Oracle Utilities
Customer Self Service

Security Guide

Release 2.2.0.0

E78232-01

August 2016

ORACLE

Oracle Utilities Customer Self Service Security Guide

Release 2.2.0.0

E78232-01

August 2016

Table of Contents

Chapter 1

Product Overview 5

Functional Overview 5

Technical Overview 7

OUCSS Architecture 7

Additional Resources 8

Chapter 2

OUCSS Security 9

OUCSS Overview 9

Portal (Tier-1) Security 9

Reference Security Roles 10

Pre-defined ADF Roles 10

Enterprise Groups/Roles 11

Pre-configured Users 11

Portal Application 11

Portal Pages 11

Self Service Portal (public) 11

Visible Public Pages 12

Hidden Public Pages 12

OUCSS Portal (oucss) 12

Visible Secured Pages 12

Hidden Secured Pages 13

Mobile Secured Pages 13

OUCSS Admin Portal (OUCSSAdmin) 14

Visible Secured Pages 14

Login Configuration 14
OUCSS Tier-2 Security 15
Taskflow/Portlet Security Overview 15
How to Configure Security Settings 15
User 15
Security 15
Field Level Security 15
Securing ADF/Web Service Connections 16
Security Credentials 16
Chapter 3
OUCSS Inbound Services Security 19
The OUCSS Offer Web Service 19
Securing Offer Web Service (Producer) 19
Attach OWSM Policy (Consumer) 20
Account Enrollment Web Service 20
Security 20
How to Invoke the Web Service 20
OUCSS REST Services 21
REST Security 21
Security Credentials 21
Creating a Security Keystore 22

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
  - Bill Charges Projection
  - 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

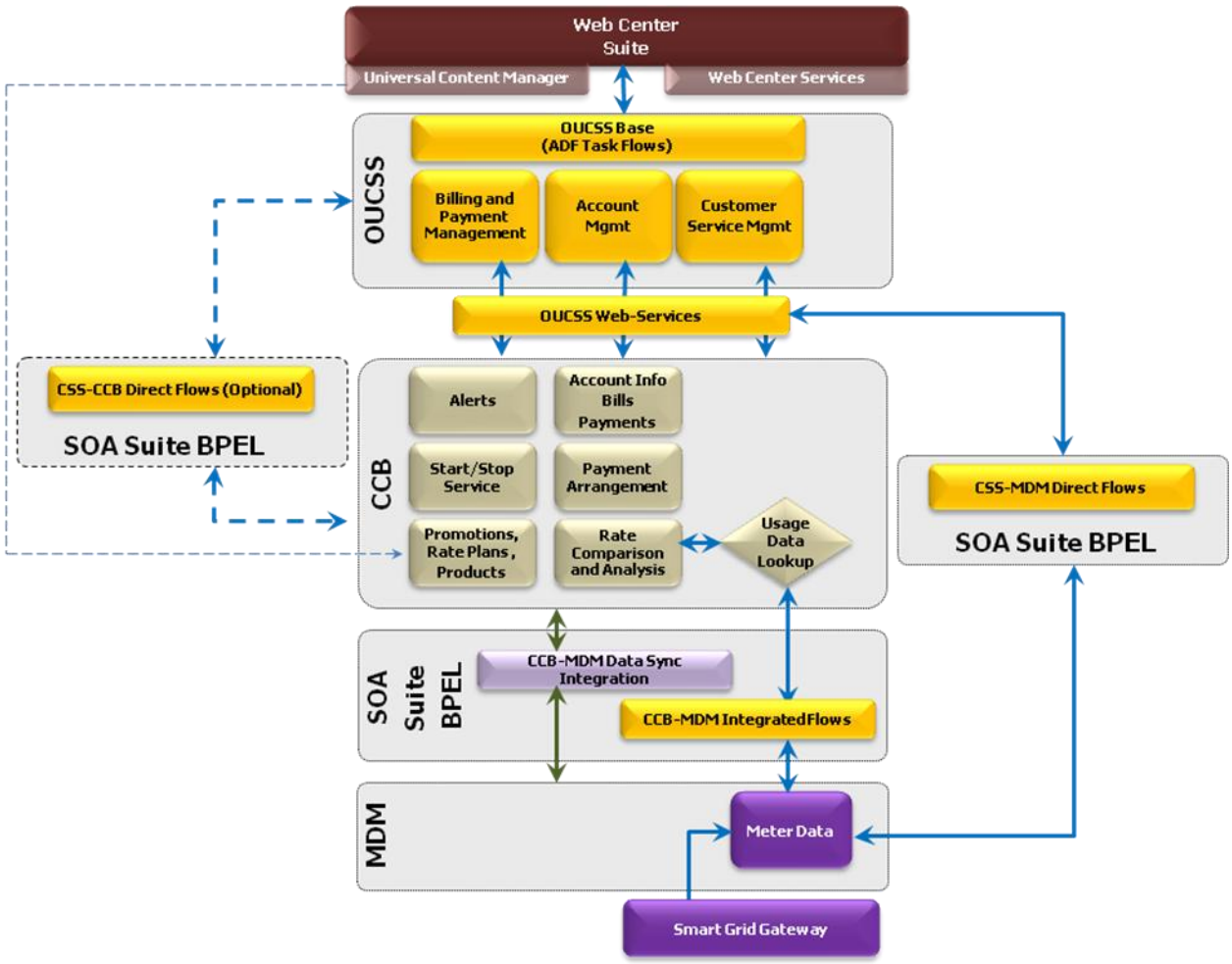
In addition the system provides a Web Service to enroll multiple users to a set of Accounts.

