Oracle B2C Service

Configuring Pass-Through Authentication Checks

21C

Oracle B2C Service
Configuring Pass-Through Authentication Checks

21C

Part Number: F44691-01

Authors: The B2C Service Information Development Team

Oracle customers have access to electronic support through Oracle Support. For information, visit Get Started with Technical Support or visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs if you are hearing impaired.

Contents

Preface

This preface introduces information sources that can help you use the application and this guide.

Using Oracle Applications

To find guides for Oracle Applications, go to the *Oracle Help Center Documentation*.

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit Oracle's Accessibility Program at *Oracle Accessibility Program Website*.

Videos included in this guide are provided as a media alternative for text-based topics also available in this guide.

Diversity and Inclusion

Oracle is fully committed to diversity and inclusion. Oracle respects and values having a diverse workforce that increases thought leadership and innovation. As part of our initiative to build a more inclusive culture that positively impacts our employees, customers, and partners, we're working to remove insensitive terms from our products and documentation. We're also mindful of the necessity to maintain compatibility with our customers' existing technologies and the need to ensure continuity of service as Oracle's offerings and industry standards evolve. Because of these technical constraints, our effort to remove insensitive terms is ongoing and will take time and external cooperation.

Contacting Oracle

Access to Oracle Support

Customers can access electronic support through Oracle Support. For information, visit *My Oracle Support* or visit *Accessible Oracle Support* if you are hearing impaired.

Comments and Suggestions

Please give us feedback about Oracle Applications Help and guides. See *Oracle B2C Service - Documentation Feedback*.

1 Introduction

Overview of Pass-Through Authentication

Pass-through authentication (PTA) lets you integrate B2C Service Customer Portal with an external customer validation source so that customers can automatically log in to your portal from an external web page.

The external source supplies login parameters to the customer portal by placing them in the URL of the customer portal page. This lets your customers log in to your website and then access the customer portal without requiring a second login specifically for the customer portal. Contact information is shared between the external source and the Oracle database since the customer portal uses external login information to create and update contact records.

Data encryption is available to more securely transmit customer information through the URL that accesses the customer portal, and several encryption options exist. Another PTA configuration option lets your customers log in directly to your customer portal, in addition to logging in with pass-through authentication from your external site. You also have the option of requiring customers to log out through the external site or allowing them to log out from your customer portal.

Although contact records can be created and updated through the PTA integration, they must be deleted through the agent desktop or another integration method, such as the XML API.

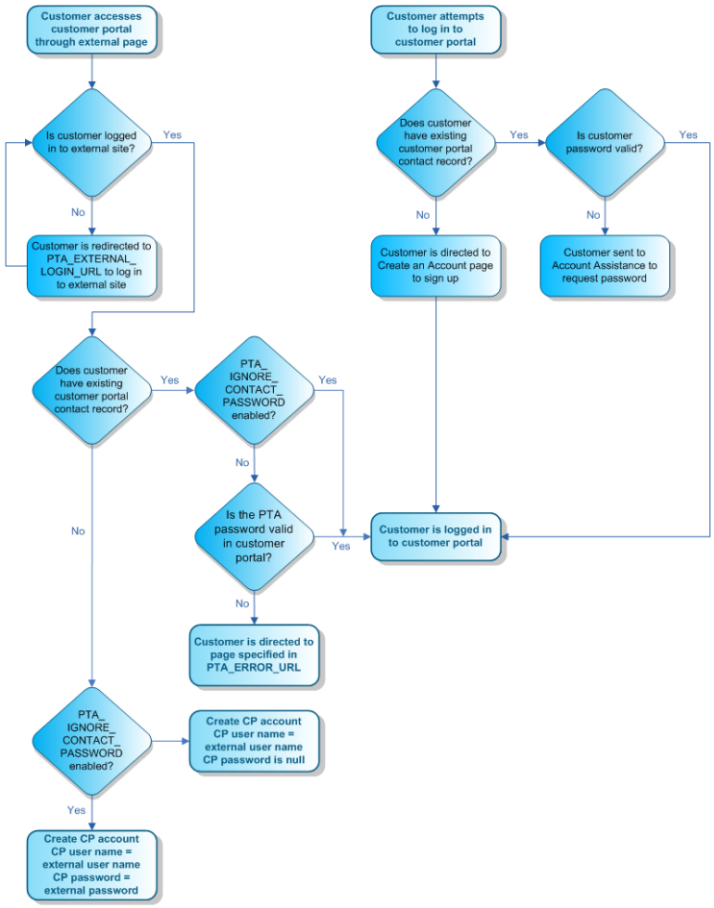
There are two paths available to the customer: Access the customer portal through an external page, or log in directly to the customer portal. When a customer accesses the customer portal through an external page, the system first checks if the customer is logged into the external site. If not, the customer is redirected to the login URL set in the PTA_EXTERNAL_LOGIN_URL configuration setting. After the customer is logged in, the system then checks if the customer has an existing customer portal contact record. If they do, the system checks if the PTA_IGNORE_CONTACT_PASSWORD configuration setting is enabled and if the PTA password is valid in the customer portal. If both are, the customer is logged in to the customer portal.

If the customer has no existing customer portal contact record, the system checks if the PTA_IGNORE_CONTACT_PASSWORD configuration setting is enabled. If it is, the PTA creates the contact record and populates the password with whatever the customer entered. If it is disabled, the PTA creates a contact record in the database with a null password.

If the customer already has an existing customer portal contact record but the PTA_IGNORE_CONTACT_PASSWORD configuration setting is not enabled, the system checks if the PTA password meets the customer portal password requirements. If it does, the customer is logged in to the customer portal. If it does not, the customer is directed to the page specified in the PTA_ERROR_URL configuration setting.

When the customer attempts to log in to the customer portal, existing customer portal contacts are checked for valid passwords before logging the customer in to the customer portal. If the customer does not have a valid password, they are directed to Account Assistance. If the customer does not have an existing customer portal contact record, the customer is directed to the Create an Account page to sign up and then log in.

This flowchart illustrates pass-through authentication as it is used with the customer portal.



Note: Contact your Oracle account manager for assistance in customizing PTA beyond the procedures detailed in this document.

