enter any information you have and click Search. Leave fields blank for a list of all values.

Find an Existing Value **Add a New Value**

▼ **Search Criteria**

Search by: Algorithm Chain ID begins with

Search Advanced Search

[Find an Existing Value](#) | [Add a New Value](#)

3. Add a new value called **AES 128 BASE64 ENCRYPTION** as an algorithm chain ID. Call the algorithm chain ID value anything you want.

< Manager Self Service

Algorithm Chain

Find an Existing Value **Add a New Value**

Algorithm Chain ID

Add

[Find an Existing Value](#) | [Add a New Value](#)

4. Add the required algorithm IDs and set the sequence of use, as shown in the following image.
Save your changes by clicking **Save**.

You need to search algorithm IDs as those are predefine in PeopleSoft.

< Manager Self Service

Algorithm Chain

Algorithm Chain ID: AES 128 BASE64 ENCRYPTION
 Algorithm Chain Description: AES 128 BASE64 ENCRYPTION

Algorithm Chain

Algorithm ID	Sequence		
PSUnicodeToAscii	1	+	-
aes_ks128_cbc_encrypt	2	+	-
base64_encode	3	+	-
PSAsciiToUnicode	4	+	-

5. Add a new value called **AES 128 BASE64 DECRYPTION** as an algorithm chain ID. Call the algorithm chain ID value anything you want.

< Manager Self Service

Algorithm Chain

Algorithm Chain ID: AES 128 BASE64 DECRYPTION

6. Add the required algorithm IDs and set the sequence of use, as shown in the following image.

Save your changes by clicking **Save**.

You need to search algorithm IDs because those are predefined in PeopleSoft.

[← Manager Self Service](#)

Algorithm Chain

Algorithm Chain ID: AES 128 BASE64 DECRYPTION
Algorithm Chain Description: AES 128 BASE64 DECRYPTION

Algorithm Chain

1-4 of 4

Algorithm ID	Sequence		
PSUnicodeToAscii	1	+	-
base64_decode	2	+	-
aes_ks128_cbc_decrypt	3	+	-
PSAsciiToUnicode	4	+	-

[Save](#) [Return to Search](#) [Previous in List](#) [Next in List](#) [Add](#) [Update/Display](#)

Define algorithm keysets

Define encrypt and decrypt algorithm keysets and define a key value for each.

1. Open the Algorithm Keyset page. Select **Navigator > PeopleTools > Security > Encryption > Algorithm Keyset**

[← Manager Self Service](#)

Algorithm Keyset

Enter any information you have and click Search. Leave fields blank for a list of all values.

[Find an Existing Value](#)

▼ **Search Criteria**

Search by: Algorithm ID ▾ begins with

☐ Case Sensitive

[Search](#) [Advanced Search](#)

2. Add an encrypt algorithm keyset.

Type an algorithm ID that begins with **aes_ks128_cbc_encrypt** and click **Search**.

[← Manager Self Service](#)

Algorithm Keyset

Enter any information you have and click Search. Leave fields blank for a list of all values.

[Find an Existing Value](#)

▼ **Search Criteria**

Search by: Algorithm ID ▾ begins with

☐ Case Sensitive

[Search](#) [Advanced Search](#)

3. Add a key value in the **Use Entered Value** field then save your changes by clicking **Save**.

NOTE: The length of the value that you enter depends on the key size of the cipher. For triple DES with a key size of 112, the value length is 16 Bytes. For a key size of 168, it is 24 bytes. Represent the value in hex notation.

You must generate the key value that you enter here. You can use any third-party key generation utility capable of producing hex encoded keys of the required length for the algorithm that you are using.

Using a key generation utility is not a requirement. Alternatively, you can build a hex encoded string manually by stringing together any combination of numbers (0-9) and letters (A-F) of the appropriate length.

Manager Self Service

Algorithm Keyset

Algorithm ID: aes_ks128_cbc_encrypt

Keysets

Keyset ID: AES_128_encrypt

☐ Use Certificate Store Value

Certificate Alias:

☐ Certificate ☐ Private Key

☒ Use Entered Value

Key Value:

0x06B8CD7D5080103B1B9B03F05DFBC0D3

Save Return to Search

4. Add a decrypt algorithm keyset.

Type an algorithm ID that begins with **aes_ks128_cbc_decrypt** and click **Search**.