Technical Overview

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

- Portal/Taskflow components are developed using Oracle Application Development Framework (ADF) 12c and are packaged as ADF shared libraries.
- 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.
- OUCSS taskflows and shared libraries are consumed directly in WebCenter Portal 12c.

OUCSS Architecture



OUCSS Architecture diagram with CSS-MDM direct flows

Additional Resources

Resource	Location
Securing WebCenter Portal Application	http://docs.oracle.com/middleware/1221/wcp/wcp-secure.htm
Customizing Taskflows	https://docs.oracle.com/middleware/1221/wcp/admin/GUID-E2AE75D5-471D-4FEB-A61C-113D34E52FBC.htm#WCADM11677
Customizing and Extending the 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://docs.oracle.com/cd/E72219_01/documentation.html).

Note: This document and the documentation mentioned above is 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 Documentation area on the Oracle Technology Network (OTN) web site (http://docs.oracle.com/cd/E72219_01/documentation.html, then choose the Oracle Utilities Customer Self Service link).

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. WebCenter 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).

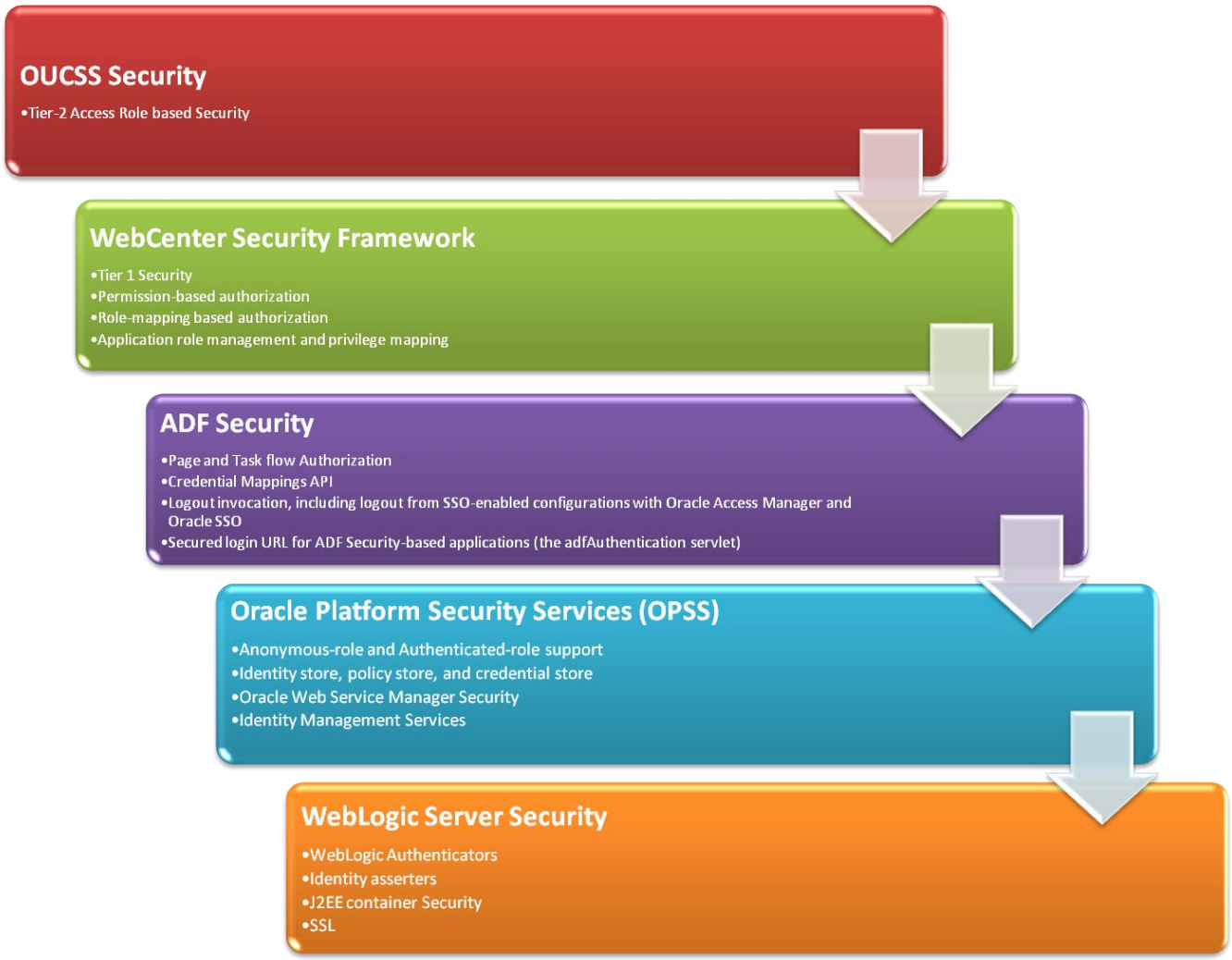
Portal (Tier-1) Security

The OUCSS solution is built using the WebCenter Portal 12c. WebCenter Portal application is 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 security documentation found at http://docs.oracle.com/middleware/1221/wcp/wcp-secure.htm.

The ADF Security framework is the preferred framework 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 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 Embedded 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 page that manages customer registration. All Public Pages 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 Portal application.

- **WSSAdminGroup:** Users of this enterprise group serve as administrators of the OUCSS application. Ideally, system administrators will be members of this group. **WSSAdminGroup** belongs to the **WSSCSRGroup**. Users of WSSAdminGroup are granted permission to access all Admin Pages and WebCenter Administrator Console.