2 Pass-Through Authentication Configuration

Enable and Configure Pass-Through Authentication

Enable pass-through authentication (PTA), set configuration options, then stage and promote your changes to the customer portal.

1. Set the PTA_ENABLED configuration setting to **Yes**.
2. Optional: Set the EGW_AUTO_CONT_CREATE configuration setting to **No**.

   EGW_AUTO_CONT_CREATE allows contact records to be created through email. By default, when an email message is sent to a Service mailbox from an address that does not exist in the Oracle database, a contact record is created automatically. By setting EGW_AUTO_CONT_CREATE to No, you avoid login issues resulting from mismatched user names and passwords.
3. If you set EGW_AUTO_CONT_CREATE to **No**, then set the message base parameter NOT_REG_EMAIL_MSG to direct new customers to your website to register and create an account.
4. Define the external login page.

   See *How You Define the External Login Page*.
5. Decide if you want to use data encryption. If you do, set the method and other encryption specifications.

   See *Why and How to Use Data Encryption*.
6. Decide if you want to allow logout from the customer portal.

   See *How You Require Customers to Log Out From the Customer Portal*.
7. *Stage Your Customer Portal Pages*.
8. *Promote Your Customer Portal Pages*.

How You Define the External Login Page

Customers who try to access your customer portal from your external page may be redirected to an external login page when they click the link. If and how this occurs depends on several factors.

- The URL of the link to the customer portal that resides on the external page
- Whether the customer is logged in to the external site
- Whether the customer portal page being accessed requires login

If the link to your customer portal on your external site passes customer information in the URL and the customer is logged in to the external site, the customer data is passed through the Customer Portal login function. The customer is then logged in to the customer portal, and the page opens. The login process is invisible to the customer, who clicks the link on the external page and sees the customer portal page open.

When the customer portal page requires login or the customer clicks the Log In link on the customer portal but is not logged in to your external site, they will be directed to the page defined by the PTA_EXTERNAL_LOGIN_URL configuration setting. Most likely, this will be the login page for your external site. You can pass next page variables and session information in this URL.

The PTA_EXTERNAL_LOGIN_URL configuration setting also accepts the error code variables you can use in the PTA_ERROR_URL configuration setting to help troubleshoot pass-through authentication login issues. When a value

is entered in the PTA_ERROR_URL configuration setting, any error code variables in the PTA_EXTERNAL_LOGIN_URL configuration setting are ignored.

For example, if the customer tries to open the Answers page but you have required login on that page, the URL you specify to redirect the login can contain the `%next_page%` variable. After they have logged in, your login functionality points them back to the customer portal, passing the validated customer information and returning them to the Answers page. The URL looks like this:

```
http://your_site/login/nextPage/%nextPage%
```

Note: The next page parameter gets passed to the page automatically even when you do not configure it, but specifying it lets you control its placement.

You can also pass URL parameters using this format:

```
http://your_site/login.php?nextPage=%nextPage%
```

The customer portal processes the customer information through its login functionality, although the customer does not see this process. If the information passed in the URL is sufficient to identify an existing contact record in the Oracle database, the customer is logged in and sees the customer portal page they originally tried to access. Any new or additional contact information that is passed through the URL is used to update the contact record.

The passed login parameters must provide data for the minimum required fields needed to log in to the customer portal (p_userid and p_passwd) or create a new contact record (p_userid, p_passwd, and p_email.addr). (In most cases, we recommend that you pass back all URL parameters to B2C Service that the application passed during the redirection.)

Note: If contact custom fields have been created on the administration interface and are required on the customer portal, the values for these fields must also be passed before a new contact record can be created.

If no contact record in the database matches the login parameters passed to the customer portal, a new contact record is created and the customer is logged in to the customer portal as the new contact. If the contact information that is passed does not contain all the fields required to create a new contact record, you can configure the customer portal to direct the customer to an alternate URL. For example, you might create a web page that lets the customer know that access is denied. Or this URL might be a form for gathering the additional required information that then re-passes the parameters to the customer portal.

URLs sent to contacts through email (for example, a link to update the incident) use the URL specified in the PTA_EXTERNAL_LOGIN_URL configuration setting. If you pass a non-blank password using p_passwd in a PTA event and the EU_CUST_ PASSWD_ENABLED configuration setting is disabled, the PTA event will fail. We recommend that you do not change the default value of the EU_CUST_PASSWD_ENABLED configuration setting, which is Yes (enabled), when using PTA.

The customer session ID can be automatically appended to the URL when the customer is redirected through the customer portal. The page specified in the PTA_EXTERNAL_LOGIN_URL configuration setting must be configured to accept the session ID.

Related Topics

- How You Interpret Error Codes

Why and How to Use Data Encryption

You can use encryption to increase the security of the customer login information passed to the customer portal pages from an external site.

By default, encryption is disabled and the data received by the customer portal page URL is Base 64 encoded and then decoded. With encryption enabled, the data is still Base 64 encoded and decoded, but then it is converted to an encrypted string.

> **Note:** If you do not want to use data encryption, you must define a value for the PTA_SECRET_KEY configuration setting in order to validate login parameters. This value should be passed as a p_li_passwd parameter encoded in the PTA login string.

Four configuration settings are used to configure PTA data encryption. For the procedure to edit configuration settings, see *Edit Configuration Settings*.