Manager Self Service

Algorithm Keyset

Enter any information you have and click Search. Leave fields blank for a list of all values.

Find an Existing Value

Search Criteria

Search by: Algorithm ID begins with aes_ks128_cbc_decrypt

☐ Case Sensitive

Search Advanced Search

5. Add a key value in the **Use Entered Value** field then save your changes by clicking **Save**.

[← Manager Self Service](#)

Algorithm Keyset

Algorithm ID aes_ks128_cbc_decrypt

Keysets 🔍 1 of 1 View All

Keyset ID AES_128_decrypt + -

☐ Use Certificate Store Value

Certificate Alias:

☐ Certificate ☐ Private Key

☒ Use Entered Value:

Key Value:

0x06B8CD7D5080103B1B9B03F05DFBC0D3

[Save](#) [Return to Search](#)

Define encryption profiles

1. Open the Encryption Profile page. Select **Navigator > PeopleTools > Security > Encryption > Encryption Profile**

[← Manager Self Service](#)

Encryption Profile

Enter any information you have and click Search. Leave fields blank for a list of all values.

[Find an Existing Value](#) [Add a New Value](#)

▼ **Search Criteria**

Search by: Encryption Profile ID begins with

[Search](#) Advanced Search

[Find an Existing Value](#) | [Add a New Value](#)

2. Add a new encryption profile for **AES 128 BASE64 ENCRYPTION**.

Click **Add a New Value**. Type a name for **Encryption Profile ID**. (The name can be anything you want.)

The screenshot shows the 'Manager Self Service' interface. At the top is a dark blue header with a left arrow and the text 'Manager Self Service'. Below this is the section title 'Encryption Profile'. There are two buttons: 'Find an Existing Value' (light blue) and 'Add a New Value' (green). The 'Add a New Value' button is highlighted. Below the buttons is a text input field labeled 'Encryption Profile ID' containing the text 'SA_VAM_FOR_PS_ENC'. Below the input field is a green 'Add' button. At the bottom of the form, there are two links: 'Find an Existing Value' and 'Add a New Value'.

3. Complete the new profile, filling in the fields as shown in the following image.

← Manager Self Service Encryption Profile

Encryption Profile

Encryption Profile ID SA_VAM_FOR_PS_ENC

Algorithm Chain ID AES 128 BASE64 ENCRYPTION

Description AES 128 BASE64 ENCRYPTION

Parameters		
Algorithm ID	PSUnicodeToAscii	Chain Sequence 1
Algorithm ID	aes_ks128_cbc_encrypt	Chain Sequence 2
<div> <div>Parameter Values</div> <div> <div> <div>Parameter Name</div> <div>IV</div> <div> <input type="checkbox"/> From Keyset </div> </div> <div> <div>Parameter Value</div> <div>0x01020304050607080102030405060708</div> </div> </div> <div> <div>Parameter Name</div> <div>SYMMETRICKEY</div> <div> <input checked="" type="checkbox"/> From Keyset </div> </div> <div> <div>Parameter Value</div> <div>AES_128_encrypt</div> </div> </div>		
Algorithm ID	base64_encode	Chain Sequence 3
Algorithm ID	PSAsciiToUnicode	Chain Sequence 4

4. Add a new encryption profile for **AES 128 BASE64 DECRYPTION**.

Click **Add a New Value**. Type a name for **Encryption Profile ID**. (The name can be anything you want.)

← Manager Self Service

Encryption Profile

Encryption Profile ID SA_VAM_FOR_PS_DEC

Find an Existing Value | Add a New Value

- Complete the new profile, filling in the fields as shown in the following image.

< Manager Self Service
Encryption Profile

Encryption Profile

Encryption Profile ID SA_VAM_FOR_PS_DEC

Algorithm Chain ID AES 128 BASE64 DECRYPTION

Description AES 128 BASE64 DECRYPTION

Parameters 1 of 4

Algorithm ID	PSUnicodeToAscii	Chain Sequence	1
Algorithm ID	base64_decode	Chain Sequence	2
Algorithm ID	aes_ks128_cbc_decrypt	Chain Sequence	3

Parameter Values 1 of 2

Parameter Name IV

Parameter Value 0x01020304050607080102030405060708

☐ From Keyset

Parameter Name SYMMETRICKEY

Parameter Value AES_128_decrypt

☒ From Keyset

Algorithm ID	PSAsciiToUnicode	Chain Sequence	4
--------------	------------------	----------------	---

Save
Return to Search
Previous in List
Next in List
Notify
Add
Update/Display

Test encryption profiles

- Open the Encryption Demo page. Select **Navigator > PeopleTools > Security > Encryption > Test Encryption Profile**
- Select Encryption Profile ID, for example, **SA_VAM_FOR_PS_ENC** or **SA_VAM_FOR_PS_DEC**
- Enter a description of the text to be encrypted in **Text to be Encrypted**.
- Click **Run Encryption Profile**.