- **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. Users of WSSAdminGroup are granted permission to access Customer Search Admin page.

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

Portal Pages

OUCSS solution imports three Portals (public, oucss and OUCSSAdmin) with pages containing OUCSS taskflows. the **Self Service** portal (public) contains all pages accessible by everyone/public users. The OUCSS Portal (oucss) contains pages that are secured and accessible only by authenticated/logged-in users. The **Admin** (OUCSSAdmin) contains admin and configuration pages that are accessible by Admin and CSR users.

The pre-configured **WSSAdmin** user is the moderator of all three Portals. This user has complete control of the portals and can add, modify, or delete any resource contained within the portals.

Portal Title	Portal Name	Accessibility	Description
Self Service	public	Public/Everyone	Portal containing public pages accessible by all users.
OUCSS Portal	oucss	Authenticated/Logged In users	Portal containing account/user related pages.
OUCSS Admin	OUCSSAdmin	WSSAdminGroup (all Pages) WSSCSRGroup (only the Customer Search page)	Portal containing admin/csr related pages.

Self Service Portal (public)

The **Self Service** Portal is a public portal to allow any user in the World Wide Web access to public pages such as Home, Login, Register, etc. This Portal is defined **public** and has no secured page.

Visible Public Pages

- Home
- Login
- Retrieve User
- Register
- Outage
- Outage Map
- Outage Table
- Report Outage

Hidden Public Pages

Apart from the public system pages provided by WebCenter Portal, the following are hidden pages in this Portal

- Validate Email

OUCSS Portal (oucss)

The **OUCSS** Portal is a secured portal to allow access only to authenticated users. This portal allows users to access account related pages like Dashboard, View Bill, Personal Information, etc. This Portal is defined private and has no public page.