Setting	Description
PTA_ENCRYPTION_METHOD	Specifies the encryption method you want to use, and is blank by default. The options are des3, aes128, aes192, and aes256.
PTA_ENCRYPTION_IV	Lets you specify an initialization vector value to use for PTA encryption. Initialization vectors are optional, but can help you increase the security of the encryption. You can enter up to a 16-byte value, given as a hex-encoded (base 16) list of bytes. The value depends on the type of encryption specified in the PTA_ENCRYPTION_METHOD configuration setting. 16 bytes are required for aes128, aes192, and aes256 encryptions, and 8 bytes are required for des3 encryption.
Optionally, you can enter a value of ENCODED if the decryption method expects the initialization vector to be read from the encrypted string (after the salt, if salt is used) and before the encrypted value. This option is more secure than hardcoded values if the proper cryptographically random values are sent along in the encrypted data.	
PTA_ENCRYPTION_KEYGEN	Specifies the keygen method used for PTA encryption. The default value is RSSL_KEYGEN_PKCS5_V20, and the other options are RSSL_KEYGEN_PK55_V15 and RSSL_KEYGEN_NONE.
PTA_ENCRYPTION_PADDING	Specifies the padding method used for PTA encryption. The default value is RSSL_PAD_ANSIX923, and the other options are RSSL_PAD_PKCS7, RSSL_PAD_NONE, RSSL_PAD_ZERO, and RSSL_PAD_ISO10126.
PTA_ENCRYPTION_SALT	Lets you specify a salt value to use for PTA encryption. Salt values are optional, but can help you increase the security of the encryption. You can enter up to an 8-byte value, given as a hex-encoded (base 16) list of bytes.
Optionally, you can enter a value of ENCODED if the decryption method expects the salt to be read from the encrypted string before the initialization vector and the encrypted value. This option is more secure than hardcoded values if the proper cryptographically random values are sent along in the encrypted data.	
PTA_SECRET_KEY	Specifies the key used to decode the encrypted PTA string. The value is blank by default. (Do not include the value of PTA_SECRET_KEY in the string itself. The setting should be used only to encrypt the value sent.)

Stage Your Customer Portal Pages

After you have edited the customer portal pages in the development area, you can stage them to see how your changes will appear on the production site.

Before you can stage development pages, the profile assigned to you must have the CP Stage permission enabled. You or your administrator can enable this permission if necessary.

Because the staging area replicates the production site but keeps the pages from being visible to customers, you can continue to modify the development pages and then stage them without exposing the changes to your customers until you are satisfied with the results.

1. Log in to B2C Service.

   Alternately, you can use the Customer Portal Administration site instead of the administration interface by entering **https://your_site/ci/deploy/index** (or **http://your_site/ci/deploy/index** if your site does not have SSL enabled.)

   Continue to Step 5 to resume this procedure.

2. Click **Configuration** on the navigation pane.
3. Expand **Site Configuration** and double-click **Customer Portal**.
4. Select the interface you want to stage from the **Interfaces** column.
5. Perform one of these tasks:
   - On the administration interface, click **Stage** on the **Customer Portal** editor ribbon.
   - On the **Customer Portal Administration** site, click **Stage** on the **Deploy** page.

   If you have created a new widget for your customer portal, you must be sure that Copy to Staging is selected for the widget on this first step of the staging process. Additionally, you must also select Yes to push all framework and widget version changes on the **Version Changes** page during the staging process. If you do not include pushing the version changes, your new widget will not be available on your staging site.

   The first window displays a list of files that have been changed in the development area since the last time files were staged. By default, all new and edited files are selected to be copied to the staging area, and any files you have removed from the development pages have the Remove From Staging action.

6. To prevent a file from being copied to the staging environment, click the **Action** drop-down list in the row associated with the file and select **No Action**.

   This lets you maintain any changes you have made to the development page without having those changes appear in the staging environment or the production pages when you promote the site.

7. To remove one or more files from the staging environment, click the **Action** drop-down list in the row associated with the file and select **Remove From Staging**.

   The selected file will be removed from the staged pages and will not be available to be copied to your production site.

8. Click **Next** to continue.

   The window displays any version changes to the framework or widgets.

9. To push all framework and widget version changes, including the addition of new widgets, select **Yes** from the drop-down list located in the bottom-left corner of the page. If you do not include pushing the version changes, any new widgets will not be available on your staging site.
10. Click **Next** to continue.

The window displays all user agent page set mappings for the interface and notes whether they are enabled or disabled. It also shows the differences in the page sets between the development and staging areas. By default, No Action is selected for the listed page sets, but if you have disabled a page set, the action will be Remove From Staging.

11. To copy a page set that you've enabled to the staging area, click the drop-down list in the **Actions** column and select **Copy To Staging**.
12. To remove a development page set from the staging area, click the drop-down list in the **Actions** column and select **Remove From Staging**.
13. Click **Next**.

    The window summarizes your selections from the earlier pages of the staging process.
14. To store a comment in the staging log file, enter a note in the field.

    You can enter up to 4,000 characters.
15. To re-initialize the staging environment, select the check box just above the Stage button.

    > **CAUTION:** If you select this check box, you will lose any file and page set selections you have made during the staging process. Re-initializing means that all files in the staging area will be deleted and replaced with their corresponding files or settings from the development area.
16. Click **Stage**.

    A message asks you to confirm that you want to copy the selected items to the staging area.

    > **Note:** You will see a message if a deploy lock is in place. Clicking No cancels the staging operation and Yes overrides the existing lock and then continues with the staging operation. Use caution when clicking Yes because you may compromise another staff member's file promote if you start overwriting files in the staging area.
17. Click **Stage** to continue.

    When the process is complete, a window lets you know staging was successful. It also displays a link to view the log. If you staged the files from the Customer Portal Administration site, the window also contains links to the staging area, where you can view the pages, and a link to the Promote page.

    If any widgets have been deleted, the message notifies you that the deleted widget has been deactivated in the staging environment. Also, if any of the widget versions are incompatible with the framework, a staging error occurs and identifies the incompatible widget.

Promote Your Customer Portal Pages

After you are satisfied with your staging area, you can promote the pages and files to production.

Before you can promote the staging area, the profile assigned to you must have the CP Promote permission enabled. You or your administrator can enable this permission if necessary.

1. Perform one of these tasks:
   - Log in to B2C Service.
   - In a web browser, enter **https://your_site_interface/ci/deploy/promote**. Continue to Step 6.
2. Click **Configuration** on the navigation pane.
3. Expand **Site Configuration**, and double-click **Customer Portal**.
4. Select the interface you want to promote from the **Interfaces** column.
5. Click **Promote**.

The window shows you the list of edited files and configurations and notes whether the file or configuration exists in the staging and production areas.

6. To store a comment in the log file, enter a note in the field.

   You can enter up to 4,000 characters.

7. Click **Promote** at the bottom of the page.

   A message asks you to confirm that you want to replace your current production area with the files from the staging area. You will see a message if a deploy lock is in place. Clicking No cancels the promote operation and Yes overrides the existing lock and continues with the promote. Use caution when clicking Yes because you may overwrite another staff member's work.