The following image shows testing encrypted results.



Encryption Profile

Encryption Demo

Encryption Profile ID:
SA_VAM_FOR_PS_ENC

Run Encryption Profile

Text to be Encrypted:
This is testing

Encrypted Text:
7gg2lGkQ7AnWJG4qXYA19Q==

The following image shows testing decrypted results.



Encryption Profile

Encryption Demo

Encryption Profile ID:
SA_VAM_FOR_PS_DEC

Run Encryption Profile

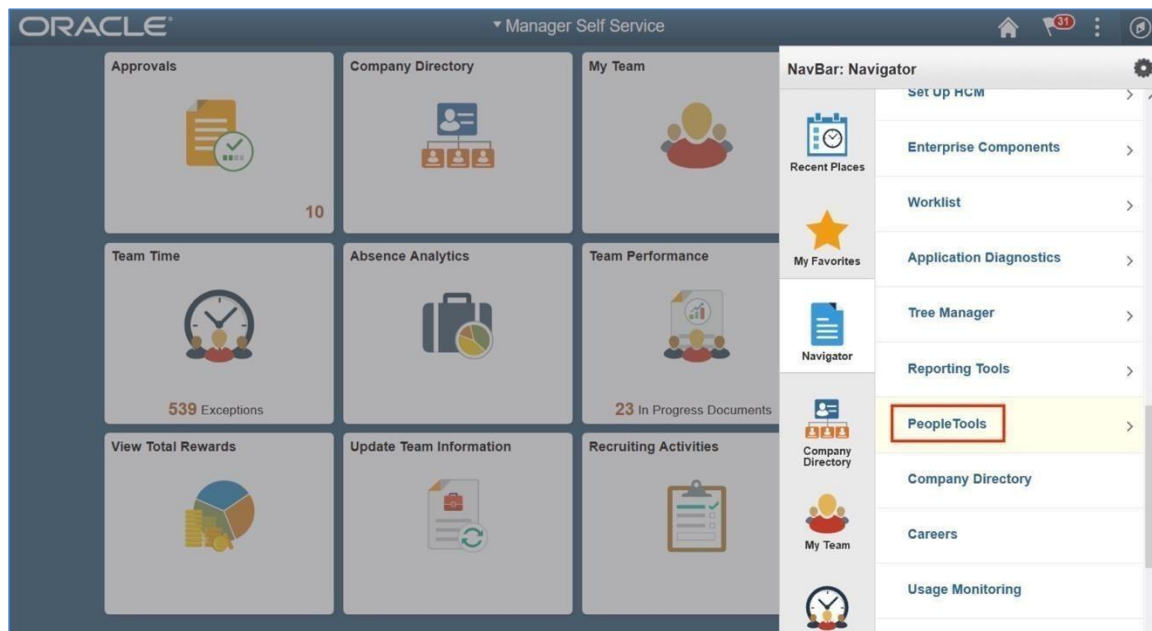
Text to be Encrypted:
7gg2lGkQ7AnWJG4qXYA19Q==

Encrypted Text:
This is testing

Set up Signon PeopleCode

The record associated with PeopleCode must be configured for the Signon PeopleCode page. The code is triggered using the public guest credentials (i.e., SALOGIN). The code must be enabled along with the function **Validate_User()** as shown below.

