Oracle® Health Sciences Mobile Clinical Research Associate Server

Security Guide

Release 1.0

E38752-01

January 2013

1 Introduction

The Oracle Health Sciences Mobile Clinical Research Associate Server (Mobile CRA) mobile application is intended to support the clinical research analyst to conduct site visits. This release will provide the CRA with alerts or notifications sent to the mobile device, location capture vis-à-vis the sites, the ability to view the status of a site "at a glance", and access the trip report. Mobile CRA consolidates the CRA's view of the trial, collecting data from clinical data management systems, clinical trial management systems, drug supply systems, randomization systems and other systems, through an open application programming interface (API) or web services model.

The system has been designed to interact with on premise Oracle clinical development management aggregation system, Oracle Health Sciences Clinical Data Analytics (CDA) and on premise Seibel Clinical Trial Management System (CTMS).

This document contains the following sections:

- General Security Principles
- Revoking Unnecessary Grants
- Disabling Unnecessary Operating System Level Services
- Designing Multiple Layers of Protection
- Security Guidelines for Mobile CRA
- Configuring Security Using Enterprise Manager
- Configuring Security for Oracle Health Sciences Mobile Clinical Research Associate
- Protecting Data
- Documentation Accessibility

2 General Security Principles

The following principles are fundamental to using any application securely.

2.1 Keeping Software Up to Date

One of the principles of good security practice is to keep all software versions and patches up to date.

2.2 Keeping Up to Date on the Latest Security Information Critical Patch Updates

Oracle continually improves its software and documentation. Critical Patch Updates are the primary means of releasing security fixes for Oracle products to customers with valid support contracts. They are released on the Tuesday closest to the 17th day of January, April, July and October. We highly recommend customers to apply these patches as soon as they are released.

2.3 Configuring Strong Passwords on the Database

Although the importance of passwords is well known, the following basic rule of security management is worth repeating:

Ensure all your passwords are strong passwords. Oracle recommends that you use a mix of uppercase and lowercase alphabets, numbers and symbols.

You can strengthen passwords by creating and using password policies for your organization. For guidelines on securing passwords and for additional ways to protect passwords, refer to the Oracle Database Security Guide specific to the database release you are using.

You should modify the following passwords to use your policy-compliant strings:

- Passwords for the database default accounts, such as SYS and SYSTEM.
- Passwords for the database application-specific schema accounts.
- You should not configure a password for the database listener as that will enable remote administration. For more information, refer to the section "Removing the Listener Password" of *Oracle® Database Net Services Reference 11g Release 2 (11.2)*.

Refer to the *Oracle 11gR2 Database Security Guide* for more information.

2.4 Following the Principle of Least Privilege

The principle of least privilege states that users should be given the least amount of privilege to perform their jobs. Overly ambitious granting of responsibilities, roles, grants - especially early on in an organization's life cycle when people are few and work needs to be done quickly - often leaves a system wide open for abuse. User privileges should be reviewed periodically to determine relevance to current job responsibilities.

Before executing DDL scripts, a database user should be created with the specified limited set of privileges. DBA access should not be given to the user.

Mobile CRA has system and object level privileges. Minimum privileges, such as connecting to the schema, are granted to schema owners. Application users do not have access to the database layer and must access it from the application.

3 Revoking Unnecessary Grants

For security purposes, you must revoke all unnecessary grants on the schema. You will require DBA privileges to perform this action.

4 Disabling Unnecessary Operating System Level Services

This section suggests various unused operating system level services that you can disable to improve security.

4.1 Disabling the Telnet Service

Oracle Health Sciences Mobile CRA does not use the Telnet service.

Telnet listens on port 23 by default. If the Telnet service is available on any computer, Oracle recommends that you disable Telnet in favor of Secure Shell (SSH). Telnet, which sends clear-text passwords and user names through a log-in, is a security risk to your servers. Disabling Telnet tightens and protects your system security.

4.2 Disabling Other Unused Services

Oracle Health Sciences Mobile CRA does not use the following services or information for any functionality:

- Simple Mail Transfer Protocol (SMTP). This protocol is an Internet standard for E-mail transmission across Internet Protocol (IP) networks.
- Identification Protocol (identd). This protocol is generally used to identify the owner of a TCP connection on UNIX.
- Simple Network Management Protocol (SNMP). This protocol is a method for managing and reporting information about different systems.
- File transfer Protocol (FTP). This protocol is used for downloading or uploading files from the file server.