8. Click **Promote** to continue.

   When the process is complete, a window lets you know the promote process was successful. It also displays a link to view the log. If you promoted the files from the Customer Portal Administration site, the window also contains a link to the production area, where you can view the promoted pages, and a link to the Rollback page.

How You Configure the Customer Portal for Pass-Through Authentication

When you implement PTA integration with the customer portal, you may want to make some changes to your customer portal pages.

These options are available.

- **Require login on customer portal pages**—You can add a login requirement to any customer portal page so that customers must be validated through the external login pagey before they can open the customer portal page. See *Require a Login for Customer Portal Pages*.
- **Edit the Your Account pages**—If you do not want customers to edit the fields on the Your Account pages, you can remove them. If you want to let them edit fields, you must edit the input field widgets on the pages containing the fields. See *Allow Customers to Edit Fields on the Account Settings Page*.

Note: After you have completed these steps, you must deploy the customer portal. If your profile does not have sufficient permissions to deploy the customer portal, coordinate with your administrator to arrange the deployment.

How You Use Pass-Through Authentication When a Chat Request is Accepted

If you use pass-through authentication (PTA) to log users into your customer portal site, you can use the same login credentials when using the syndicated ProactiveChat widget API, and when a chat request is accepted.

To use PTA, you have to subscribe to the evt_beforeDataRequest event, which is initiated after a chat is accepted and after chat agent availability is checked. In the callback method for the event, you can build your PTA string similar to the way it is done within customer portal code. The encoded PTA string can then be added to the data arguments.

Add code similar to this to the web page containing the widget.

```
<script type="text/javascript">
 function addPta(type, args, instance){
 var ptaToken = 'thisIsYourEncryptedPTAString';
 var data = args[0];
 if(data){
 data.pta = ptaToken;
RightNow.Client.Event.evt_beforeDataRequest.subscribe(addPta);
</script>
```

In the example, the callback method addPta is called when the event is fired.

Edit Configuration Settings

Follow this procedure to edit pass-through authentication configuration settings.

1. Click **Configuration** on the navigation pane.
2. Expand **Site Configuration**, and double-click **Configuration Settings**. The Search window opens.

   > **Note:** You must perform a search before any data displays.

   From the Search window you can filter the configuration settings that display on the editor. Alternatively, you can click the Cancel button to bypass the Search window and perform your search using the buttons on the ribbon or the search fields on the top of the editor.
3. Type the name of the configuration setting you want to edit in the **Key** field. You can type a partial name, using the percent (%) or asterisk (*) symbols as wildcard characters. For instance, you can search for configuration settings beginning with PTA_ by entering “pta_%” in the **Key** field.

   > **Tip:** To display the configuration settings you need, you may need to click the Select All check box in the **Configuration Base** field.
4. Select the row that displays the configuration setting you want to edit.
5. Perform one of these tasks:
   - Click **Edit Selection**. Either the **Site** or interface_name window opens depending on the whether the configuration setting applies to the entire B2C Service site or to specific interfaces.
   - Double-click the setting to open it on the content pane and edit the value field.
6. Type or select the new value. Editing options are specific to the field’s data type. For example, if a setting can be enabled or disabled, a Yes/No drop-down list displays in the **Value** field.
7. Perform one of these tasks:
   - To confirm a value entered in the **Site** or interface_name window, click the window’s **OK** button, and then click **Save**.
   - To confirm a value entered in the editor on the content pane, click **Save**.

     > **Note:** You may be required to log out of the administration interface and log back in for your changes to take effect.

Remove Your Account Pages and Links

Use this procedure to remove your account pages and links.

1. Edit the `account/overview.php` file to remove the Settings section and the link for updating settings. (By default, the Change Your Password link is hidden when customers log in with PTA.)

   > **Note:** If you enable dual-mode login, you might want to keep this section for customers who log in directly to the customer portal without being validated through an external source. In that case, you might want to create an alternate Your Account page.

   Delete these lines of code.

   ```
   <h2><a class="rn_Profile" href="/app/account/profile#rn:session#">#rn:msg:SETTINGS_LBL#</a></h2>
   <div class="rn_Profile">
   <a href="/app/account/profile#rn:session#">

   #rn:msg:UPDATE_YOUR_ACCOUNT_SETTINGS_CMD#</a><br/>
   <rn:condition external_login_used="false">
   <a href="/app/account/change_password#rn:session#">

   #rn:msg:CHANGE_YOUR_PASSWORD_CMD#</a>
   </rn:condition>
   </div>
   ```

2. Edit the `templates/standard.php` file to remove Account Settings from the drop-down list on the Your Account tab of the template.

   Locate this line of code.

   ```
    subpages="#rn:msg:ACCOUNT_OVERVIEW_LBL# > /app/account/overview,
   #rn:msg:SUPPORT_HISTORY_LBL# > /app/account/questions/list,
   #rn:msg:ACCOUNT_SETTINGS_LBL# > /app/account/profile,
   #rn:msg:NOTIFICATIONS_LBL# > /app/account/notif/list"/></li>
   ```

   Delete `#rn:msg:ACCOUNT_SETTINGS_LBL#> /app/account/profile,.`

3. Delete these page files:
   - `account/profile.php`
   - `account/change_password.php`
   - `account/change_password.php`
   - `utils/submit/password_changed.php`
   - `utils/submit/profile_updated.php`

3 Custom Login and Logout

Require a Login for Customer Portal Pages

You can add a login requirement to any customer portal page to require that customers be authenticated through the external login page before accessing the customer portal page.

> **Note:** The CP_FORCE_PASSWORDS_OVER_HTTPS configuration setting requires all logged-in customer portal activity to occur over HTTPS. If this setting is enabled, which it is by default, pass-through authentication requests must be sent using HTTPS to ensure that information is being sent securely.

1. To require login on the Support Home page, edit the `home.php` file by adding `login_required="true"` to the meta tag line of the page code. Your modified code might look like the following:

   ```
   <rn:meta title="#rn:msg:SHP_TITLE_HDG#" template="standard.php" clickstream="home"
    login_required="true" />
   ```

2. To require a login on for any of these pages, edit the page's `.php` file to add `login_required="true"` to the meta tag line of the page code as you did in the previous step.
   - `error.php` – Prevents customers from seeing PTA-specific error codes.
   - `answers/detail.php`*`answers/detail.php`* – Prevents customers from viewing answer details.
   - `answers/list.php` – Prevents customers from viewing the Answers page.
   - `chat/chat_landing.php` – Prevents customers from participating in a chat session with an agent.
   - `chat/chat_launch.php` – Prevents customers from requesting a chat session.
3. If you have specified a value for PTA_EXTERNAL_LOGIN_URL, repeat Step 1 for the `utils/login_form.php` file.