Visible Secured Pages

- Home
- Accounts
- Details
  - Dashboard
  - Financial History
  - Budget Billing (Post Paid accounts only)
  - View Bill
  - Make Payment
  - 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
- Multi-Account
  - Set Accounts
  - Financial History
  - Usage Compare
  - Usage Aggregate
- Notification
  - Inbox
  - Profile
  - Preferences
- Forms
  - Log an Issue
  - Form List
- Outages
  - Display Map
  - Display List
  - Report Public Outage
- New Customer
- User Profile

Hidden Secured Pages

OUCSS Portal contains the following are hidden pages

- Add Meter Read
- Manage Address
- Manage Phone
- Manage Bill Notification
- Manage Electronic Bill
- Form Update
- Language & Timezone (for Update)

Mobile Secured Pages

OUCSS Portal contains the following are pages that are displayed when accessing the Portal using a mobile/smart phone. These pages breakdown complex pages (e.g. Dashboard) and display individual taskflows for better rendering.

- Change Account Access
- Account Summary
- Alerts

- Service Charges to Date
- Consumption Summary
- Usage Overview
- Manage Auto Pay
- Prepaid Balance and Changes
- Prepaid Estimates and Cost
- Promotions & Offers

OUCSS Admin Portal (OUCSSAdmin)

The **OUCSS Admin** Portal is a secured portal to allow access only to Admin and CSR users. This portal allows CSR users to access Customer Search page and Admin users to admin/configuration related pages like Resources, Labels, Lookups, etc. This Portal is defined hidden and has no public page.

Visible Secured Pages

- Customer Search
- Configuration Options
- Resources
- Access
- Security
- Edge Application
- Line of Business
- Portlets
- Language
- Labels
- Lookup
- Messages
- Train
- Offers

Login Configuration

The OUCSS Login taskflow 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 Login Configuration section in *OUCSS Implementation Guide* for more details

OUCSS Tier-2 Security

Taskflow/Portlet Security Overview

The Tier 2 security controls operations performed by users based on the access role by hiding and showing links and buttons on the taskflows views. 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 Security page in **OUCSS Admin** Portal.

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

Users are allowed specific operations (Add, Update etc) by hiding/showing user interface components (buttons, links) 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

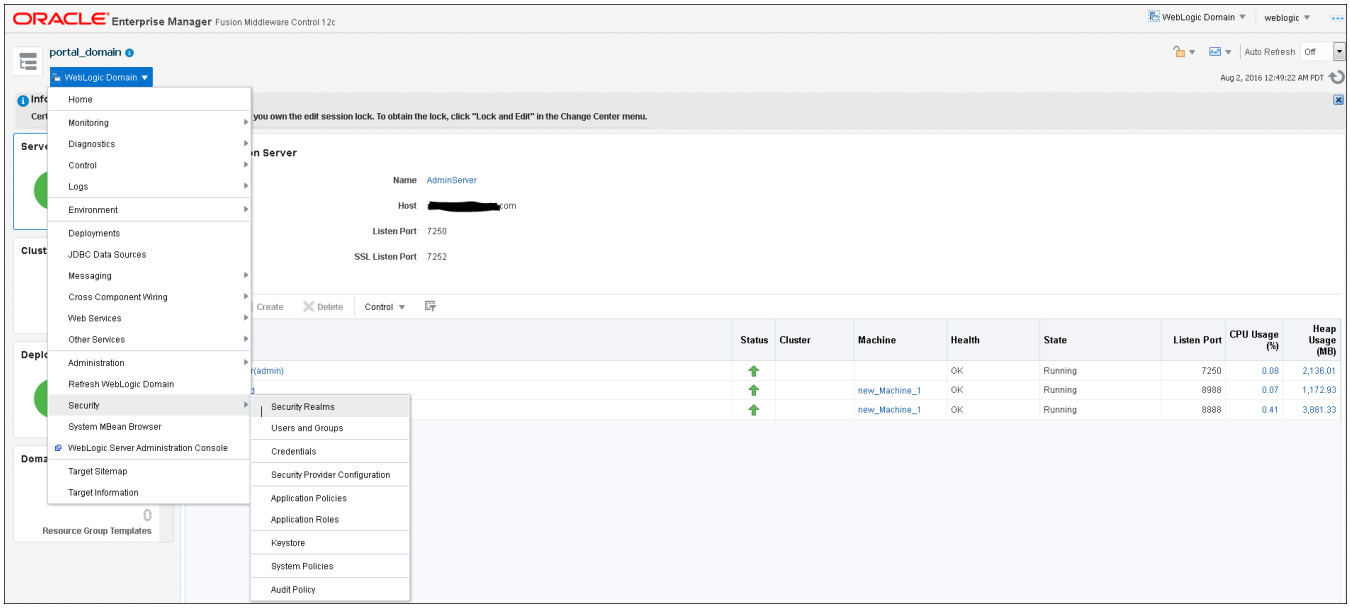
OUCSS taskflows retrieve data from edge applications (CCB, MDM, etc.) using Web Services. These Web Service calls are secured using OWSM policies. Based on the security annotation configured in Edge Application, one of the following WSM policies is used **wss_http_token_client_policy, wss_http_token_over_ssl_client_policy, wss_username_client_policy** to pass the user credential. The required CSF Keys are automatically created on installation.