Therefore, restricting these services or information does not affect the use of Oracle Health Sciences Mobile CRA. If you are not using these services for other applications, Oracle recommends that you disable these services to minimize your security exposure. If you need SMTP, identd, or SNMP for other applications, be sure to upgrade to the latest version of the protocol to provide the most up-to-date security for your system.

5 Designing Multiple Layers of Protection

When designing a secure deployment, design multiple layers of protection. If a hacker should gain access to one layer, such as the application server, that should not automatically give them easy access to other layers, such as the database server.

Providing multiple layers of protection may include:

- Enabling only those ports required for communication between different tiers, for example, only allowing communication to the database tier on the port used for SQL*NET communications, (1521 by default).
- Placing firewalls between servers so that only expected traffic can move between servers.

6 Security Guidelines for Mobile CRA

MobileCRA application timeout should be reasonably timed. It should not be too long and pose a security risk, while a small timeout hampers productivity.

6.1 Security Guidelines for Database Objects and Database Options

This section describes security guidelines for Mobile CRA database objects and database options.

6.1.1 Oracle Health Sciences Mobile Clinical Research Associate Server Objects

CRA contains database objects. You can use DDL scripts, PL/SQL procedures and functions to create database objects, and DML scripts to create seed data. These files are part of the media pack.

The guidelines for installing and configuring Oracle Database Server are available here http://docs.oracle.com/cd/E11882_01/network.112/e16543/toc.htm.

The Mobile CRA application has the following different schemas:

1. Rules Engine
   - System Grants provided or needed

     Connect, Resource, Create Materialized View, Select Any Table
   - Grant `Select` on CDA (RXI) schema for following tables:

     ```
     W_RXI_STUDY_D
     W_RXI_STUDY_SITE_D
     W_HS_STUDY_ACCESS_SEC
     W_HS_APPLICATION_USER_D
     W_HS_STUDY_SITE_ACCESS_SEC
     ```
2. MobileCRA Server
   - System Grants provided or needed

     Connect, Resource
3. MobileCRA CTMS (Trip Report)
   - System Grants provided or needed

     Connect, Resource
4. Push Notification Server
   - System Grants provided or needed

     Connect, Resource
5. MobileAQ
   - System Grants provided or needed

     Connect, Resource
   - AQ related grants

     ```
     Grant aq_user_role
     Grant execute ON sys.dbms_aqadm
     Grant execute ON sys.dbms_aq
     Grant execute ON sys.dbms_aqin
     Grant execute ON sys.dbms_aqjms
     ```

6.1.2 Oracle Database Options

The Oracle Database has options that provide additional security features. Mobile CRA may include data that falls under HIPAA guidelines in the United States and similar guidelines elsewhere. These features can help you comply with those guidelines.

Database Vault

Mobile CRA includes data that may fall under HIPAA or other regulations outside the United States. These data are highly sensitive and only those with a need to know should have access to it. To prevent database administrators and others from seeing the data, it is recommended that Oracle Database Vault be used to limit access to the Mobile CRA schema to the Mobile CRA user to prevent DBAs and other "superuser" accounts from accessing the data. Note that Database Vault requires a separate license.

Oracle Audit Vault

Oracle Audit Vault automates the audit collection, monitoring, and reporting process, turning audit data into a key security resource for detecting unauthorized activity.

Consider using this feature to satisfy compliance regulations such as SOX, PCI, and HIPAA, and to mitigate security risks. Note that Oracle Audit Vault requires a separate license.

Transparent Data Encryption

Transparent Data Encryption is one of the three components of the Oracle Advanced Security option for Oracle Database 11g Release 2 Enterprise Edition. It provides transparent encryption of stored data to support your compliance efforts. If you employ Transparent Data Encryption, applications do not have to be modified and continue to work seamlessly as before. Data is automatically encrypted when it is written to disk and automatically decrypted when accessed by the application. Key management is built in, eliminating the complex task of creating, managing and securing encryption keys. Note that the Advanced Security Option is licensed separately from the database.

Tablespace Encryption

Tablespace Encryption is another component of the Oracle Advanced Security option for Oracle Database 11g Release 2 Enterprise Edition. Tablespace encryption facilitates encryption of the entire tablespace contents, rather than having to configure encryption on a column-by-column basis. It encrypts data at the datafile level to keep users from viewing the oracle datafiles directly. Oracle recommends that you perform tablespace encryption for maximum protection.