   > **CAUTION:** Do not edit this file if PTA_EXTERNAL_LOGIN_URL is blank.

How You Require Customers to Log Out From the Customer Portal

You can require customers who log in to your customer portal from an external site to also log out from the external site.

If you do, the Logout link is removed from the customer portal. Customers who log out from the external site must be redirected to the *ci/pta/logout* page, where all cookies are cleared and customers are logged out of the customer portal. Customers do not see this page, but are instead directed to the page defined in the PTA_EXTERNAL_ POST_LOGOUT_URL configuration setting after they log out of the customer portal. This might be your external home page, for example, or a page with a message that confirms successful logout.

You can also allow customers to log out from the customer portal even when they have logged in from an external site using pass-through authentication. The PTA_EXTERNAL_ LOGOUT_SCRIPT_URL configuration setting defines the page where customers are directed after logging out of the customer portal, and it allows the display of the Logout link on the customer portal. (If this setting is blank, customers cannot log out of the customer portal because no Logout link displays. In this case, they must log out through the external site instead.) When customers

click the Logout link, they are logged out of the customer portal and directed to the external URL specified in the PTA_EXTERNAL_LOGOUT_SCRIPT_URL configuration setting. Your code defines what happens next. For example, you might log customers out of your external site automatically when they log out of customer portal. In that case, customers can be directed to the page specified in the PTA_EXTERNAL_POST_LOGOUT_URL configuration setting.

Related Topics

- How You Log Out of Pass-Through Authentication with Communities Disabled
- How You Log Out of Pass-Through Authentication with Communities Enabled

How You Implement a Customer Login Script

To develop a login-parameters integration, you must embed code within your login script to format a URL that passes data from your external validation source to the customer portal.

The embedded code can be written in any scripting language, including PHP, JSP, or ASP. The login parameters from the external validation source must be placed in the customer portal URL and must be encoded using Base 64 encoding. In addition to using the Base 64 function, certain characters must also be replaced in the URL (+ becomes _, / becomes ~, and = becomes *).

Note: You must use a login script for every link from your website to the customer portal. If contacts exit the customer portal and re-enter later in their session, they are not automatically logged in. Therefore, we recommend that all links to the customer portal contain pass-through data.

URLs use this format: http://your_domain/ci/pta/login/redirect/answers/list/p_li/encoded_login_parameters

Note: You can replace `answers/list` with any customer portal page (for example, `home`), or use the p_next_page parameter to return customers to their original customer portal page.

The PTA controller accepts the p_li encrypted password parameter with either a GET or POST request. The POST parameter is checked only if p_li is not part of the URI (uniform resource identifier).

The parameters that can be passed to the customer portal are detailed in the table. Each parameter represents the associated field in the *contacts* table of the Oracle database. For additional parameters that can be passed to the customer portal, see *Additional Parameters*.

Parameter	Field in *contacts* table	Notes
p_userid	login	This parameter is required to log in and create a contact record. It cannot be updated with pass-through authentication.
p_passwd	password	This parameter is required to log in and create a contact record or log in as an existing contact. It cannot be updated through pass-through authentication. The value can be null. This parameter is ignored when the PTA_IGNORE_CONTACT_PASSWORD configuration

Parameter	Field in *contacts* table	Notes
		setting is enabled. See *How You Enable Dual-Mode Login*.
p_email.addr	email	This parameter is required to log in and create a contact record. Its value must be unique.
p_title	title	
p_name.first	first_name	
p_name.last	last_name	
p_alt_name.first	alt_first_name	
p_alt_name.last	alt_last_name	
p_email_alt1.addr	email_alt1	
p_email_alt2.addr	email_alt2	
p_addr.street	street	
p_addr.city	city	
p_addr.postal_code	postal_code	This parameter must not contain special characters. (For example, 59715-1111 should be passed as 597151111.)
p_addr.country_id	country_id	This parameter must be passed as a country's ID number. See *How You Find Code Numbers and Report IDs*.
p_addr.prov_id	prov_id	This parameter must be passed as a state or province's ID number. See *How You Find Code Numbers and Report IDs*.
p_ph_office	ph_office	
p_ph_mobile	ph_mobile	
p_ph_fax	ph_fax	
p_ph_asst	ph_asst	
p_ph_home	ph_home	

Parameter	Field in *contacts* table	Notes

How You Log Out of Pass-Through Authentication with Communities Disabled

When Social Experience communities are disabled, customers can log out of the external site or the customer portal.

Logging out of the external site works normally: After customers log out from the external site, the customer portal logout page is invoked, clearing cookies and logging out the customer, who is redirected to the page specified in the PTA_EXTERNAL_POST_LOGOUT_URL configuration setting. This setting must contain the fully qualified URL of the page you want to redirect customers to.

When communities are disabled and customers click the Logout link on the customer portal, they are logged out of the customer portal and redirected to the page defined by the PTA_EXTERNAL_LOGOUT_SCRIPT_URL configuration setting. This page is the page that logs customers out of the external site, and you can pass a source page parameter to send customers back to the page they were on when they logged out. You also can send them to any other page.

Related Topics

- How You Require Customers to Log Out From the Customer Portal
- Edit Configuration Settings

How You Log Out of Pass-Through Authentication with Communities Enabled

When Social Experience communities are enabled, customers can log out from the external site, the customer portal, or the community.

Logging out of the external site is the same whether communities are enabled or not, except that customers are also logged out of the communities in the process.

When customers click the Logout link on the customer portal, they are directed to the community logout script using the source page parameter in the PTA_EXTERNAL_LOGOUT_SCRIPT_URL configuration setting. Customers are then logged out of the external site and redirected to PTA_EXTERNAL_LOGOUT_SCRIPT_URL. This setting must contain the fully qualified URL of the page you want to redirect customers to.