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

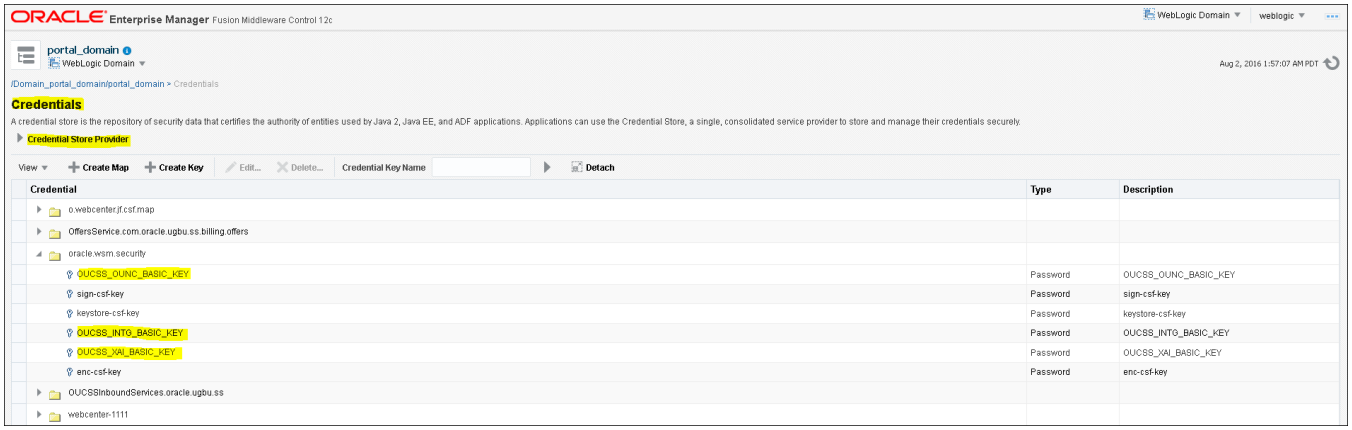
- **OUCSS_XAI_BASIC_KEY:** configured to CCB credentials and is used with CCB connections.
- **OUCSS_INTG_BASIC_KEY:** configured to SOA credentials and is used with MDM, NMS and other SOA connections.
- **OUCSS_OUNC_BASIC_KEY**: configured with OUNC SOA server credentials and used with OUNC connections.

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:

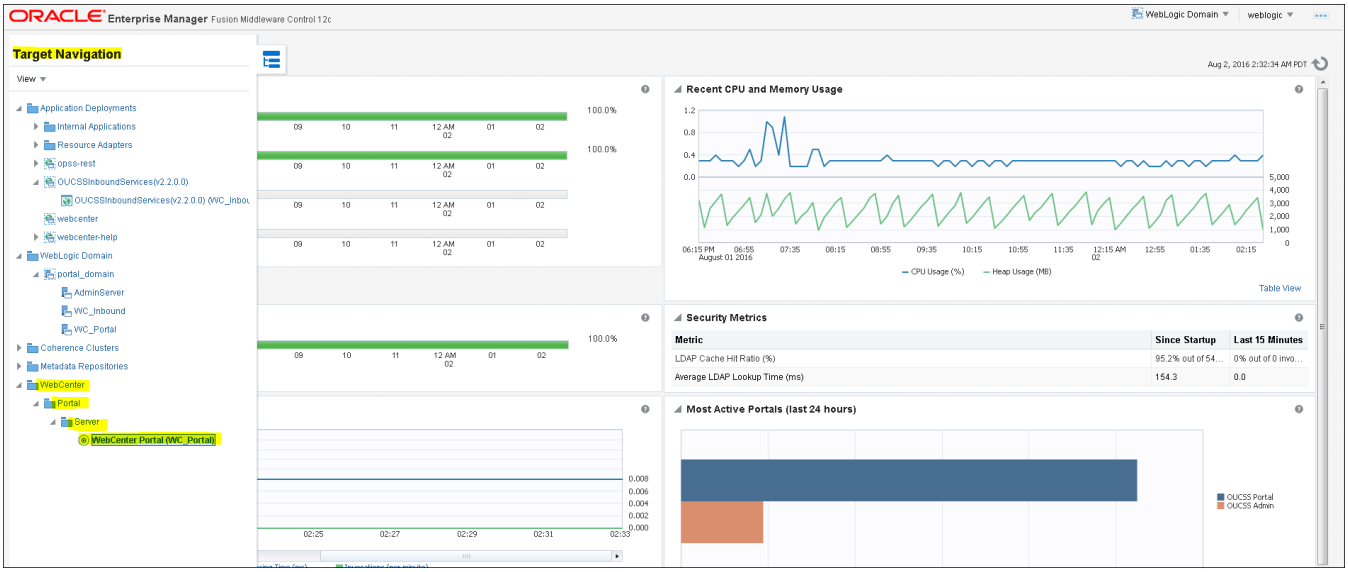


4. Under **Credentials** select and expand `oracle.wsm.security`. **OUCSS_XAI_BASIC_KEY**, **OUCSS_INTG_BASIC_KEY**, and **OUCSS_OUNC_BASIC_KEY** should be present, as shown in the following image:

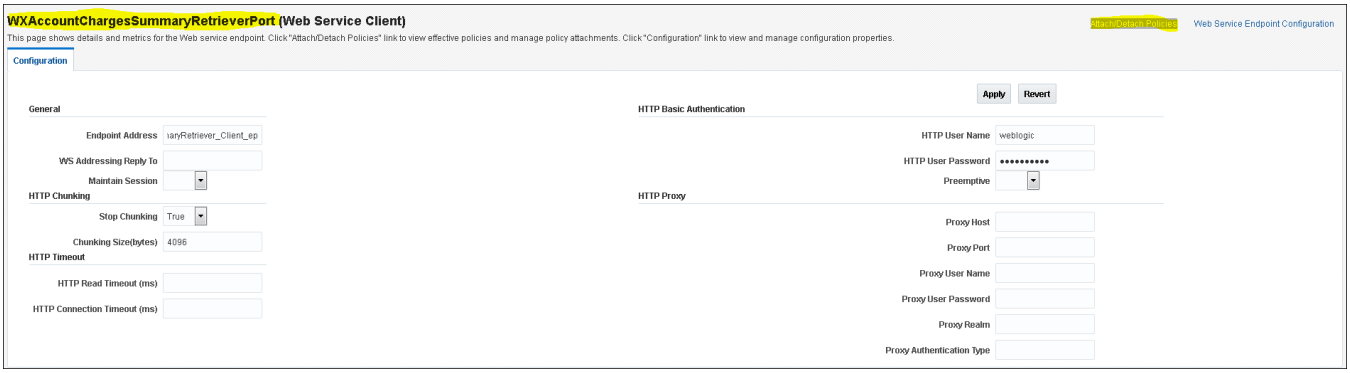


To modify the CSF Key associated with a Connection:

1. Login to Enterprise Manager.
2. Click on the deployed application. For WebCenter Portal choose WebCenter > Portal > Server > WebCenter Portal (WC_Portal) from Target Navigation menu.