6.2 Security Guidelines for the Middle Tier

This section describes the security guidelines for the Mobile CRA middle tier.

- The server should only use https.
- Mobile CRA uses a system account credential from CDA and the Health Sciences Push Notification Server (HSPNS). All these accounts are configured safely in the Oracle Credential store. For more details, refer to the *Oracle Health Sciences Mobile Clinical Research Associate Server Installation Guide*.
- Mobile CRA uses Single sign on (SSO) token from CTMS. SSO token should be generated in CTMS and used for accessing CTMS. SSO token is safe because it can be regenerated without exposing user passwords. Mobile CRA uses this SSO token to access CTMS on behalf of various users.

- Mobile CRA supports Lightweight Directory Access Protocol (LDAP) and SSO. LDAP configuration for Mobile CRA should be done in the Oracle WebLogic server (WLS). For more information, refer to Oracle WebLogic server documentation.
- If configuring against LDAP, both CTMS and Mobile CRA should be setup to the centralized LDAP.
- An application group, `mobilecra-admins`, should be created in WLS or LDAP for Mobile CRA. An admin user has to be a part of this administration group to manage or configure the Mobile CRA application. General WLS user and password management guidelines apply.
- AdminUI, an ADF based application, can be configured with SSO. For more information, refer to Oracle SSO documentation.
- Oracle Business Intelligence Enterprise Edition (OBIEE) has its own credential store, which is the WLS security realm.

6.2.1 Removing Unused Applications from Oracle WebLogic

Currently, the Oracle WebLogic Server installation includes the entire JDK and some additional Oracle WebLogic Server development utilities (for example, wlsvc). These applications are not needed and should be removed. The following are recommendations for making a Oracle WebLogic Server installation more secure:

- Do not install the Oracle WebLogic Server sample applications.
- Delete development tools, such as the Configuration Wizard and the jCOM tools.
- Delete the Derby database, which is bundled with Oracle WebLogic Server for use by the sample applications and code examples as a demonstration database.

For more details, refer to the Determining Your Security Needs section in *Oracle® Fusion Middleware Securing a Production Environment for Oracle WebLogic Server 12c Release 1 (12.1.1)*

6.2.2 Enabling SSL

Due to the complexity in setting up SSL it is not enabled by default during installation. Communications between the browser and the application servers should be restricted to SSL.

It is optional to enable SSL, but Oracle recommends SSL for a production environment.

To enable SSL:

1. Log into Oracle WebLogic Server Administration Console.
2. Click the **Environment** node in the Domain Structure pane and click **Servers** in Environment table.
3. Click the server where you deployed the oracle.hs.mobilecra.ear file.
4. Click the **Configuration** tab.
5. Click the **General** tab.
6. If Save is disabled, click **Lock & Edit** in the Change Center pane.
7. Select the **SSL Listen Port Enabled** check box and enter a port number.
8. To disable non-SSL port, deselect the **Listen Port Enabled** check box.
9. Click **Save.**

10. Click **Activate Changes** in the Change Center pane, if it is enabled.

11. Click the **Control** tab.

12. Click the **Start/Stop** tab.

13. Click **Restart SSL**

14. Click **Yes**. The following message appears.

    ```
    SSL channels have been successfully restarted.
    ```

You must also configure SSL, identity, and trust. For more information, refer to *Oracle® Fusion Middleware Securing Oracle WebLogic Server 11g Release 1 (10.3.5).*

6.2.3 Configuring SSL

To set up SSL, perform the following steps:

1. Obtain an identity (private key and digital certificates) and trust (certificates of trusted certificate authorities) for Oracle WebLogic Server. Use the digital certificates, private keys, and trusted CA certificates provided by Oracle WebLogic Server, the CertGen utility, the keytool utility, or a reputable vendor such as Entrust or Verisign to perform this step.

2. Store the identity and trust. Private keys and trusted CA certificates which specify identity and trust are stored in keystores.

3. Configure the identity and trust keystores for Oracle WebLogic Server in the Oracle WebLogic Server Administration Console.

4. Set SSL configuration options for the private key alias and password in the Oracle WebLogic Server Administration Console. Optionally, set configuration options that require the presentation of client certificates (for two-way SSL).

