Oracle Utilities Customer Self Service

Security Guide

Release 2.1.0.2

E58329-02

June 2015

Oracle Utilities Customer Self Service Security Guide

Release 2.1.0.2

E58329-02

June 2015

Table of Contents

Chapter 1

Product Overview

Oracle Utilities Customer Self Service is a flexible and user-friendly packaged utility portal that is pre-integrated with Oracle Utilities applications. This solution provides consumers with the ability to manage their accounts, take control of their consumption, and receive alerts and updates. It increases utility efficiency by facilitating interaction with consumers and highlighting incentives to optimize energy usage and reduce costs.

The application can provide both unsecured public access for finding general information and utility offerings, and secured access for registered and enrolled users to perform account specific operations.

Functional Overview

Oracle Utilities Customer Self Service modules include the following functionality:

- Account Management Module:
    - User registration
    - Password management
    - Self-service information management
    - Account information management
    - Alerts and notifications
    - Forms Management
- Billing and Payment Management Module:
    - Billing notification preferences
    - Account charges summary
    - View bill/payment history

  - Service charges to-date
  - Compare rate plans and analysis
  - Setup electronic billing
  - One-time payments
  - Automatic recurring payments
  - View rate plans and products
  - View promotions
  - Payment Arrangement
  - Budget Management and Billing
  - Prepaid Customer Enhancements
- Customer Service Management Module:
  - Add scalar meter read data
  - Detailed service usage
  - Download Usage Data (Usage Download)
  - Start, Stop, or Transfer Service for a new or existing customer
- Outage Module:
  - Outage Table - Display outage information for the utility as text. Outage Map - Display a geographic map showing outage information for the utility. My Outage Details - To show the current outages and planned outages for a given account
  - Report Public Outage - To report an outage for a public location
  - Report Premise Outage - To report an outage at a customer's premise for a given account.
- Commercial Account Management
  - Multiple Account management
  - Multiple Account Data Download
  - Multiple Account Financial History
  - Multiple Account Aggregation
  - Multiple Account Usage Comparison

Two additional secured areas are available to provide the following capabilities:

- Administration
  - View and manage metadata used by the application (labels, messages, other entities)
  - View and manage access roles and security rules
- Customer support
  - Allow a CSR login and view core modules as selected customer

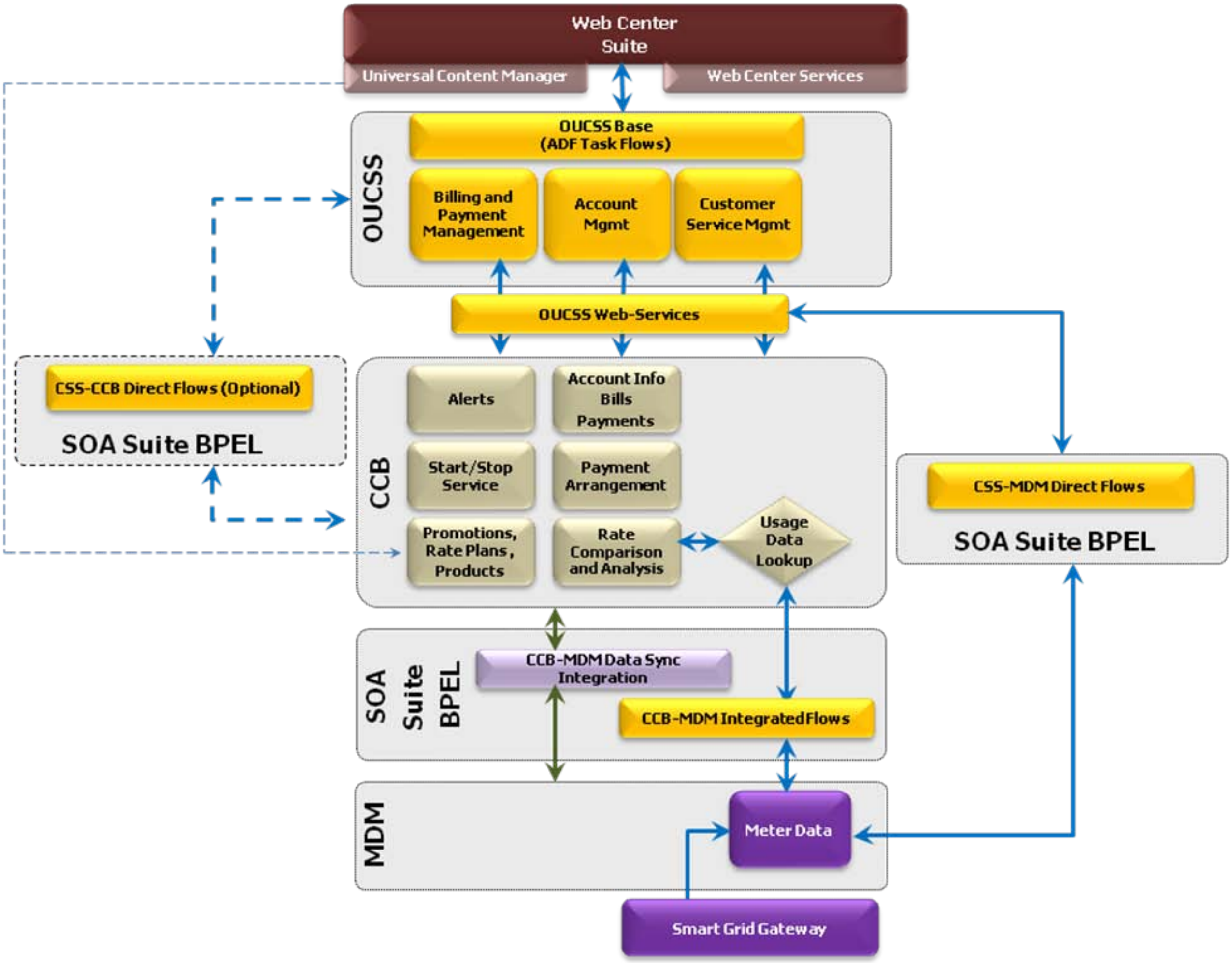
In addition the system provides a Web Service to enroll multiple users to a set of Accounts.

Technical Overview

Oracle Utilities Customer Self Service is based on service oriented standards based architecture and leverages industry leading Oracle application development technology.

- Portal/Taskflow components are developed using Oracle Application Development Framework (ADF) 11g and are packaged as ADF shared library.
- Taskflows/Portlets are pre-integrated with Oracle Utilities Customer Care and Billing, Oracle Utilities Meter Data Management and Oracle Utilities Network Management System applications using a standards-based Web Service API and Oracle SOA Suite.
- Oracle WebCenter 11g is the recommended portal platform for consumption with the following approaches:
  - OUCSS taskflows consumed directly in WebCenter Custom Portal application.
  - OUCSS taskflows can also be consumed as WSRP 2.0 portlets in WebCenter Custom Portal application
  - OUCSS Portal application based on Oracle WebCenter Framework (with preconfigured security, navigation model and page templates) is provided with the release package to facilitate implementation and development activities.

OUCSS Architecture



OUCSS Architecture diagram with CSS-MDM direct flows

Additional Resources

Resource	Location
Securing WebCenter Portal Application	http://docs.oracle.com/cd/E29542_01/webcenter.1111/e63259/jpsdg_security.htm
Customizing Taskflows : Oracle WebCenter Spaces	http://docs.oracle.com/cd/E29542_01/webcenter.1111/e63259/jpsdg_taskflows.htm
Customize and Extend OUCSS Portal Customizing and Extending the OUCSS Custom Portal Whitepaper OUCSS Implementation Guide OUCSS Install Guide	Available for download in the Oracle Utilities Customer Self Service section of the Oracle Utilities Documentation area on the Oracle Technology Network (OTN) web site (http://www.oracle.com/technetwork/apps-tech/utilities/documentation/index.html).