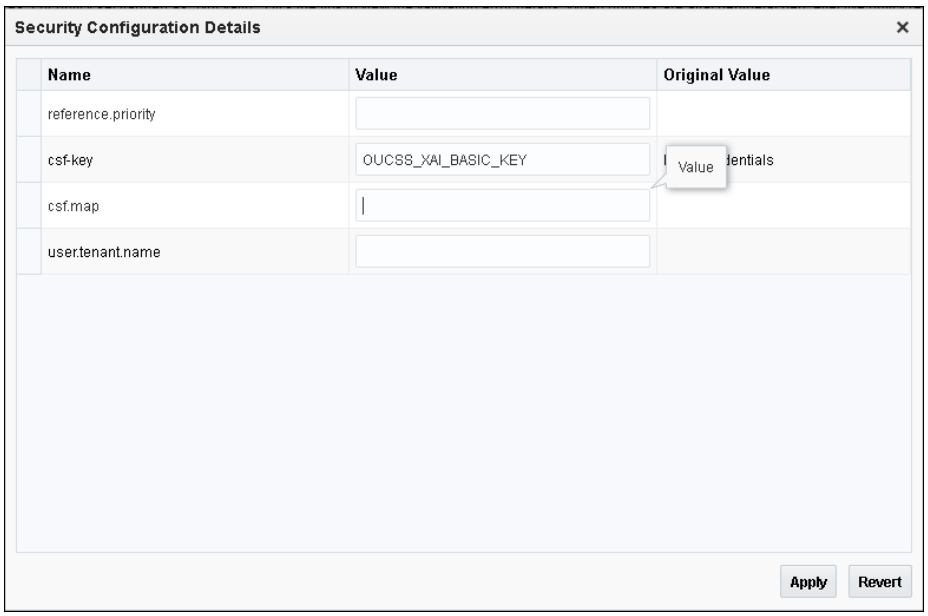


3. From the **WebCenter Portal** menu select **ADF > Configure ADF Connections**.
4. Select the target connection and click **Edit**.
5. Open the **Advanced Connection Configurations** menu and select the port to update the OWSM Policies.
6. From the configuration screen click on the **Attach/Detach Policies** link.



7 Select the active policy (e.g: `oracle/wss_http_token_client_policy)` in the **Directly Attached Policies** table, then click on **Overide Policy Configutation** button.

8 Update the csf-key to modify the key and then click on **Apply**.



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 (v2.2.0.0)** > **OUCSSInboundServices (v2.2.0.0)** deployed application to go to the application page.
3. Select **Web Services** from the **Application Deployment** menu.
4. From the **Web Service Details** table, click **OffersServiceSoapHttpPort** to modify the port details.
5. Click on the **Attach/Detach** link to attach desired policy and 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., **webcenter**).
3. From the **WebCenter Portal** 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. Click on Attach/Detach Policies link and attach the policy in order to attach authentication details.
7. Click **Apply** 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 https://docs.oracle.com/middleware/1212/owsm/OWSMS/owsm-predefined-policies.htm#OWSMS5487 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.