For more details, refer to Configuring SSL section in *Oracle® Fusion Middleware Securing Oracle WebLogic Server 12c Release 1 (12.1.1).*

6.2.4 Disabling Other Unused Services

Oracle Health Sciences Mobile CRA does not use the following services or information for any functionality:

- Simple Mail Transfer Protocol (SMTP). This protocol is an Internet standard for E-mail transmission across Internet Protocol (IP) networks.

- Identification Protocol (identd). This protocol is generally used to identify the owner of a TCP connection on UNIX.

- Simple Network Management Protocol (SNMP). This protocol is a method for managing and reporting information about different systems.

- File transfer Protocol (FTP). This protocol is used for downloading or uploading files from the file server.

Therefore, restricting these services or information does not affect the use of Mobile CRA. If you are not using these services for other applications, Oracle recommends that you disable these services to minimize your security exposure. If you need SMTP, identd, or SNMP for other applications, be sure to upgrade to the latest version of the protocol to provide the most up-to-date security for your system.

6.2.5 Protecting User Accounts

Oracle WebLogic Server defines a set of configuration options to protect user accounts from intruders. In the default security configuration, these options are set for maximum protection. You can use the Administration Console to modify these options on the **Configuration** > **User Lockout** page.

As a system administrator, you have the option of turning off all the configuration options, increasing the number of login attempts before a user account is locked, increasing the time period in which invalid login attempts are made before locking the user account, and changing the amount of time a user account is locked. Remember that changing the configuration options lessens security and leaves user accounts vulnerable to security attacks. For more details, refer to Configuring Security for a WebLogic Domain section in *Oracle® Fusion Middleware Securing Oracle WebLogic Server 12c Release 1 (12.1.1)*.

7 Configuring Security Using Enterprise Manager

This section contains the following topics:

- Defining Credentials Used by Oracle Health Sciences Mobile Clinical Research Associate on page 1-8
- Configuring User-level Security on page 1-14

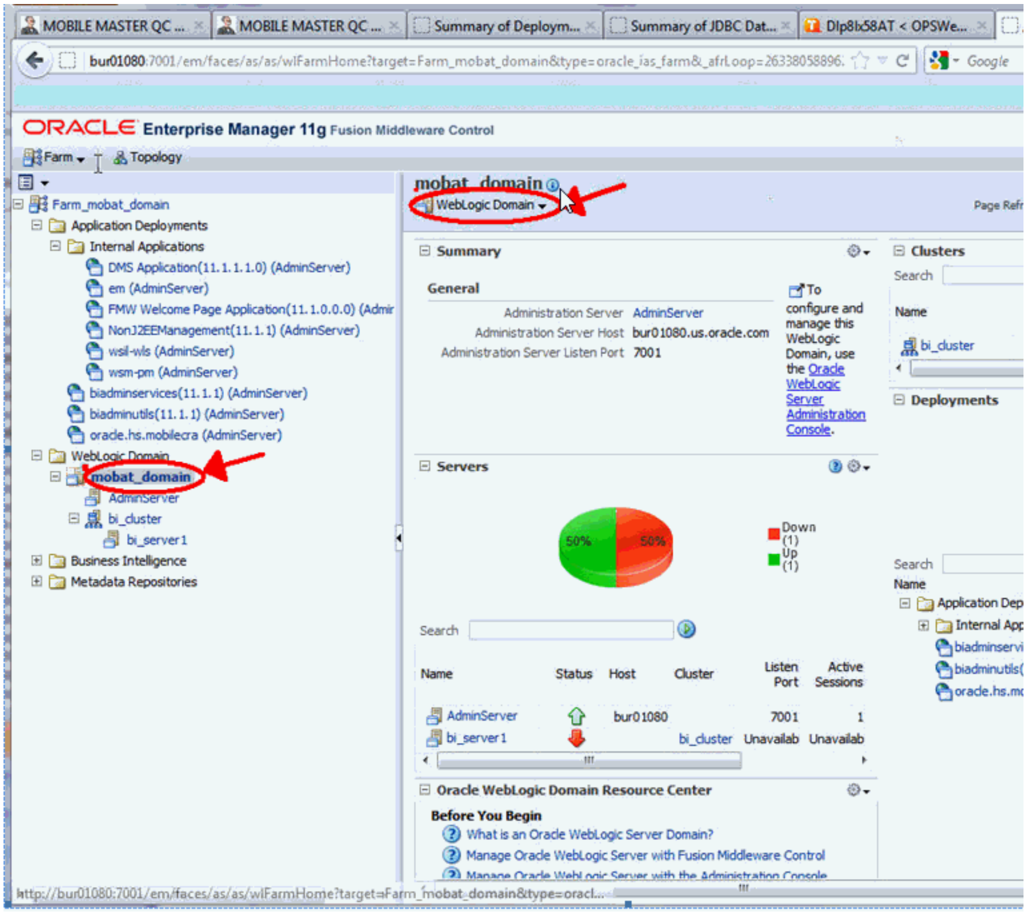
7.1 Defining Credentials Used by Oracle Health Sciences Mobile Clinical Research Associate