1. Open the Signon PeopleCode page. Select **PeopleTools > Security > Security Objects > Signon PeopleCode**



2. Add a new row by clicking the + button on the last row to the far right.

Sequence	Enabled	Record	Field Name	Event Name	Function Name	Exec Auth Fail
1	<input type="checkbox"/>	FUNCLIB_PWDCTL	PWDCTL	FieldChange	Password_Controls	<input checked="" type="checkbox"/>
2	<input type="checkbox"/>	FUNCLIB_LDAP	LDAPAUTH	FieldDefault	WWW_Authentication	<input type="checkbox"/>
3	<input type="checkbox"/>	FUNCLIB_LDAP	LDAPAUTH	FieldDefault	LDAP_Authentication	<input checked="" type="checkbox"/>
4	<input type="checkbox"/>	FUNCLIB_LDAP	LDAPAUTH	FieldDefault	SSO_Authentication	<input type="checkbox"/>
5	<input type="checkbox"/>	FUNCLIB_LDAP	LDAPAUTH	FieldDefault	LDAP_ProfileSynch	<input type="checkbox"/>
6	<input type="checkbox"/>	FUNCLIB_LDAP	LDAPAUTH	FieldDefault	OAMSSO_AUTHENTICATION	<input type="checkbox"/>

- Enter the next incremental value available in **Sequence**. In this example, the number 7.
- Type **SA_SIGNON** in the **Record** text field; it should auto-complete as you type.
- Type **SA_AUTH** in the **Field Name** text field.
- Type **FieldDefault** in the **Event Name** text field.

- e. Type **Validate_User** in the **Function Name** text field.
- f. Set the **Exec Auth Fail** checkbox.
- g. Save your changes by clicking **Save**.

Signon PeopleCode

Signon

☒ Invoke as user signing in

☐ Invoke as User ID: Password:

*Sequence	Enabled	*Record	*Field Name	Event Name	Function Name	Exec Auth Fail
7	<input checked="" type="checkbox"/>	SA_SIGNON	SA_AUTH	FieldDefault	Validate_User	<input checked="" type="checkbox"/>

Save Refresh

PeopleSoft Server pages restriction

Because of copyright restriction, SecureAuth Corporation cannot provide documentation that outlines modifications to PeopleSoft pages that redirects users to a SecureAuth appliance for the expire.html, signon.html, signin.html, and start.html pages, to bypass the standard PeopleSoft user sign-on experience. Consult Oracle Corporation for assistance with modifying these pages.

The Oracle Corporation software documentation license agreement is provided for your convenience.

```
<!-- Copyright (c) 2000, 2013, Oracle and/or its affiliates. All rights reserved. --> <!--
* *****
* This software and related documentation are provided under a
* license agreement containing restrictions on use and
* disclosure and are protected by intellectual property
* laws. Except as expressly permitted in your license agreement
* or allowed by law, you may not use, copy, reproduce,
* translate, broadcast, modify, license, transmit, distribute,
* exhibit, perform, publish or display any part, in any form or
* by any means. Reverse engineering, disassembly, or *decompilation of this software, unless
* required by law for *interoperability, is prohibited. *The information contained herein
* is subject to change without
* notice and is not warranted to be error-free. If you find any *errors, please report them
* to us in writing. *
* Copyright (C) 1988, 2017, Oracle and/or its affiliates.
* All Rights Reserved.
* ***** -->
```

Deploy and configure the SecureAuth appliance

Use the following instructions to do the following:

- Set up the SecureAuth realm
- Deploy the custom PeopleSoft Signin.html
- Validate the workflows
- Perform deep linking
- Troubleshoot

Set up the SecureAuth realm

1. Follow default rules for defining the **Data** and **Workflow** information for the realm.
2. Copy the files **PeopleSoft.aspx** and **PeopleSoft.aspx.vb** located under \SecureAuth from the decompressed .zip file to the SecureAuth Identity Platform realm to be used for SSO into PeopleSoft.
For example, copy the files to D:\SecureAuth\SecureAuth1\Customized.
3. On the Post Authentication page of the PeopleSoft realm, select **Use Custom Redirect** from the **Authenticated User Redirect** dropdown.
4. Assign the page **Customized/PeopleSoft.aspx** in the **Redirect To** text box.

The screenshot shows the SecureAuth4 administration console. The top navigation bar includes links for Overview, Data, Workflow, Adaptive Authentication, Multi-Factor Methods, Post Authentication (selected), API, Logs, System Info, and Logout. The left sidebar shows the 'SecureAuth4' section with 'Custom Groups' set to 'All' and a list of realms: SecureAuth0 (SecureAuth Administration), SecureAuth1 (PeopleSoft), and SecureAuth998 (OATH Enrollment). The main content area is divided into three sections: 'Post Authentication', 'Password Reset', and 'Multi-Factor App Enrollment'. In the 'Post Authentication' section, 'Authenticated User Redirect' is set to 'Use Custom Redirect', and the 'Redirect To' field is 'Customized/PeopleSoft.aspx'. The 'Password Reset' section has a link to 'Configure password reset page'. The 'Multi-Factor App Enrollment' section has 'OATH Options' with 'OATH Seed or Token' set to 'OATH Seed (Single)', 'One Time Provisioning' set to 'False - Reuse same seed', 'Show OTP on enrollment page' set to 'False', and 'Passcode Length' set to '6 digits'.