Note: This document and the documentation mentioned above are subject to revision and updating. For the most recent version of this and related documentation, as well as information on functionality and known issues for other Oracle products that may be required for installation and proper functionality of this product, check the Oracle Utilities Customer Self Service section of the Oracle Utilities Documentation area on the Oracle Technology Network (OTN) web site (http://www.oracle.com/technetwork/apps-tech/utilities/documentation/index.html).

Chapter 2

OUCSS Security

OUCSS Overview

The OUCSS solution is implemented as ADF taskflows. These taskflows are consumed in an ADF application (such as WebCenter Portal). To allow flexibility in consuming OUCSS taskflows, the security is implemented in two tiers.

- **Tier-1 Security**: This security is implemented by the consuming application (e.g. OUCSS Portal). The Tier-1 security handles login (authentication) as well as authorization. The pages containing OUCSS taskflows are secured and are accessed through specific roles only. The consumer application manages page security.
- **Tier-2 Security** controls actions and fields within taskflows/modules. This controls the actions a logged user is allowed based on the access role associated with the selected account. The access control is configured and controlled using the OUCSS Security admin page and saved in the OUCSS schema. Tier-2 security is not possibile for public or pages that do not involve an account selection (e.g., User Profile).

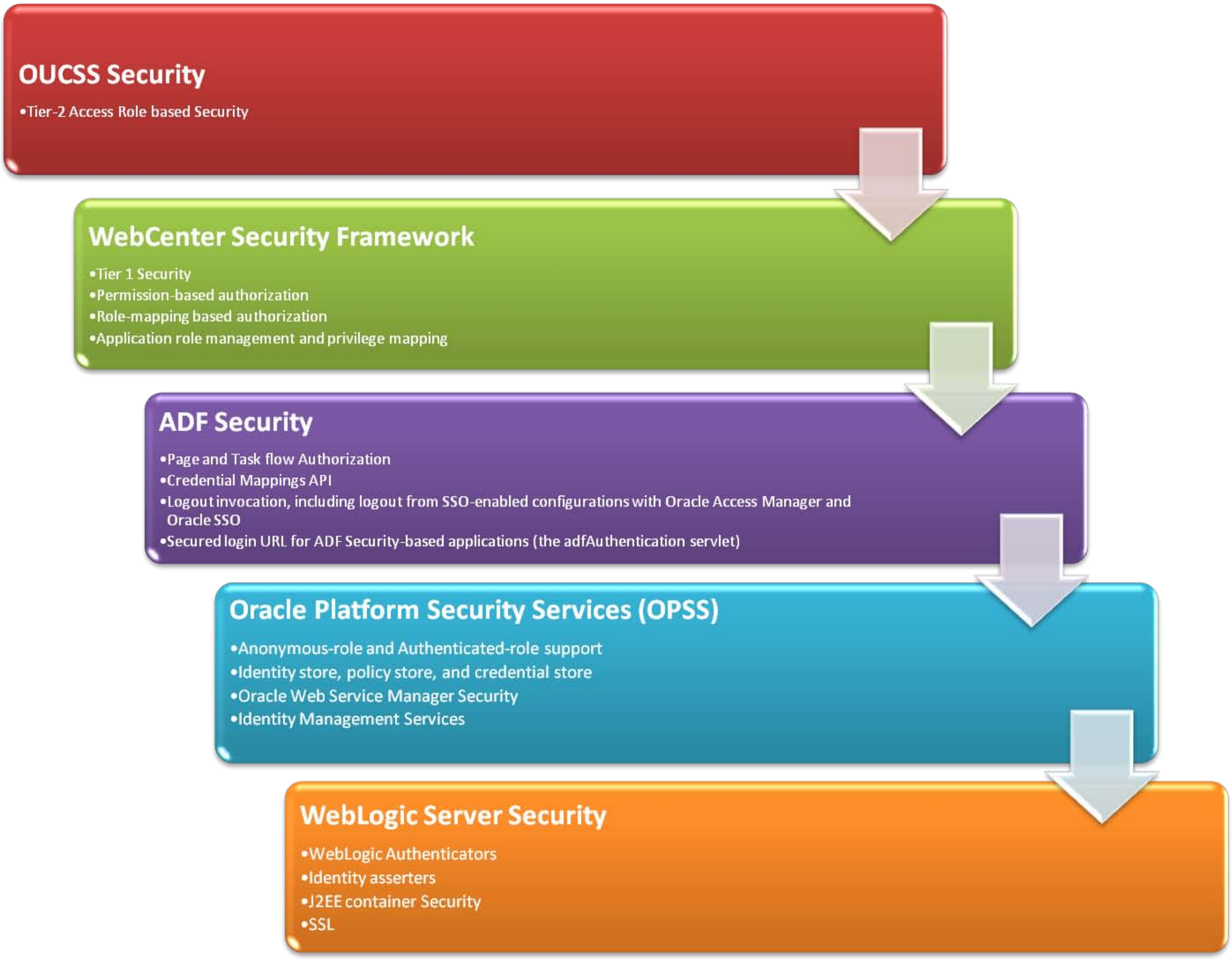
OUCSS Portal (Tier-1) Security

The OUCSS Portal is built using the WebCenter Portal Application framework. Portal Framework applications are dynamic and often involve input from users in the form of customizations and preferences, and consequently require a flexible security model. The WebCenter security model is based on the ADF security model rather than the more traditional J2EE security model.

For more information on Portal security, see the "Securing Your WebCenter Portal Framework Application" chapter in *Oracle® Fusion Middleware Developing Portals with Oracle WebCenter Portal and Oracle JDeveloper*.

The ADF Security framework is the preferred technology to provide authentication and authorization services to a Fusion Web application. ADF Security is built on top of the Oracle Platform Security Services (OPSS) architecture, which itself is well-integrated with Oracle WebLogic Server.

For more information on ADF security, see the "Enabling ADF Security in a Fusion Web Application" chapter in the *Oracle® Fusion Middleware Fusion Developer's Guide for Oracle Application Development Framework*.


OUCSS Security
•Tier-2 Access Role based Security
WebCenter Security Framework
•Tier 1 Security
•Permission-based authorization
•Role-mapping based authorization
•Application role management and privilege mapping
ADF Security
•Page and Task flow Authorization
•Credential Mappings API
•Logout invocation, including logout from SSO-enabled configurations with Oracle Access Manager and Oracle SSO
•Secured login URL for ADF Security-based applications (the adfAuthentication servlet)
Oracle Platform Security Services (OPSS)
•Anonymous-role and Authenticated-role support
•Identity store, policy store, and credential store
•Oracle Web Service Manager Security
•Identity Management Services
WebLogic Server Security
•WebLogic Authenticators
•Identity asserters
•J2EE container Security
•SSL

OUCSS Portal Security Layers

Reference Security Roles

Most of the pages in the application are secured and are accessed only by specific enterprise groups/roles. Some pages are public and can be accessed by any user without logging in.

As part of the default implementation, two enterprise groups and two users are imported into LDAP as part of the OUCSS installation. The enterprise groups are used to differentiate regular users from Admin and CSR users.

Pre-defined ADF Roles

ADF Security (which is implemented using OPSS) provides the following built-in roles. OUCSS uses the the following roles to secure taskflows and other portal resources for regular (non Admin/non CSR) users.