To define the credentials used by Mobile CRA in the Oracle credential store, perform the following:

1. Log in to WebLogic Enterprise Manager as admin by navigating to the URL. For example, `http://<servername>/em`.
2. Select **WebLogic Domain** from the server_domain panel on the left side.
3. Select the domain name.

   The details of server_domain are displayed on the right-side window panel.
4. Under server_domain, select **WebLogic_domain**.

Figure 1 server_domain Screen



General

Administration Server AdminServer
Administration Server Host bur01080.us.oracle.com
Administration Server Listen Port 7001

To configure and manage this WebLogic Domain, use the Oracle WebLogic Server Administration Console.

Search

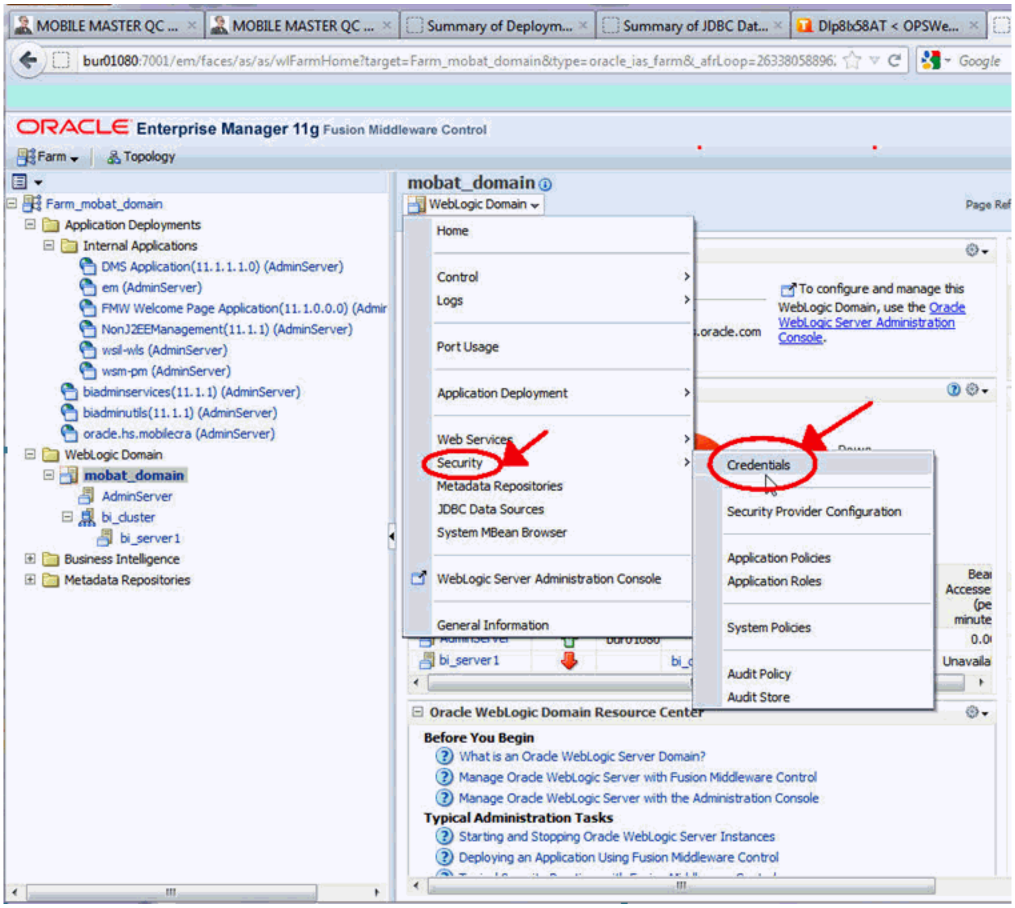
Name	Status	Host	Cluster	Listen Port	Active Sessions
AdminServer	⇧	bur01080		7001	1
bi_server1	⇩		bi_cluster	Unavailab	Unavailab

What is an Oracle WebLogic Server Domain?
Manage Oracle WebLogic Server with Fusion Middleware Control
Manage Oracle WebLogic Server with the Administration Console

http://bur01080:7001/em/faces/as/as/wlFarmHome?target=Farm_mobat_domain&type=oracl...