5. Update the realm settings (web.config) to include the following settings. Do **not** replace <appSettings>.

```
<appSettings>
/* obtained from PeopleSoft server. see deployment guide */
<add key="PSVersion" value="{V2.1}" />
/* obtained from PeopleSoft server. see deployment guide */
<add key="PSKey" value="" />
<add key="PSIV" value="" />
<add key="PSRedirectURL"
value="http://<<FQDN>>:<<port>>/psc/ps/EMPLOYEE/HRMS/c/NUI_FRAMEWORK.PT_LANDINGPAGE.GBL?" />
/* the default PeopleSoft signon URL, where users can NOT be redirected to */
<add key="PSSignIn" value="http://<<FQDN>>/psc/ps/" />
</appSettings>
```

Deploy the custom PeopleSoft signin.html page

Copy and replace the custom signin.html page to the default sign-in path in PeopleSoft. The following is an example path in a Linux server.

```
/home/psadm2/psft/pt/8.56/webserv/peoplesoft/applications/peoplesoft/PORTAL.war/WEB-INF/psftdocs/ps
```


This page has a custom JavaScript code that initiates the auto-redirect to the SecureAuth login page. Update the psTarget URL as needed. The script supports deep linking within PeopleSoft if the saRedirect variable is populated properly. If not, the default value noted as psTarget is used to build the correct redirect URL to SecureAuth.

```
<script language="JavaScript">    var sDomain
=
"<%=AuthTokenDomain%>";    try {
        document.domain = "<%=AuthTokenDomain%>";
    }
    catch (err) {};

    var saRedirect = "<%=error%>";    var
psTarget =
"https://yourdomain.com
/psc/HRPRDES/EMPLOYEE/HRMS/s/WEBLIB_PTBR.ISCRIPT1.FieldFormula.IScript_StartPage";

    if(!saRedirect) {        saRedirect =
"https://yourdomain.com/secureauth1/secureauth.aspx?RedirectUrl=" + encodeURIComponent(psTarget);
    }

    top.location.href = saRedirect;

</script>
```

Validate the sign-in workflow

1. Open a browser and navigate to the SecureAuth realm used for PeopleSoft, for example, <https://localhost/secureauth1/secureauth.aspx>
2. Log in with the user account to use to verify the sign-in workflow. In the following example, GMILES is the user account to be verified and it is added in the **Username** text field.

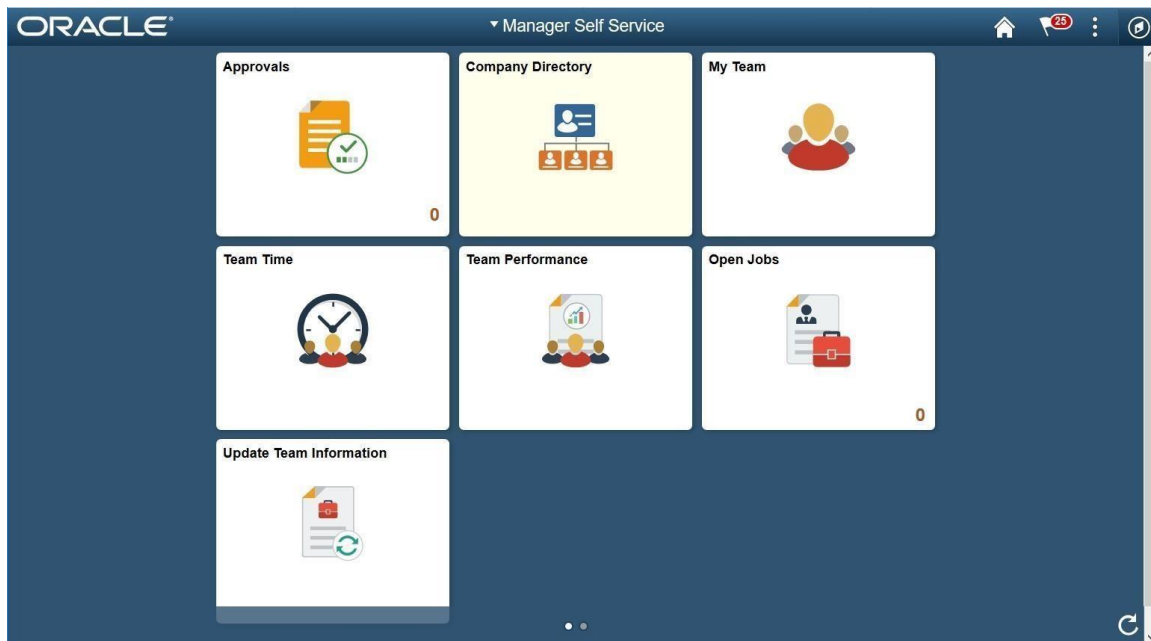
This account must be a valid account that is in the user store configured for the realm and accessible by the PeopleSoft system database.