- **anonymous-role:** means the resource will be accessible to anyone who visits the site. A grant to this role is necessary if you want to make a Web page associated with an ADF security-aware resource accessible before a user logs in. For example, you would grant to **anonymous-role** for a taskflow that manages customer registration. All Public Pages and taskflows are granted this role in the OUCSS Portal.
- **authenticated-role:** means the resource will be accessible only to authenticated users (users who visit the site and log in). For example, you would grant to **authenticated-role** for an account list taskflow. All Secured Pages and taskflows are granted this role in the OUCSS Portal

Enterprise Groups/Roles

Apart from the above pre-defined roles, There are two enterprise groups available in the OUCSS Portal application.

- **WSSAdminGroup:** Users who belong to this enterprise group serve as administrators of the OUCSS application. Ideally, system administrators will be members of this group. **WSSAdminGroup** belongs to the **WSSCSRGroup**. All Admin Pages are granted these roles.
- **WSSCSRGroup:** Users who belong to this enterprise group can perform CSR-related functions. Ideally, the CSRs who directly interact with consumers will be members of this group.

Pre-configured Users

- **WSSAdmin** is the administrator of OUCSS Portal . This user can manage all resources of the OUCSS Portal. The **WSSAdmin** user is a member of **WSSAdminGroup**.
- **WSSCSR** is provided for a certain group of users that need to perform CSR-related functions. This user is part of **WSSCSRGroup** and can carry out the actions by impersonating any registered user who has access to a utility account.

Portal Application

Pages

The OUCSS Portal allows any user access to public pages such as Home, Register, Reset Password, etc. It also implements secured pages related to an individual's accounts.

Public Pages

- Home
- Login
- Outage
- Register
- Outages
    - Display Map
    - Display List
    - Report Public Outage

Public Hidden Pages

- Forget User ID/Password
- Page Not Found
- UnAuthorized Page
- Error Page
- Validate Email

Secured Pages

Secured pages can be accessed only by authenticated users.

Desktop

- Accounts
- Details
  - Dashboard
  - Financial History
  - Budget Billing (Post Paid accounts only)
  - View Bill
  - Payment Arrangement (Post Paid accounts only)
  - Compare Rates
  - Usage Details
  - Personal Information
  - My Outages
  - Report Outage (Premise)
  - Start Service
  - Stop Service
  - Transfer Service
  - Account Documents
- Notification
  - Inbox
  - Profile
  - Preferences
- New Customer
- User Profile
- Forms Management
  - Log an Issue
  - Form List

- Old (Supported) Portlets
  - Billing History
  - Usage Details
- Multi-Account
  - Set Accounts
  - Financial History
  - Usage Compare
  - Usage Aggregate

Mobile

- Accounts
- Dashboard
  - Change Account Access
  - Account Summary (Postpaid Accounts)
  - Alerts
  - Service Charge To Date
  - Consumption Summary
  - Usage Overview
  - Financial History
  - View Bill
  - Automatic Payment
  - Prepaid Balance And Charges (Prepaid Accounts)
  - Prepaid Estimate And Cost (Prepaid Accounts)
  - My Outages
  - Report Outage (Premise)
  - Promotion & Offers
  - Log an Issue
  - Form List
  - Inbox
  - Profile
  - Preferences

Hidden Secured Pages

Desktop

- One Time Payment
- Add Scalar Read

- Manage Address
- Manage Phone
- Manage Electronic Bill Option
- Manage Billing Notification Preference
- Manage Automatic Payment Option

Mobile

- One Time Payment
- Add Scalar Read
- Manage Automatic Payment Option

Admin Pages

Admin pages are accessible only by WSSAdminGroup users. The **Customer Search** page is also accessible by members of WSSCSRGroup.

- Customer Search (also accessible by members of WSSCSRGroup)
- Configuration Options
- Resources
- Access
- Security
- Edge Application
- Line of Business
- Portlets
- Language
- Labels
- Lookup
- Messages
- Train
- Offers

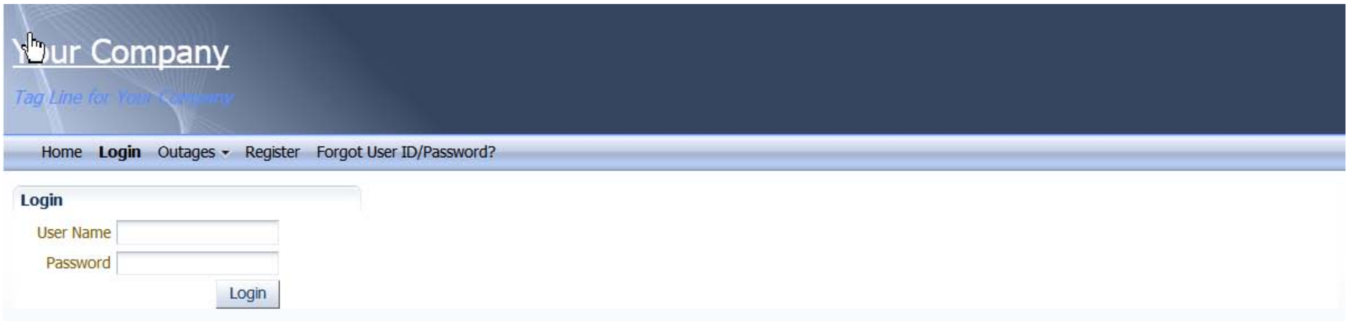
Login Configuration

The OUCSS Portal supports consolidated account login or a LOB-based context login (e.g., Residential, Commercial, etc.). Each context can be customized to use separate Page Templates, Navigation, and pages. Please see the *OUCSS Implementation Guide* for more details.

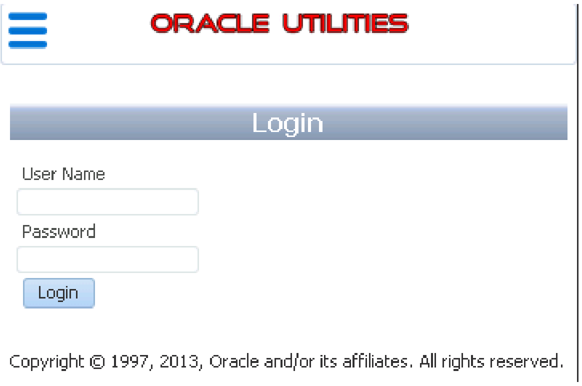
Consolidated Account Login

The lob/context selection is hidden when consolidated account is enabled in OUCSS Login taskflow. The context is null (no context) in this mode. The selection of Portal Resources is determined based on the account selected by the user. For example, if the user clicks on Residential Account, then the Portal Resources configured for Residential LOB are loaded.

Desktop



Mobile



Copyright © 1997, 2013, Oracle and/or its affiliates. All rights reserved.