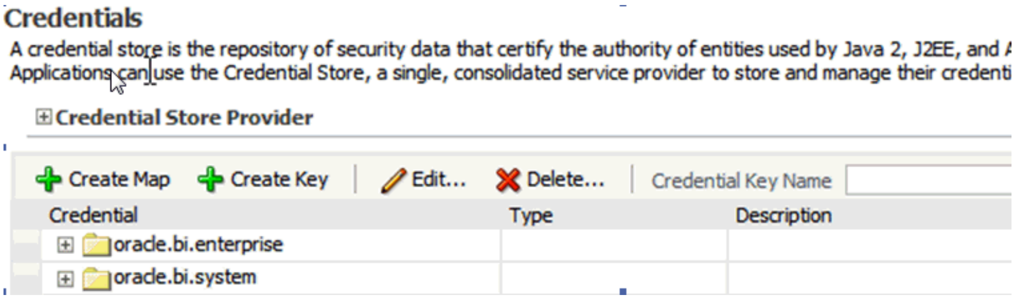
5. From the **WebLogic Domain** drop-down list, select **Security** > **Credentials**.

Figure 2


MOBILE MASTER QC ...
MOBILE MASTER QC ...
Summary of Deploym...
Summary of JDBC Dat...
Dlp8b58AT < OPSWe...
bur01080:7001/em/faces/as/as/wlFarmHome?target=Farm_mobat_domain&type=oracle_ias_farm&_afrLoop=26338058896:
Google
ORACLE Enterprise Manager 11g Fusion Middleware Control
Farm
Topology
Farm_mobat_domain
Application Deployments
Internal Applications
DMS Application(11.1.1.1.0) (AdminServer)
em (AdminServer)
FMW Welcome Page Application(11.1.0.0.0) (Admir
NonJ2EEManagement(11.1.1) (AdminServer)
wsil-wls (AdminServer)
wsm-pm (AdminServer)
biadminservices(11.1.1) (AdminServer)
biadminutils(11.1.1) (AdminServer)
oracle.hs.mobilecra (AdminServer)
WebLogic Domain
mobat_domain
AdminServer
bi_cluster
bi_server1
Business Intelligence
Metadata Repositories
mobat_domain
WebLogic Domain
Page Ref
Home
Control
Logs
Port Usage
Application Deployment
Web Services
Security
Metadata Repositories
JDBC Data Sources
System MBean Browser
WebLogic Server Administration Console
General Information
Credentials
Security Provider Configuration
Application Policies
Application Roles
System Policies
Audit Policy
Audit Store
To configure and manage this WebLogic Domain, use the Oracle WebLogic Server Administration Console.
.oracle.com
bi_server1
Beai Accesse (pe minute
0.0
Unavaila
Oracle WebLogic Domain Resource Center
Before You Begin
What is an Oracle WebLogic Server Domain?
Manage Oracle WebLogic Server with Fusion Middleware Control
Manage Oracle WebLogic Server with the Administration Console
Typical Administration Tasks
Starting and Stopping Oracle WebLogic Server Instances
Deploying an Application Using Fusion Middleware Control

The Credentials screen is displayed.

Figure 3 Credentials



Credentials

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

Credential	Type	Description
oracle.bi.enterprise		
oracle.bi.system		

6. Click **Create Map** to create a new credential and enter `oracle.hs.mobilecra`. The updated list of credentials is displayed.

7. Select `oracle.hs.mobilecra`, click **Create Key**. The **Select Map** field will be updated with the map name. Perform the following:

   a. Enter key as `notificationService.credential`. This is the user name and password provided by Oracle for accessing the push notification service.

Mobile CRA uses this information to access the Oracle push notification service.

b. Enter type as `Password`.

c. Enter the mobile notification server user name and password provided by Oracle.