The image shows a web browser window displaying the SecureAuth login page for PeopleSoft. At the top is the SecureAuth logo. Below it, the text "PeopleSoft" is centered. A message reads: "Please select the 'Public Computer' option if this is not a machine you use regularly, then enter your User ID below and click 'Submit' to access the system." There are two radio buttons: "This is a public computer" (unselected) and "This is a private computer" (selected). Below the radio buttons is a text input field labeled "Username:" containing the text "GMILES". The input field has a red rectangular border. To the right of the input field is a small "X" icon. Below the input field is a blue "Submit" button. At the bottom of the page, there is a "Restart Login" link and a copyright notice: "Copyright 2018 SecureAuth Corp. All rights reserved."

3. The browser will redirect to PeopleSoft and log the user in, arriving at the page specified in the **PSRedirectURL** configuration of the realm.

The following image is an example of the home page for user GMILES, which was verified by the SecureAuth realm after redirection from SecureAuth and successful login to PeopleSoft.



Perform deep linking

The SecureAuth appliance realm can redirect a user to a page other than the default landing page specified in the web.config entry described earlier. This is often used, for example, for portal links or personalized links users might receive in an email to review a specific report. This functionality is built into the post-authentication page installed earlier in this document.

- Default behavior

By default, all users will be redirected to the landing page specified in **PSRedirectUrl**.

- Linking behavior

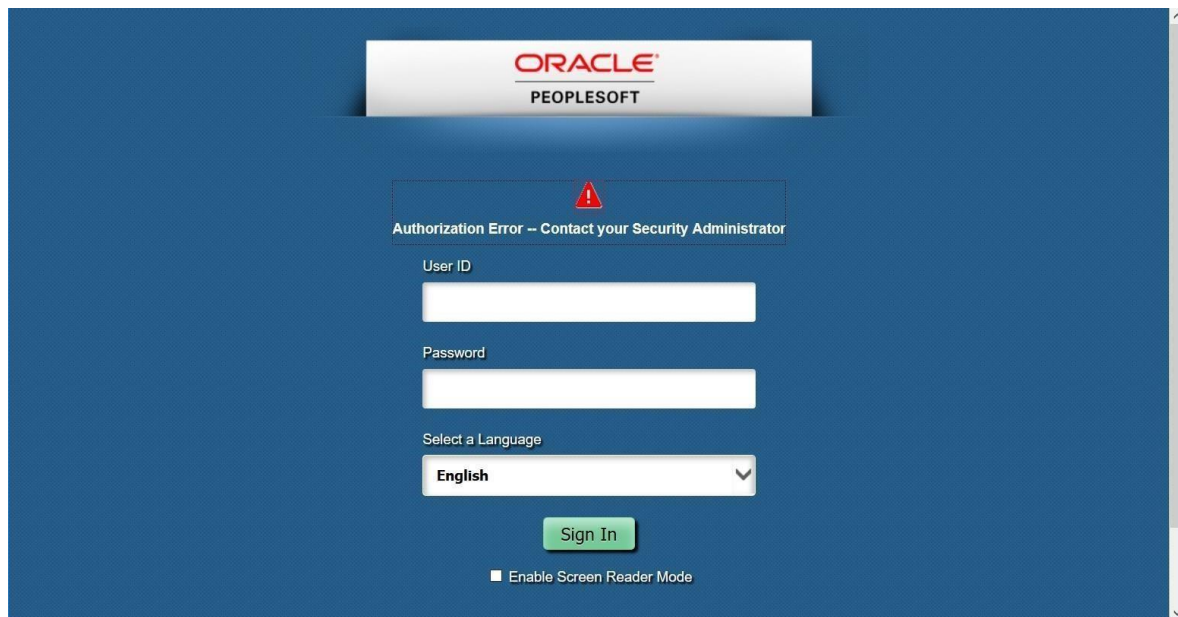
To support redirecting a user to a specific page other than the default, when formatting a published link to PeopleSoft, format the URL to point to the appliance realm and append the parameter **RedirectUrl URL Encoded**. The following example shows a link set up in this way:

`http://secureauthserver/realmnumber/secureauth.aspx?RedirectUrl=`

`https%3A%2F%2Fpeoplesoftserver%2Fspecificpage%3Foptionalparamter1%3Dvalue%26optionalparamter2%3Dvalue`

Troubleshooting

If an error is encountered during the process, the screen below is displayed.



For further information about troubleshooting, the log file will outline the cause of the error (as outlined below):

1. If you experience any difficulty, close all browser sessions and attempt the workflow again. If this does not solve the issue, restart the PeopleSoft system.
2. Credential validation is handled by standard SecureAuth realm functionality. Contact SecureAuth Technical Support if you encounter an issue with logging a user in at the SecureAuth realm level.
3. If you encounter the issue noted above where the user is logged in as **SALOGIN**, contact SecureAuth Technical Support.

Arrange for an online support session with your local PeopleSoft administrator that has access to PeopleSoft administrative functions and has access to the operating system file system to retrieve log files.

The log file for Signon PeopleCode is available in the **Validate_User** function described earlier in this document. A copy of the audit can be retrieved. By default, the file name will be *SECUREAUTH_SA_SIGNON_SA_AUTH.FieldDefault.txt*.

References and release notes

The reference details Oracle documentation for sign-on and user exits. The release notes track all significant changes from the most recent to older.

Reference

- Oracle: Employing Signon PeopleCode
https://docs.oracle.com/cd/E26239_01/pt851h3/eng/psbooks/tsec/chapter.htm?File=tsec/htm/tsec09.htm

Release notes

Version 2.2.1 – 04/10/2019

- Enhancement: all the settings are configurable using a table in the database.
- Enhancement: PeopleSoft project updated to include all the objects, no further PeopleCode change is needed.
- Enhancement: SALOGIN and the WebprofileUser is a configurable value.
- Enhancement: LOG file name and path is configurable and has more details for troubleshooting.
- Fix: issues with deep linking in PSC vs PSP pages, default redirect as a fall back mechanism.

Version 2.2 – 11/23/2018

- Fix: PeopleCode was calling Error before logging, resulting in some error conditions not being included in the audit file.
- Fix: Deep link feature was truncating parameters.
- Fix: Log file was not being closed at the end of Validate_User.
- Maintenance: Explicitly defined all variables in PeopleCode.
- Enhancement: Switched to form POST to send user credentials to PeopleSoft.
- Enhancement: Post-authentication page now supports User ID mapping based on realm configuration.

Version 2.1 – 10/22/2018

- Fix: Expiry tolerance now supports +/- between servers instead of only +.
- Enhancement: Added support for redirection after login to support deep links.

Version 2.0 – 09/25/2018

- Enhancement: Replaced secure cookie with querystring parameter to support both on-premises and SaaS implementations.
- Enhancement: Added support for SP-Initiated workflow so when a user enters their credentials at a PeopleSoft login they will be redirected to SecureAuth.
- Enhancement: Added expiration to encrypted token.
- Maintenance: Redesigned the PeopleCode distribution to use a new Record instead of adding to FUNCLIB_LDAP2 for PeopleCode Signon.

Version 1.0 – 6/15/2018

Initial release supporting IdP-Initiated from SecureAuth to PeopleSoft using a secure cookie for authentication.

Upgrade information

Before upgrading SecureAuth software, open a Support ticket. The process of upgrading to a newer SecureAuth software version might cause the SecureAuth VAM to become invalid and stop working. When your site is ready to upgrade SecureAuth software, get started by [creating a support ticket](#) and selecting **I have a question or issue regarding SecureAuth Value-Added Modules (VAMs)** from the "Submit a request" list. A SecureAuth Tailoring engineer will contact you to evaluate and ensure that the VAM will work with updated SecureAuth software.