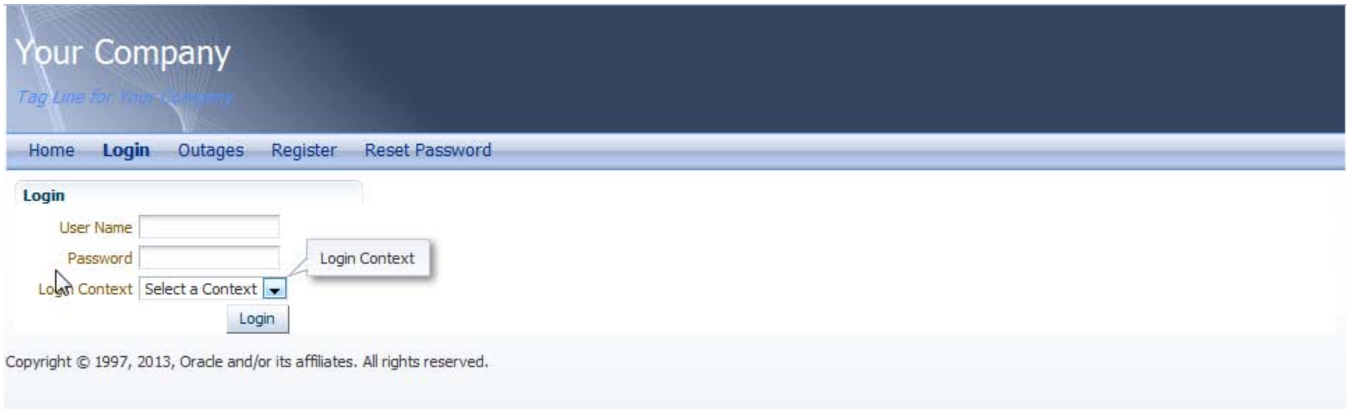
LOB Context Login

If the consolidated account mode is disabled, then the Login taskflow enables selection of an LOB to filter the accounts. The Portal resources (Page Templates, Navigation model, skins, etc.) are pre-select based on the selected LOB.

Generic Context Login

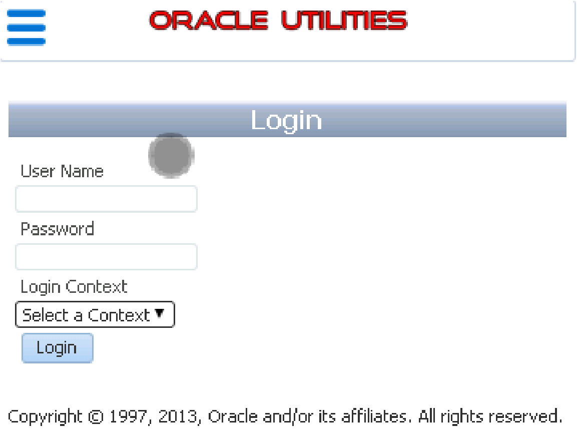
By default, when the Login taskflow is generic, the LOB taskflow parameter is empty. In this mode, a list box is shown to allow users to select the Context and enter username and password credentials at the time of Login.

Desktop



Copyright © 1997, 2013, Oracle and/or its affiliates. All rights reserved.

Mobile

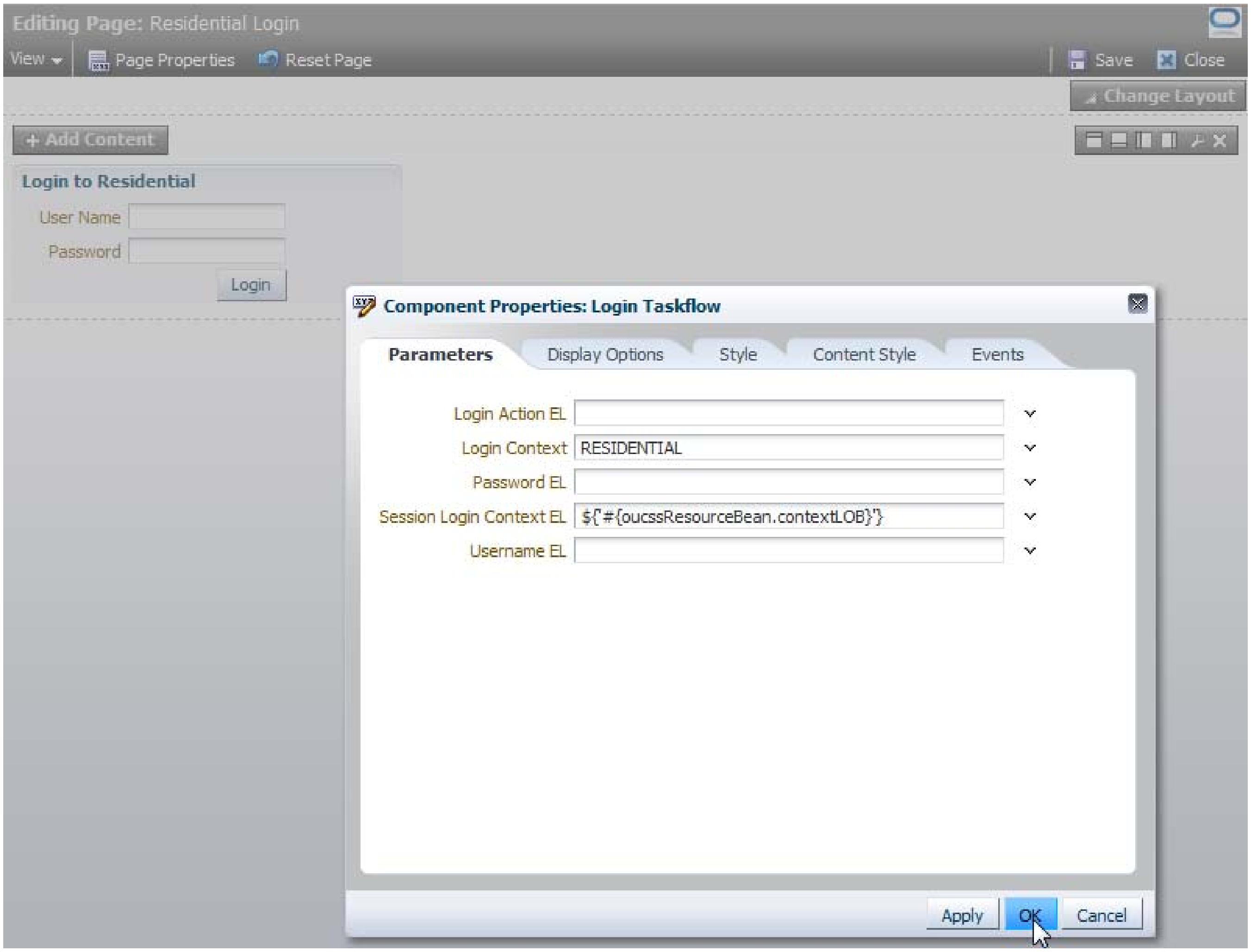


Copyright © 1997, 2013, Oracle and/or its affiliates. All rights reserved.

Login to a Specific LOB

To create a Context Specific taskflow, drop the Login taskflow and update the **Login Context** input parameter with the LOB code defined in the OUCSS Lob table. This will enable the Login to log in with the configured context.

Also, to set the Context into session, update the **Session Login Context EL** with EL to store the context. For the OUCSS Portal, use the EL `${'oucssResourceBean.contextLOB'}`.