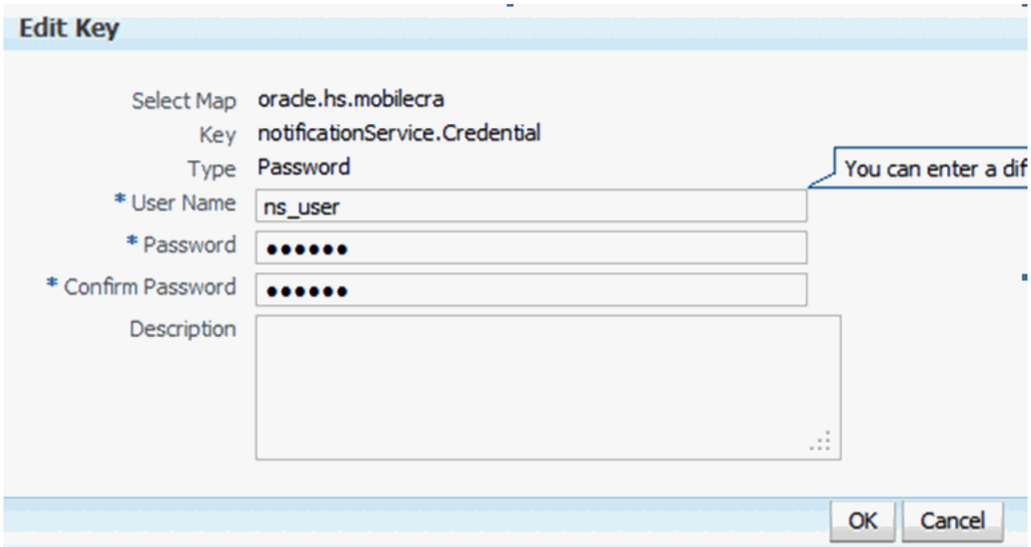
d. Re-enter the password in the **Confirm Password** field.

e. If you wish, provide the description of the key in the **Description** field.

f. Click **OK**.

You can edit the details in the **Edit Key** screen.

Figure 4 Edit Key Screen



Edit Key

Select Map oracle.hs.mobilecra
Key notificationService.Credential
Type Password
* User Name ns_user
* Password ●●●●●●
* Confirm Password ●●●●●●
Description

g. Click **OK**.

8. Click **Create Key** to create another key. The **Select Map** field will be updated with the map name. Now perform the following:

   a. Enter key as `ctmsAdapter.systemCredential`. This is the CTMS user name and password. Mobile CRA uses this information to access CTMS.

   b. Enter type as `Password`.

   c. Enter the CTMS user name and password.

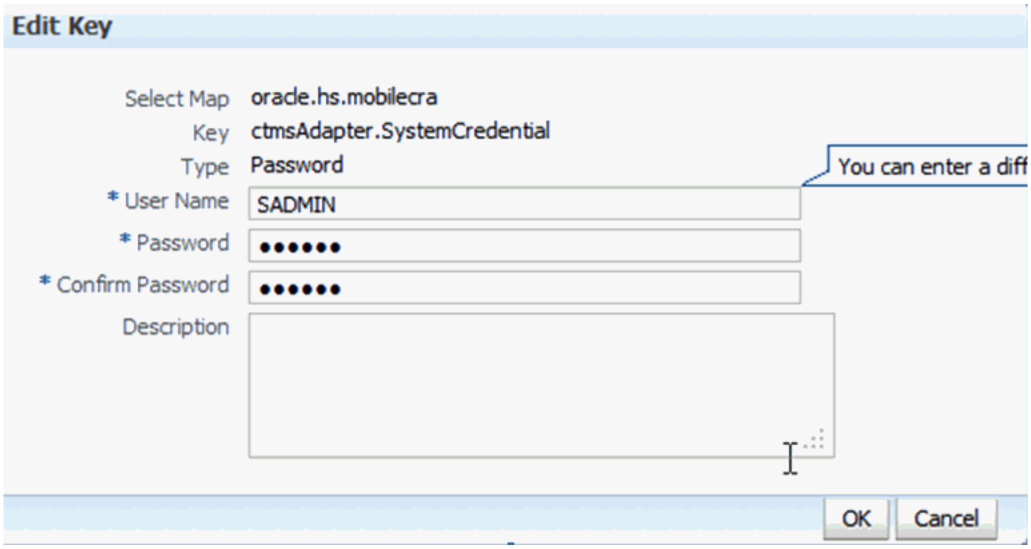
   d. Re-enter the password in the **Confirm Password** field.

   e. If you wish, provide the description of the key in the **Description** field.

   f. Click **OK**.