When customers click the communities logout link, they are logged out of the communities, redirected to a logout page for the customer portal (*ci/social/logout*), logged out of the customer portal, and then redirected to the page specified in PTA_EXTERNAL_LOGOUT_SCRIPT_URL.

> **Note:** The code for communities must be modified to pass the encoded URL of the page from which the customer logs out.

Related Topics

- How You Require Customers to Log Out From the Customer Portal

4 Customer Permissions

Allow Customers to Edit Fields on the Account Settings Page

When customers log in to the customer portal through PTA, by default they cannot edit the fields on that page.

This is because the *allow_external_login_updates* attribute of the input widgets on the page defaults to false. If you want to retain the default behavior, you will probably want to remove the Account Settings and Change Your Password pages and any links to them. If, instead, you want to let customers change their contact information, you can add attributes to the fields you want to be able to edit.

Follow these steps to allow customers to edit fields on the Account Settings page.

1. Open the `account/profile.php` file.
2. To let customers edit the First Name and Last Name fields, locate the line of code that defines the ContactNameInput widget and add the *allow_external_login_updates* attribute to it. The code looks like the following:

```
<rn:widget path="input/ContactNameInput" table="contacts" required = "true"
 allow_external_login_updates="true" />
```

3. To let customers edit other input fields, locate the line of code that defines the FormInput widget for the field and add the *allow_external_login_updates* attribute to it. For example, the code to let customers change their email address looks similar to this:

```
<rn:widget path="input/FormInput" name="contacts.email" required="true" validate_on_blur="true"
 allow_external_login_updates="true" />
```

> **Note:** Regardless of how you set the attribute for the Username field (*contacts_login*), customers cannot change this field when PTA is enabled.

How You Use Pass-Through Authentication with Service Level Agreements

In addition to requiring login on customer portal pages, you may want to restrict certain pages only to customers who have a specific type of service level agreement (SLA).

These code examples assume you want to edit the **Ask a Question** page to require an SLA.

If you require an SLA to submit incidents, edit the meta tag line of the `ask.php` file. Your modified code might look something like this, where the added code is in bold text.

```
<rn:meta title="#rn:msg:ASK_QUESTION_HDG#" template="standard.php"
clickstream="incident_create" login_required="true"
sla_required_type="incident" sla_failed_page="/app/error/error_id/2"/>
```

If you require an SLA to request a chat session, edit the **chat/chat_landing.php** and **chat/chat_launch.php** files. Your modified code might look something like this, where the added code is in bold text.

```
<rn:meta clickstream="chat_landing" include_chat="true"
login_required="true" sla_required_type="incident"

sla_failed_page="/app/error/error_id/2" />
<rn:meta title="#rn:msg:LIVE_CHAT_LBL#" template="standard.php"
clickstream="chat_request" login_required="true"
sla_required_type="incident" sla_failed_page="/app/error/error_id/2"
/>
```

5 Dual-Mode Login

How You Enable Dual-Mode Login

Dual-mode login lets customers create an account on the customer portal and then log in later using PTA even though the external site does not have access to the customer portal password.

The PTA_IGNORE_CONTACT_PASSWORD configuration setting, which is disabled by default, lets you configure a site that accepts both PTA login and the normal customer portal login. It is, therefore, possible for customers to have one password on the external site and another on the customer portal. When the PTA_IGNORE_CONTACT_PASSWORD configuration setting is enabled, the customer portal does not evaluate the customer's password when the customer logs in with PTA because the external site has already authorized the login.

> **Note:** Encryption is enforced when dual-mode login is enabled, so you must enter a valid encryption method in the PTA_ENCRYPTION_METHOD configuration setting or customers cannot log in and an error page displays.

Related Topics

- How You Create an Account with Dual-Mode Login Enabled
- How You Allow Customers to Update Accounts With Dual-Mode Login Enabled
- Why and How to Use Data Encryption

How You Create an Account with Dual-Mode Login Enabled

Customers can log in to the customer portal directly or from an external site.

When the PTA_IGNORE_CONTACT_PASSWORD configuration setting is enabled, customers who access the customer portal directly can create an account as they normally do. The password they enter is stored in their B2C Service contact record. They can then log in to the customer portal with the user name and password they defined.

Customers who enter the customer portal from an external site using PTA can also create an account. However, their password for the external site, which was passed through the page URL with encrypted PTA, is ignored, and the customer's contact record will have a blank password. Customers can access the customer portal with PTA through the external site, but they will not be able to log in to the customer portal directly until they have completed the account creation process through the customer portal Account Assistance page.

Related Topics

- How You Enable Dual-Mode Login
- How You Allow Customers to Update Accounts With Dual-Mode Login Enabled

How You Allow Customers to Update Accounts With Dual-Mode Login Enabled

Customers can update an account regardless of whether they access the customer portal directly or from and external site.

When the PTA_IGNORE_CONTACT_PASSWORD configuration setting is enabled, customers who access the customer portal directly can update their account, including changing their password, as they normally do. To access the customer portal in the future, they must log in with their user name and new password. The new password will not affect their ability to log in through an external site with the setting enabled.

Customers who enter the customer portal from an external site using PTA can also update their account. Although their password is ignored when the PTA_IGNORE_CONTACT_PASSWORD configuration setting is enabled, they have been authenticated through their login to the external site. As a result, the customer portal allows them to update their account, including their customer portal password.

> **Note:** The contact fields on the standard Account Settings page are read-only because the *allow_external_login_updates* attribute of those input widgets defaults to false. If you want to let customers edit these fields, you must edit the input widgets to set the attribute to true. Regardless of the attribute's setting in the Username field, customers cannot change this field when PTA is enabled. See *Allow Customers to Edit Fields on the Account Settings Page*.

6 Reference

Pass-Through Authentication Configuration Settings

A number of configuration settings must be modified to configure pass-through authentication. These settings are listed here and described in detail in the topics referenced in the table.

Configuration settings are modified using the Configuration Settings editor. For more information about configuration settings, see *How the Configuration Settings Editor Works*.