Editing Page: Residential Login

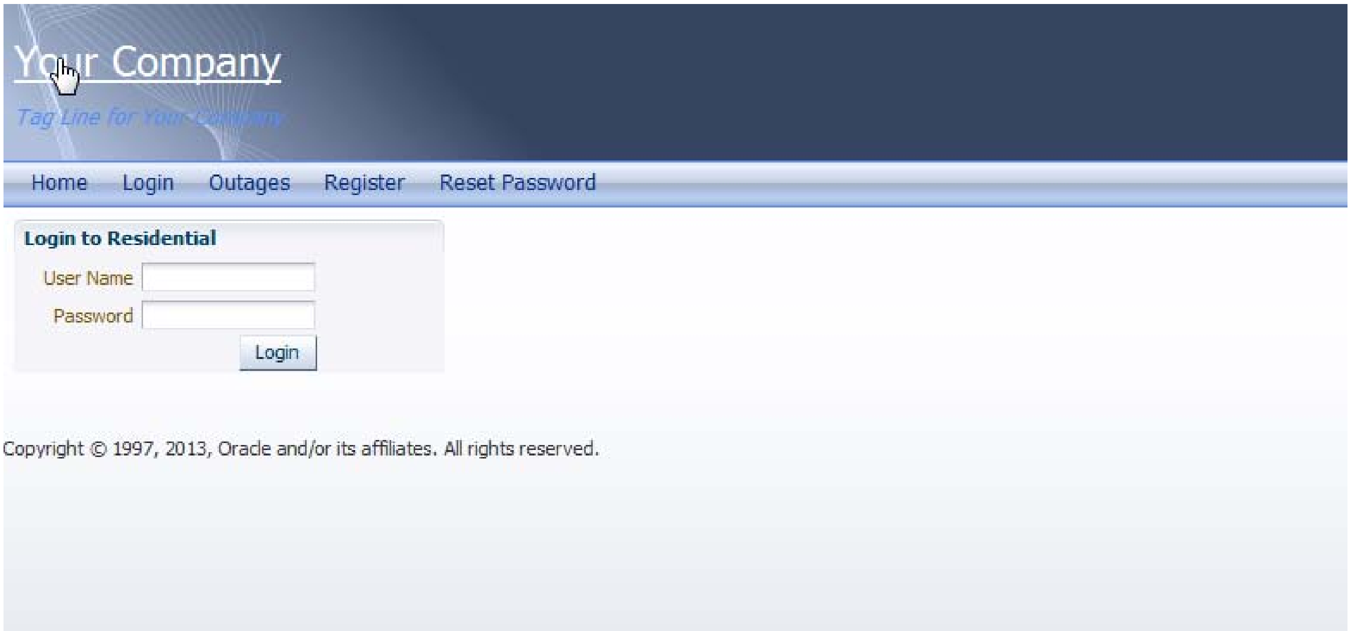
Login to Residential

User Name

Password

Component Properties: Login Taskflow

Login Action EL	
Login Context	RESIDENTIAL
Password EL	
Session Login Context EL	${'#{oucssResourceBean.contextLOB}'}
Username EL	



Your Company

Tag Line for Your Company

Login to Residential

User Name

Password

OUCSS Tier-2 Security

Taskflow/Portlet Security Overview

The Tier 2 security controls access to the links and buttons on the taskflows/portlets. The access rights for a logged in user are loaded from the database based on the configuration.

Taskflow/Portlet security restricts access to its transactions as follows:

- Each taskflow/portlet must be defined in Portlets table with a list of actions allowed for this portlet.
- Available actions should be defined for each Line Of Business and Access Role. Each user has a Line Of Business and Access Role.
- Specific user interface components (buttons, links) can be hidden or visible based on the access role.

When you grant an **Access Role** access to a portal, you must also define the permitted action.

For example, you may indicate a Line Of Business/Access Role has inquire-only access to a taskflow/portlet , whereas another role may also have change privilege to the same taskflow/portlet.

How to Configure Security Settings

In order to add or change security settings, the user must log in to the system as administrator.

> **Note:** Changes in security for a specific user or group of users will be visible in the system only after the user logs out and logs in again.

User

A link between Line of Business/Access Role and User is established when the user enrolls/registers to an account.

A new link between User and Access Role is also established when a user is invited to an account. If the access is revoked, this link is removed.

Security

Go to the **Admin** group on the **Top** menu, then choose **Security**.

For each combination of Line of Business and Access Role, specify portals/taskflows that a user can access and list of actions that can be performed.

Field Level Security

Specific user interface components (buttons, links) can be hidden or made visible, based on the access role.

The Java Managed Bean of each mobile exposes a methods to check for permissions. The methods **isReadPermission()**, **isUpdatePermission()** and **isAddPermission()** are used to check for **Read/View**, **Update**, and **Add** permissions, repectively.

For example, to show or hide the **Update** button on the **View Mailing** address taskflow/portlet, the rendered property of the button is set to use the **isUpdatePermission** method (EL corresponds to #{bean.**updatePermission}**).

```
<af:commandButton text="#{ssBundle.ACCOUNT_UPDATE_LBL}"
              partialSubmit="true" id="amupclnk"
              inlineStyle="white-space:nowrap"
              disabled="#{pageFlowScope.accountAddressManagedBean.updatePageURL eq null}"
```

```
                rendered="#{pageFlowScope.accountAddressManagedBean.updatePermission}">
```

Securing ADF/Web Service Connections

Security Credentials

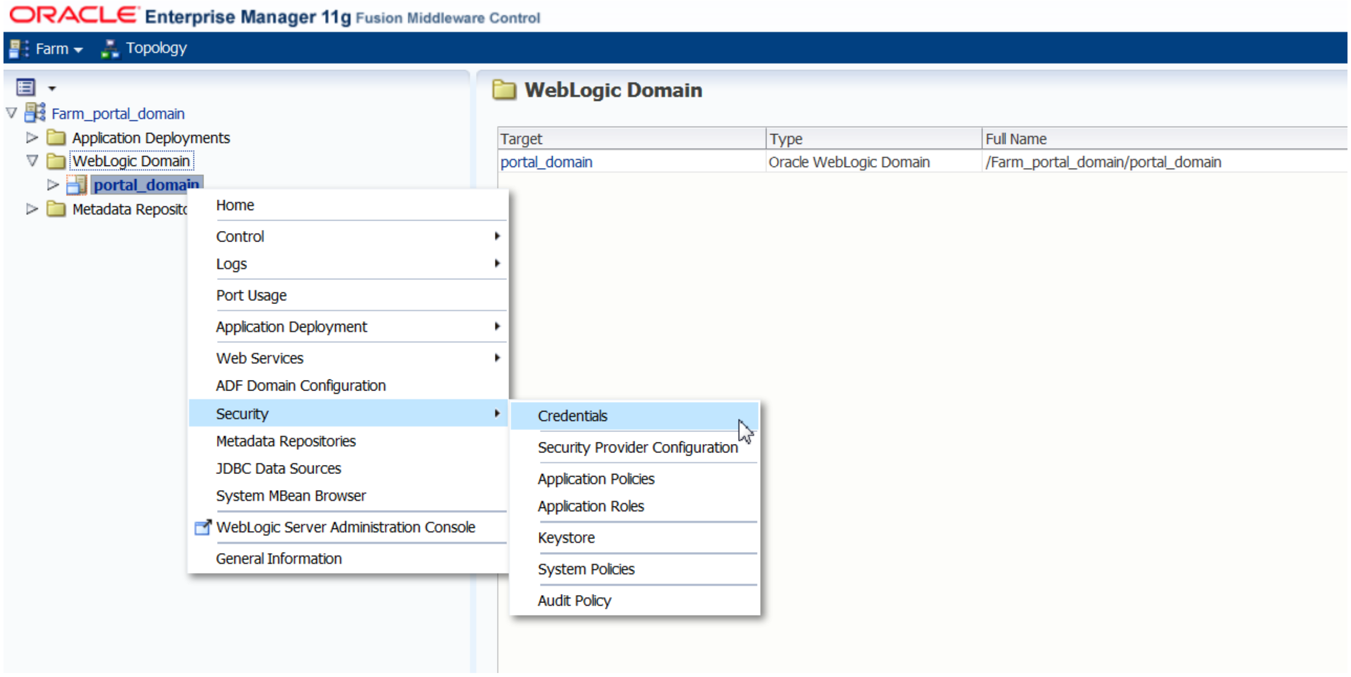
OUCSS taskflows retrieve data from edge applications (CCB, MDM, etc.) using Web Services. These Web Service calls are secured using OWSM policies. The policy used is **wss_http_token_client_policy**, and the required CSF Keys are automatically created on installation.