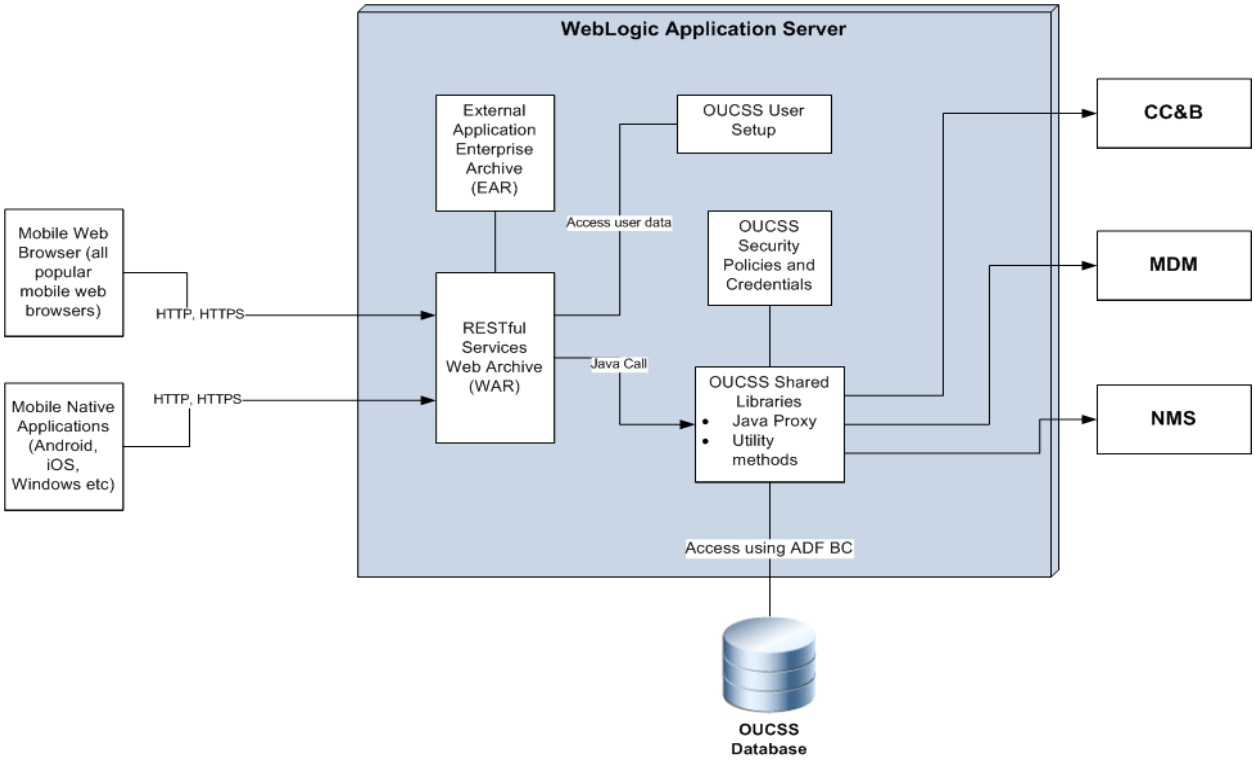
How to Invoke the Web Service

- 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 `jax-rs 2.0` 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.



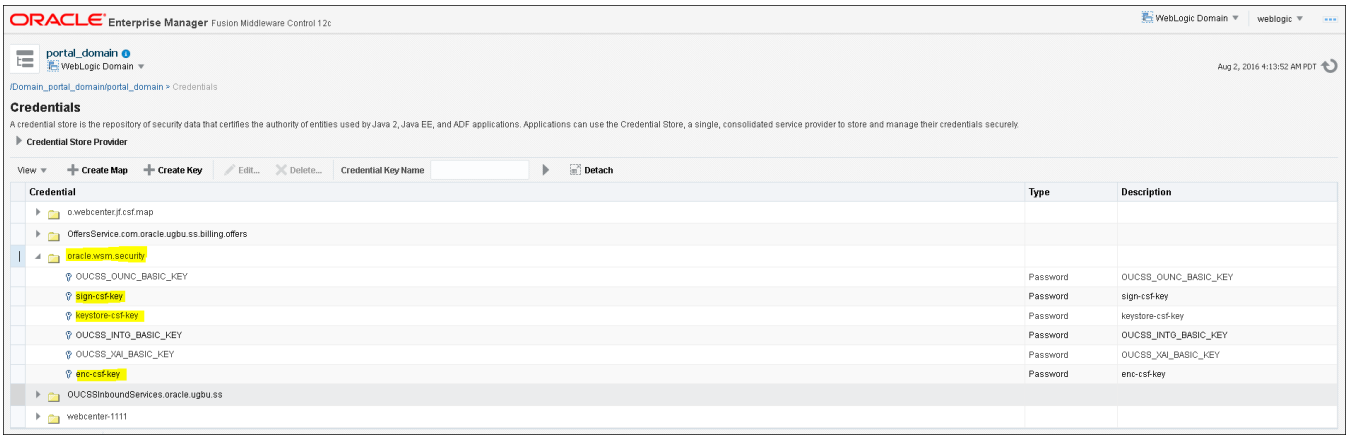
REST Security

REST services are secured using the policy **oracle/multi_token_rest_service_policy**. See https://docs.oracle.com/middleware/1212/owsm/OWSMS/owsm-predefined-policies.htm#OWSMS5487 for more information on this policy. The policy supports 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



Creating a Security Keystore

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

1. Go to `<<Java_Home>>/bin` and run the `keytool` command to generate a Java keystore (jks). The Java keystore 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. WebLogic 12c supports OPSS Key Store by default (instead of the Java Key Store). To import the default-keystore.jks into the OPSS Key Store:

   - Connect to WLST using WLS Admin user.
   - Run the following WLST commands to import the key store to OPSS key store.

   ```
   svc = getOpssService(name='KeyStoreService');

   svc.importKeyStore(appStripe='owsm',name='keystore',password='<<keystore-password>>',
   aliases='orakey', keypasswords='<<sign-csf-key-password>>', type='JKS', permission=true,
   filepath='<<KeyStorePath>>/default-keystore.jks');
   ```

   Note: Replace keystore-password and sign-csf-key-password with the values used when creating the java key store.

3. Restart the servers for the changes to take effect.