Setting	Description
EGW_AUTO_CONT_ CREATE	This setting, which is enabled by default, allows the creation of new contact records when an email is received from an email address that does not already exist in the database. To avoid potential login issues when using PTA, this setting should be disabled. See *Enable and Configure Pass-Through Authentication*.
EU_CUST_PASSWORD_ ENABLED	This setting, which is enabled by default, enables the display of the contact password field on customer portal pages. This setting should be enabled when using PTA. See *How You Define the External Login Page*.
PTA_ENABLED	Enables the use of pass-through authentication. See *Enable and Configure Pass-Through Authentication*.
PTA_ENCRYPTION_IV	Specifies the initialization vector you want to use for PTA encryption. See *Why and How to Use Data Encryption*.
PTA_ENCRYPTION_ KEYGEN	Specifies the keygen method you want to use for PTA encryption. Refer to *Why and How to Use Data Encryption*.
PTA_ENCRYPTION_ METHOD	Specifies the encryption method you want to use for PTA logins. Refer to *How You Enable Dual-Mode Login* and *Why and How to Use Data Encryption*.
PTA_ENCRYPTION_ PADDING	Specifies the type of padding you want to use for PTA encryption. See *Why and How to Use Data Encryption*.
PTA_ENCRYPTION_ SALT	Specifies the salt value you want to use for PTA encryption. See *Why and How to Use Data Encryption*.
PTA_ERROR_URL	Specifies the URL where customers are redirected when PTA login attempts fail. If this setting is blank, customers are redirected to the URL specified in the PTA_EXTERNAL_LOGIN_URL setting. See *How You Interpret Error Codes*.
PTA_EXTERNAL_ LOGIN_URL	Contains the URL to a login page where customers are directed if they try to access a customer portal page that requires authentication. See *How You Define the External Login Page*.

Setting	Description
PTA_EXTERNAL_ LOGOUT_SCRIPT_URL	Specifies the URL where customers are directed to log out of the customer portal. If this setting has a value, customers can log out of the customer portal. If the setting is blank, customers will not be able to log out from the customer portal since the logout widget will not display. See *How You Require Customers to Log Out From the Customer Portal*.
PTA_EXTERNAL_POST_ LOGOUT_URL	Contains the URL to the page where you want to redirect customers after they log out of the external system. See *How You Require Customers to Log Out From the Customer Portal*.
PTA_IGNORE_ CONTACT_PASSWORD	Specifies whether contact passwords are honored during PTA logins. See *How You Enable Dual-Mode Login*.
PTA_SECRET_KEY	Contains the secret key used to validate login integration parameters when encryption is disabled, or the key to decode the PTA string when encryption is enabled. See *Why and How to Use Data Encryption*.

Additional Parameters

Besides the fields from the contacts table, you can also pass parameters to the customer portal.

Parameter	Notes
p_ccf_*	This parameter represents a contact custom field in B2C Service. The * must be replaced with the number of the cf_id for the contact custom field. If this is a menu custom field, the numbers (not the actual text) for each menu item must be specified as the value in the integration login code. See *How You Find Code Numbers and Report IDs*.
p_chan_*	This parameter represents the contact's social channel. The * must be replaced with the ID number of a valid channel: 11—Twitter 12—YouTube The value represents the user name for the channel. For example, if you want to pass the contact's Twitter user name, you would pass the parameter and value p_chan_11="jane.doe", where jane.doe is the user name.
p_li_expiry	This parameter is a time stamp that defines how long the PTA login information is valid. When the time expires, the login information is no longer accepted and contacts are redirected to the page specified in the PTA_ERROR_URL configuration setting, and an error code of 16 is passed to the page. See *How You Interpret Error Codes*. **Note:** You can generate the value using a UNIX date/time stamp generator.
p_li_passwd	This parameter represents the string specified in the PTA_SECRET_KEY configuration setting. Note: This parameter is required if the PTA_SECRET_KEY configuration setting contains a value and the PTA_ENCRYPTION_METHOD configuration setting does not contain a value.

Parameter	Notes
p_org_id	This parameter represents an organization ID to associate with a contact. Note: You must manually assign any service level agreements (SLA) that you want to associate with the organization, including those controlling privileged access.
p_state.css	This parameter represents the contact's state for B2C Service. 0—Disabled 1—Enabled
p_state.ma	This parameter represents the contact's state for B2C Service Outreach. 0—Disabled 1—Enabled
p_state.sa	This parameter represents the contact's state for Opportunity Tracking. 0—Disabled 1—Enabled

How You Interpret Error Codes

When a customer attempts to log in using pass-through authentication, there are a number of factors that can cause login failure, including an invalid user name or password, a duplicate email address in the database, and problems with the PTA string.

To help you debug login errors or provide informational messages, customers can be redirected to a custom page displaying an error code and session information when an error occurs.

The URL of the page where customers are redirected is specified in the PTA_ERROR_URL configuration setting. To display an error code, the URL must be appended with the `%error_code%` variable. Session information can be provided in the form of a base64-encoded string if the `%session%` variable is also appended. Session information displays only if login tracking cookies are disabled on the customer's computer.

> **Note:** The PTA_ERROR_URL configuration setting is blank by default. If you do not specify a value for the setting, customers are redirected to the URL in the PTA_EXTERNAL_LOGIN_URL configuration setting when a login error occurs. If you choose not to use PTA_ERROR_URL, you can append the `%error_code%` and `%session%` variables to the end of the URL specified in PTA_EXTERNAL_LOGIN_URL. See *How You Define the External Login Page*.

For example, assume that you set the configuration setting value to:

```
http://your_site/my_login_error_page.php/%error_code%
```

If login fails because the password exceeds the 20-character limit, the URL that is returned is:

```
http://your_site/login/nextPage/home/error/15
```

The error code, 15 in this example, lets you know what caused the failure.

The table describes error codes found in the URL. These codes are the same whether the `%error_code%` variable is used in the PTA_ERROR_URL or the PTA_EXTERNAL_LOGIN_URL configuration setting.