The connections use one of the following CSF Keys declared Security Credentials:

- **OUCSS_XAI_BASIC_KEY:** configured to CCB credentials and is used with CCB connections.
- **OUCSS_INTG_BASIC_KEY:** configured to SOA credentials and is used with MDM, NMS and other SOA connections.
- **OUCSS_OUNC_BASIC_KEY**: configured with OUNC SOA server credentials and used with OUNC connections.

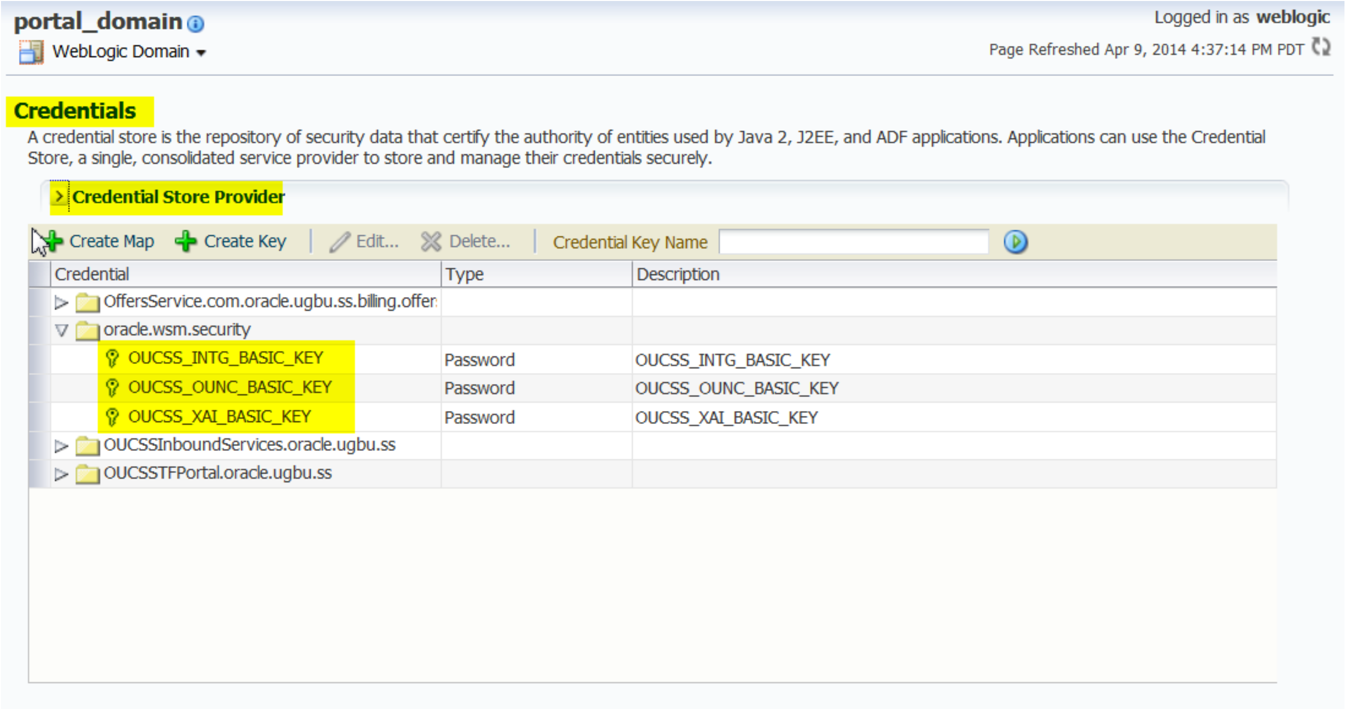
To add or modify credentials:

1. Log in into the Oracle Enterprise Manager console at `http://<WLSAdminHost>:<WLSAdminServerPort>/em` as WLS Admin.
2. Select **Weblogic_Domain**, then <**portal_domain_name**>.
3. Click <**portal_domain_name**>, then choose **Security** > **Credentials**, as shown in the following image:



Target	Type	Full Name
portal_domain	Oracle WebLogic Domain	/Farm_portal_domain/portal_domain

4. Under **Credentials** select and expand `oracle.wsm.security`. **OUCSS_XAI_BASIC_KEY**, **OUCSS_INTG_BASIC_KEY**, and **OUCSS_OUNC_BASIC_KEY** should be present, as shown in the following image:



portal_domain

WebLogic Domain

Logged in as weblogic

Page Refreshed Apr 9, 2014 4:37:14 PM PDT

Credentials

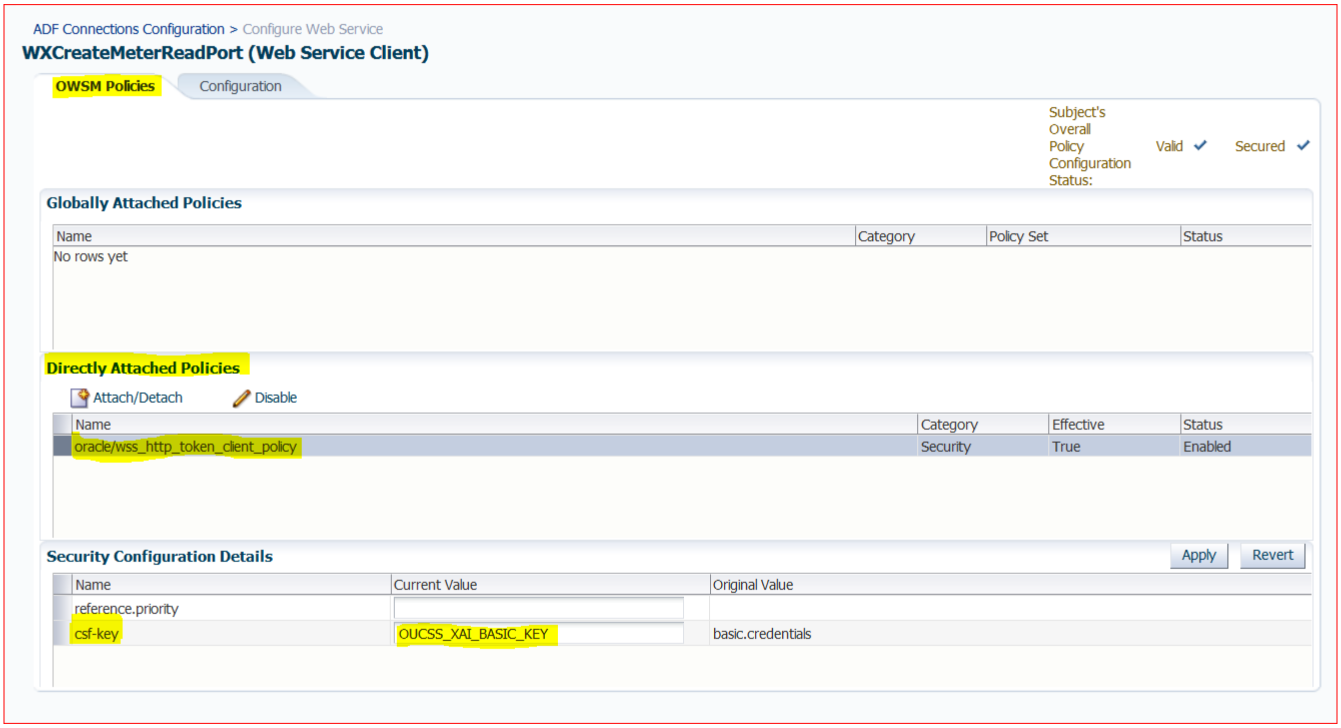
A credential store is the repository of security data that certify the authority of entities used by Java 2, J2EE, and ADF applications. Applications can use the Credential Store, a single, consolidated service provider to store and manage their credentials securely.

