Oracle Service Cloud's (OSC's) single-sign-on (SSO) solution is called Pass Through Authentication (PTA). The official documentation for it is available [here](http://documentation.custhelp.com/euf/assets/docs/november2015/pdfs/november2015_PTA_guide.pdf). (Fix this URL with the appropriate version’s documentation.)

With PTA you can parameterize a URL to automatically log a user into the Customer Portal (CP). Before you can use PTA, though, a minimum of three configuration parameters have to be set. (In the agent console: Configuration > Site Configuration > Configuration Settings. In the “Key” field, enter “%PTA%” and search to see all PTA configs.) They are:

* PTA\_ENABLED = Yes
* PTA\_ERROR\_URL = [http://www.espn.com/%error\_code%](http://www.espn.com/%25error_code%25)
* PTA\_SECRET\_KEY = HipposAreUngainly

(I always pick on espn.com for testing PTA because it’s readily available, is unlikely to offend anyone’s sensibilities, and doesn’t eat my error code. If a PTA login attempt fails, it’ll redirect you to e.g. <http://espn.go.com/7>, which is more useful than it looks – the “7” on the end is an error code that you can look up in the documentation to see what the problem is.) You can change the secret key to whatever you want. Here, I’ve picked an arbitrary value.

Once those three are set up, you can begin building the PTA URL. The basic CP URL for your site is

<http://brahminusa.custhelp.com/> replace

To hit the PTA controller, we're going to add some parameters onto this URL like so:

<http://brahminusa.custhelp.com/ci/pta/login/redirect/answers/list> replace

This URL may look familiar. It's CodeIgniter under the hood. In case you're not familiar with CodeIgniter, this says

1. "Hit the standard controller" (ci)
2. "named pta.php" (pta),
3. "calling the function named 'login'" (login).
4. "If successful, redirect" (redirect)
5. "to answer/list.php" (answers/list).

answer/list.php is the standard redirect location, although this is easy to change if you’d rather redirect PTA logins somewhere else.

What this URL is still missing is the authentication parameters. So let's add those:

<http://brahminusa.custhelp.com/ci/pta/login/redirect/answers/list/p_li/p_userid=mikewaldron@helixmail.com&p_email=mikewaldron@helixmail.com&p_first_name=Mike&p_last_name=Waldron&p_passwd=password12345&p_li_passwd=HipposAreUngainly&p_org_id=-2147483647> replace

**p\_li** is a special parameter that means "here comes a PTA authentication string," Following it is the PTA authentication string, which contains seven parameters:

* p\_userid is the user’s login name. (Frequently this is the same as the user’s email address, but this isn’t universal.)
* p\_email is the user’s email address
* p\_first\_name is the user’s first name
* p\_last\_name is the user’s last name
* p\_passwd is the user’s password...in theory. In practice, it doesn’t seem to matter what the value is, but the p\_passwd parameter has to be present
* p\_li\_passwd is a sitewide secret key that must be known to generate PTA URLs
* p\_org\_id is the user’s organization ID. In this case, it has no value, as indicated by MIN\_INT (-2147483647)

The parameter string can be encrypted, for additional security, but that's not strictly necessary. You will want to base64 encode the authentication parameters (everything after the "/p\_li/") and make sure the result is URL-safe. I do it like this in PHP:

$ptaDataString = base64\_encode($params);  
$ptaDataString = strtr($ptaDataString, array('+' => '\_', '/' => '~', '=' => '\*'));

but you can do it any way you like. The final result looks like this:

<http://brahminusa.custhelp.com/ci/pta/login/redirect/answers/list/p_li/cF91c2VyaWQ9bWlrZXdhbGRyb25AaGVsaXhtYWlsLmNvbSZwX2VtYWlsPW1pa2V3YWxkcm9uQGhlbGl4bWFpbC5jb20mcF9maXJzdF9uYW1lPU1pa2UmcF9sYXN0X25hbWU9V2FsZHJvbiZwX3Bhc3N3ZD1wYXNzd29yZDEyMzQ1JnBfbGlfcGFzc3dkPUhpcHBvc0FyZVVuZ2Fpbmx5JnBfb3JnX2lkPS0yMTQ3NDgzNjQ3> change

and if you hit that URL it should log you into the customer portal with my test account.