Error Code	Description
1	The PTA string parameter was not found. This parameter contains all of the encoded PTA information in the URL, so it must be present to log in.
2	PTA information after pre_pta_decode hook was not in the correct format. A string or an array was expected, but something else was received.
3	PTA string could not be Base 64 decoded. There was an error within the string that caused the decoding process to fail.
4	One of the PTA string parameters was not well formed. For example, it did not contain “p_” or was missing an “=” separator between the key and value.
5	The p_userid string was passed in, but it did not have a value. This pair is required for login.
6	The value of the p_li_passwd pair was incorrect. This error applies only if no value is set for the PTA_ENCRYPTION_METHOD configuration setting.
7	The specified credentials were invalid.
8	Login failed because PTA is not enabled for the interface.
9	Data decryption failed.
10	Login failed because PTA_ENCRYPTION_METHOD does not contain a valid value.
11	Login failed because the PTA_ENCRYPTION_PADDING configuration setting does not contain a valid value.
12	Login failed because the PTA_ENCRYPTION_KEYGEN configuration setting does not contain a valid value.
13	Login failed because the PTA_IGNORE_CONTACT_PASSWORD configuration setting is enabled, but no encryption scheme has been set in PTA_ENCRYPTION_METHOD.
14	Login failed because the format of the data after the pre_pta_convert hook was not an array.
15	Login failed because the password exceeded the 20-character maximum length.

Error Code	Description
16	Login failed because the PTA token expired and is no longer valid. A new token must be generated to authenticate the customer.
17	Login failed because two or more email addresses have the same value.

How You Find Code Numbers and Report IDs

You must use code numbers (ID numbers) in pass-through authentication to specify parameters such as countries, provinces, custom fields, and organization IDs.

The administration interface provides three ways to look up the codes for these types of fields:

- Hovering over the field name
- Displaying report IDs in the Reports explorer
- Using the NamedID helper object

When exploring reports, you can view the report ID (ac_id) by displaying the ID column in the explorer details.

Many records and items contain an Info button on the **Home** tab of the ribbon. When you click the Info button, record details display, including the record ID number.

How You Pass Login Parameters

These examples show how to generate a form to pass login parameters to B2C Service.

Using these examples, you can retain all query_string parameters and append key-value pair parameters.

Replacing certain variables with meaningful values will make the scripts easier for you to understand.

- your_domain: the domain name used by your B2C Service site
- your_interface: your interface name
- li_password: the string specified in the PTA_SECRET_KEY configuration setting

CAUTION: This example code snippet is for illustrative purposes only and will be improperly formatted if you attempt to cut and paste directly from it.

```
<?
//Assumption is that user has been validated/logged in and you have their contact record
//available and can access their profile data
//Build up PTA data array
$ptaDataArray = array(

//Common contact fields (not a complete listing, this is just a sampling)
//The $contact variable is assumed to be the data of the user logging in
'p_userid' => $contact->login,
```

```
'p_passwd' => $contact->password,

//Only needs to be sent if PTA_IGNORE_CONTACT_PASSWORD is disabled
'p_email.addr' => $contact->emailAddress,
'p_name.first' => $contact->firstName,
'p_name.last' => $contact->lastName,

//Example of sending in custom field value where the custom field
ID is 3 'p_ccf_3' => $contact->customField3Value,

//Example of sending in channel field value where the channel field ID is 14
'p_chan_14' => $contact->channelField14Value);

//Add secret key if not using encryption
if (PTA_ENCRYPTION_METHOD configuration setting IS NOT set)
{
$ptaDataArray['p_li_passwd'] = Value of PTA_SECRET_KEY config setting;
}

//Convert PTA data array to string
$ptaDataString = "";
foreach($ptaData as $key=>$value)
{
$ptaDataString .= ($ptaDataString === "") ? '' : '&';
 $ptaDataString .= "$key=$value";
}

//Optionally encrypt data if using encryption with the method, secret key, padding a keygen
//methods. The function called here is made up. The actual function will vary depending on
//which language you are using
if (PTA_ENCRYPTION_METHOD IS set)
{
$ptaDataString = encryptData($ptaDataString, PTA_ENCRYPTION_METHOD,
PTA_SECRET_KEY, PTA_ENCRYPTION_PADDING, PTA_ENCRYPTION_KEYGEN);
}

//Base64 encode the data
$ptaDataString = base64_encode($ptaDataString);

//Make sure the data is URL safe
$ptaDataString = strtr($ptaDataString, array('+' => '_', '/' =>
'~', '=' => '*'));

//Specify which page to take the user to
if (%next_page% URL parameter exists)
$redirectPage = %next_page% parameter;
else
$redirectPage = 'home';

//Send the user to the PTA controller to log them in
header("Location: http://your _CP_site/ci/pta/login/redirect/$redirectPage/p_li/$ptaDataString");
exit;
```

How You Use the pre_pta_decode Hook

The pre_pta_decode hook lets you write custom PHP code, which is executed after accepting the PTA string from the URL and before calling the login routine.

After the hook runs, the p_li parameter is processed and passed to the PTA controller. The hook also passes the redirect parameter so you can modify the location where the customer is directed.

It is not possible to return a custom error message from this hook, so if you want to cover the situation of an interrupted PTA login, you must add a `header()` location redirect and `exit()` in your hook. There are two data formatting options: string or array.

- **String format**—After the hook executes, the login integration data that was passed to the hook is evaluated to see if it is still a string. If it is, the data is assumed to be a standard base_64 encoded string. An algorithm is run to convert the string into an array of contact pairdata in key->value pairs. This allows the pass-through authentication to work as it would if no hook handler is defined and no extra encryption is added.
- **Array format**—After the hook executes, the p_li parameter is evaluated to see if it has been converted to an array. If so, the format of this array is assumed to be the contact pairdata key->value structure. Here's an example of this structure.

```
array(
 [p_passwd]=>
 [p_userid]=>username
 [p_email.addr]=>email@example.com
```

How You Use the pre_pta_convert Hook

You can use a pre_pta_convert hook that runs after the data has been decoded and converted into an array, and before it is converted to the correct pair data structure.

This lets you modify the PTA data sent in the URL on the fly without having to decrypt and convert it yourself.

In this hook, a single parameter named "decodedData," which is in the form of an array, is passed. This example shows the data in the URL in the first line and the decoded/decrypted data passed to the hook by reference in the second line.

```
JnBfdXNlcmlkPXVzZXJuYW1lJnBfZW1haWw9dGVzdEBleGFtcGx lLmNvbQ**
[p_userid => 'username', p_email => 'test@example.com']
```

Any modifications to the array are picked up by the PTA controller when the data is converted into contact API pairs.