Credential Store Provider

Credential	Type	Description
▷ OffersService.com.oracle.ugbu.ss.billing.offer		
▽ oracle.wsm.security		
OUCSS_INTG_BASIC_KEY	Password	OUCSS_INTG_BASIC_KEY
OUCSS_OUNC_BASIC_KEY	Password	OUCSS_OUNC_BASIC_KEY
OUCSS_XAI_BASIC_KEY	Password	OUCSS_XAI_BASIC_KEY
▷ OUCSSInboundServices.oracle.ugbu.ss		
▷ OUCSSTFPortal.oracle.ugbu.ss		

To modify the CSF Key associated with a Connection:

1. Login to Enterprise Manager.
2. Click on the deployed application (e.g., **OUCSSPortal**).
3. From the **Application Deployment** menu select **ADF > Configure ADF Connections**.
4. Select the target connection and click **Edit**.
5. Open the **Advanced Connection Configurations** menu and select the port to update the OWSM Policies.
6. Select the **OWSM Policies** tab and select the `oracle/wss_http_token_client_policy` in the **Directly Attached Policies** table.
7. Update the csf-key to modify the key to be used.



WXCreateMeterReadPort (Web Service Client)

Subject's Overall Policy Configuration Status: Valid ✓ Secured ✓

Globally Attached Policies

Name	Category	Policy Set	Status
No rows yet			

Directly Attached Policies

Name	Category	Effective	Status
oracle/wss_http_token_client_policy	Security	True	Enabled

Security Configuration Details

Name	Current Value	Original Value
reference.priority		
csf-key	OUCSS_XAI_BASIC_KEY	basic.credentials

Chapter 3

OUCSS Inbound Services Security

The following applications are deployed as part of the OUCSS Inbound Services application.

- OUCSS Offers Web Services
- Account Enroll Service
- OUCSS Rest Services

The OUCSS Offer Web Service

This service is implemented using ADF BC and is exposed as a Web Service. It uses the Offer Set Code and Locale to fetch the required data from Offers tables in the OUCSS schema. The Offer taskflows use this data and renders it in the required format.

By default the Offers Web Service is not secured. Implementation can secure the Web Service by adding an OWSM policy using Enterprise Manager. If the Web Service is secured, then the Offer Service connection needs to be attached with the required OWSM policy.

Securing Offer Web Service (Producer)

The following procedure describes how to to secure the Offer Service.

1. Login to Enterprise Manager.
2. Click on the **OUCSSInboundServices** deployed application to go to the application page.
3. Select **Web Services** from the **Application Deployment** menu.
4. From the Web Service table, click **OffersServiceSoapHttpPort** to modify the port details.
5. Goto the **OWSM Policies** tab. Click the **Attach/Detach** button with the desired policy to secure the Web Service.

Attach OWSM Policy (Consumer)

The following procedure describes how to implement and use your own Web Service.

1. Login to Enterprise Manager.
2. Click on the deployed application (e.g., **OUCSSPortal**).
3. From the **Application Deployment** menu select **ADF > Configure ADF Connections**.
4. Select the **Offers Service** connection and click **Edit**.
5. Open the **Advanced Connection Configurations** menu and select the port to update the OWSM Policies.
6. Select the **OWSM Policies** tab.
7. Attach the policy in order to invoke the secured Web Service.
8. Click **Apply** again to commit the changes to the Offer Service connection.

Account Enrollment Web Service

This Web Service provides operations to enroll multiple users to a set of Accounts or to manage users. Users may or may not be registered in the Self-Service application.

Security

The Account Enroll service is secured using the OWSM server policy `oracle/multi_token_rest_service_policy`. See http://docs.oracle.com/cd/E28280_01/web.1111/b32511/policies.htm#CJAIEDEG for more information on this policy.

This policy enforces one of the following authentication policies, based on the token sent by the client:

- **HTTP Basic** - Extracts the username and password credentials from the HTTP header.
- **SAML 2.0** - Bearer token in the HTTP header. Extracts SAML 2.0 Bearer assertion in the HTTP header.
- **HTTP OAM** security - Verifies that the OAM agent has an authenticated user and establishes the user's identity.
- **SPNEGO over HTTP** security - Extracts Simple and Protected GSSAPI Negotiation Mechanism (SPNEGO) Kerberos token from the HTTP header.

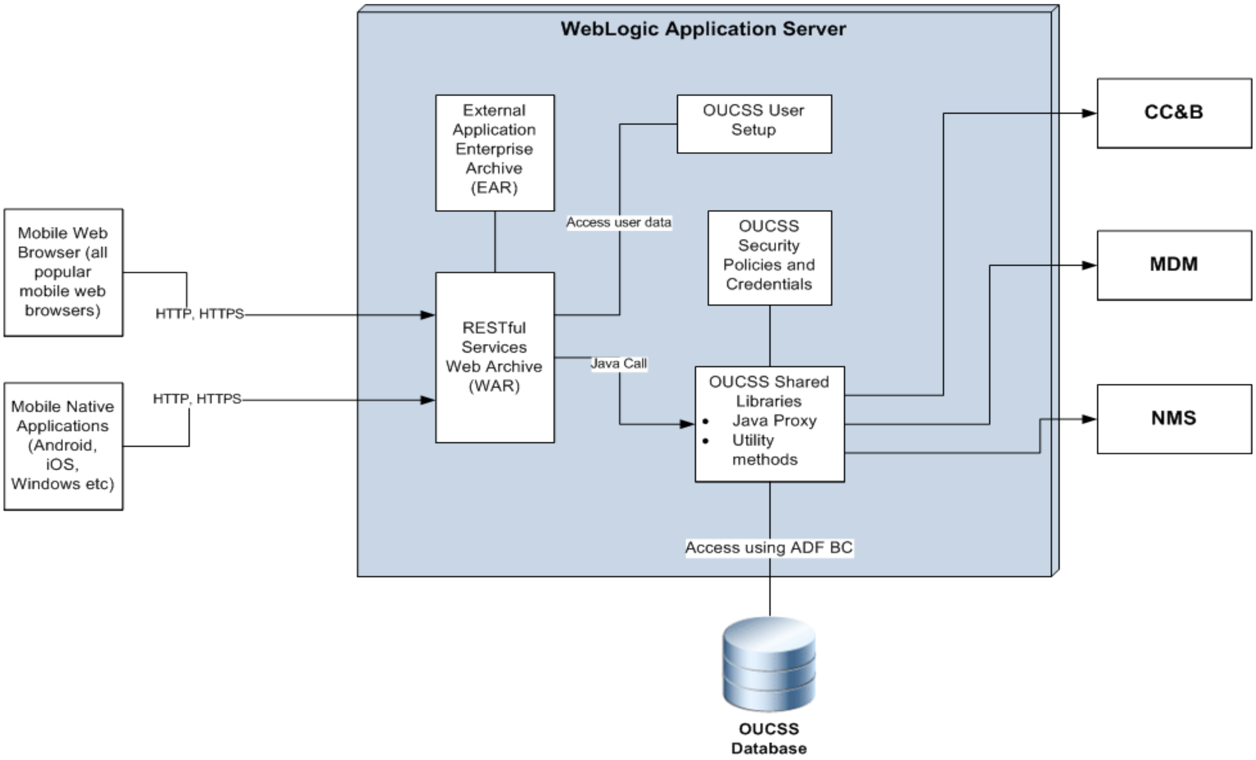
How to Invoke the Web Service

- The Account Enrollment Web Service is deployed as part of a separate application called **OUCSSInboundServices**.
- The URL is `http://<<server>>:<<port>>/ <<context>>/AccountEnrollService?wsdl`, where `server` and `port` reflect the information provided in the **deployTarget** section of **oucssInbound** in `InstallProperties.xml`.
- Select the **Operation** to call when invoking the Web Service.
- Provide the security credentials (e.g., use the HTTP Authorization header with base 64-encoded username/password).
- Based on the **Operation** selected, populate the request and invoke the service.
- If the call is successful, a SUCCESS message is returned. Otherwise, any errors are returned in the output.

OUCSS Rest Services

OUCSS REST services are RESTful (Representation State Transfer) Web Services created mainly to be consumed by mobile applications and to provide the Core OUCSS features on a mobile platform. Most of the REST services in turn use the SOAP XAI/BPEL services to retrieve data from edge applications. A Web Service proxy is created for each of the SOAP XAI/BPEL Web Services. A few REST services are created to retrieve data from the OUCSS Admin database.

The REST Service uses Jersey JAX-RS and Jackson libraries which are part of the `jersey_bundle 1.9` shared libraries shipped as part of WebLogic Server. The REST service produces either JSON or XML output based on the media type set for “Accept” header of the HTTP request.


WebLogic Application Server
External Application Enterprise Archive (EAR)
OUCSS User Setup
Access user data
OUCSS Security Policies and Credentials
Mobile Web Browser (all popular mobile web browsers)
HTTP, HTTPS
RESTful Services Web Archive (WAR)
Java Call
Mobile Native Applications (Android, iOS, Windows etc)
HTTP, HTTPS
OUCSS Shared Libraries
• Java Proxy
• Utility methods
CC&B
MDM
NMS
Access using ADF BC
OUCSS Database

REST Security

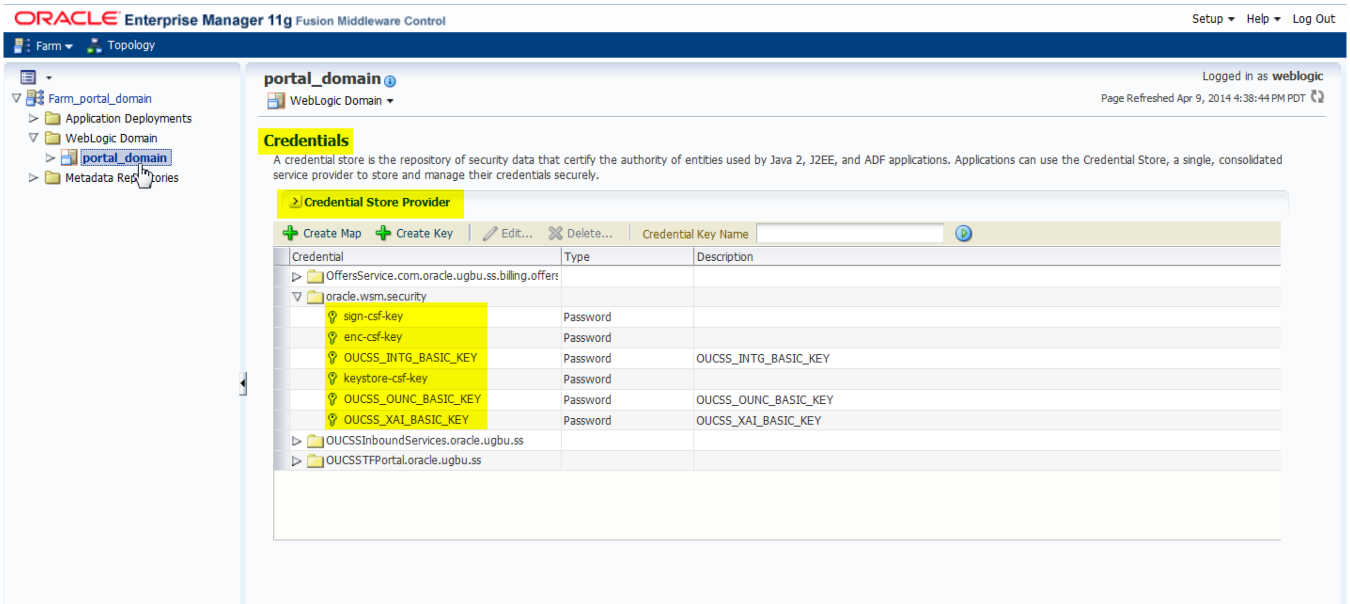
REST services are secured using the policy **oracle/multi_token_rest_service_policy**. See http://docs.oracle.com/cd/E28280_01/web.1111/b32511/policies.htm#CJAIEDEG for more information on this policy.

One of the ways to authenticate is through Basic authentication.

Security Credentials

As part of install, the CSF keys related to the keystore are created.

1. Perform the steps described in the Security Credentials section to go to the **Credentials** screen in EM.
2. Under **Credentials**, select and expand `oracle.wsm.security` and add/modify the following CSF-Keys:
   - `keystore-csf-key`
   - `sign-csf-key`
   - `enc-csf-key`



A credential store is the repository of security data that certify the authority of entities used by Java 2, J2EE, and ADF applications. Applications can use the Credential Store, a single, consolidated service provider to store and manage their credentials securely.

Credential	Type	Description
OffersService.com.oracle.ugbu.ss.billing.offers		
oracle.wsm.security		
sign-csf-key	Password	
enc-csf-key	Password	
OUCSS_INTG_BASIC_KEY	Password	OUCSS_INTG_BASIC_KEY
keystore-csf-key	Password	
OUCSS_OUNC_BASIC_KEY	Password	OUCSS_OUNC_BASIC_KEY
OUCSS_XAI_BASIC_KEY	Password	OUCSS_XAI_BASIC_KEY
OUCSSInboundServices.oracle.ugbu.ss		
OUCSSTFPortal.oracle.ugbu.ss		

Creating a Security Keystore

Account Enroll and REST services are secured using the OWSM Policy. In order for these services to work, a keystore is required to be set up.

1. Go to `<<Java_Home>>/bin` and run the `keytool` command to generate a java keystore (jks). The Java keystore (jks) is required to authenticate and encrypt the messages by OWSM.

   Sample command:

   ```
   keytool -genkeypair -keyalg RSA -alias orakey -keypass <<sign-csf-key-password>> -
   keystore default-keystore.jks -storepass <<keystore-password>> -validity 3600
   ```

   - For **alias** use the username from `/oucssInstall/oucssConnection/OUCSS_Inbound/sign-csf in InstallProperties.xml`
   - For **keypass** use the password from `/oucssInstall/oucssConnection/OUCSS_Inbound/sign-csf in InstallProperties.xml`
   - For **storepass** use the password from `/oucssInstall/oucssConnection/OUCSS_Inbound/keystore-csf in InstallProperties.xml`

   See http://docs.oracle.com/javase/6/docs/technotes/tools/windows/keytool.html for more about the the Key and Certificate Management tool.

2. Copy the jks file created in step 1 to `<<Domain_Home>>/config/fmwconfig` folder. `<<Domain_Home>>` is the domain home in which the application is deployed.