   You can edit the details in the **Edit Key** screen.

Figure 5 Edit Key Screen



Edit Key

Select Map oracle.hs.mobilecra

Key ctmsAdapter.SystemCredential

Type Password

* User Name SADMIN

* Password ••••••

* Confirm Password ••••••

Description

g. Click **OK**.

9. Click **Create Key** to create another key. The **Select Map** field will be updated with the map name. Now perform the following:

   a. Enter `ctmsAdapter.SSOTokenCredential` as the key.

      This is the SSO token that is generated in CTMS. For generating the CTMS SSO token, refer to the *Oracle Siebel Clinical Trial Management System Installation Guide*. Mobile CRA uses this token to access CTMS on behalf of CTMS users.

   b. Enter type as `Generic`.

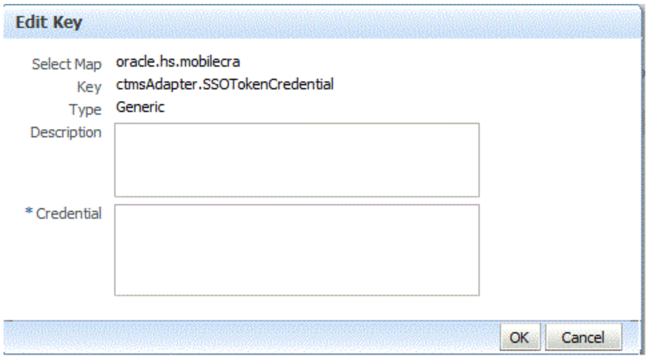
   c. If you wish, provide the description of the key in the **Description** field.

   d. Enter the user name and password credentials which are a token on CTMS instance.

   e. Click **OK**.

      You can edit the details in the Edit Key screen.

Figure 6 Edit Key Screen



Edit Key

Select Map oracle.hs.mobilecra

Key ctmsAdapter.SSOTokenCredential

Type Generic

Description

* Credential

f. Click **OK**.

10. Click **Create Key** to create another key. The **Select Map** field will be updated with the map name. Now perform the following:

    a. Enter key as `cdaAdapter.ObieeCredential`. This is the user name and password for OBIEE. This credential has access to all the OBIEE answers used in alerts.

    b. Select **Map**. This field is already populated with the name of the map being updated.

    c. Enter type as `Password`.

    d. Enter the user name and password.

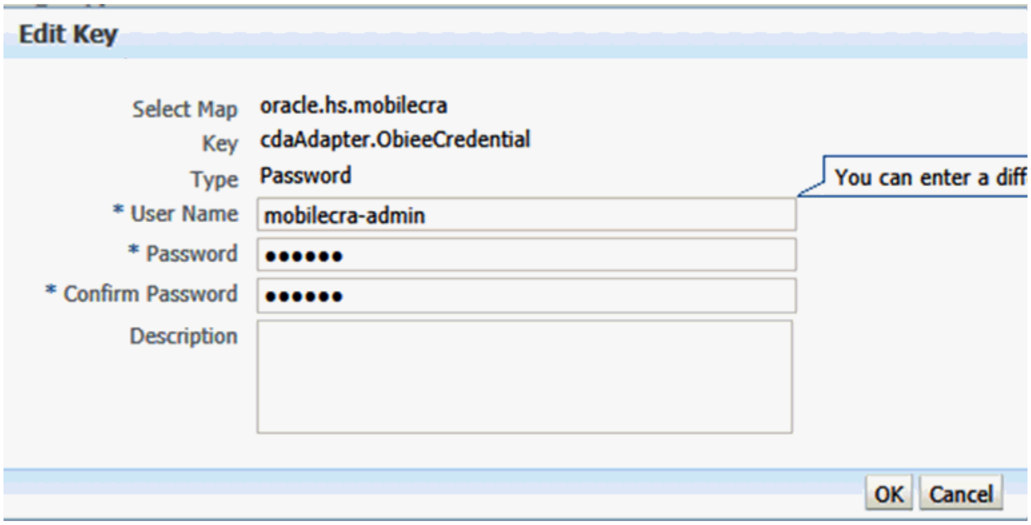
    e. Re-enter the password in the **Confirm Password** field.

    f. If you wish, provide the description of the key in the **Description** field.

    g. Click **OK**.

    You can edit the details in the Edit Key screen.

Figure 7 Edit Key Screen



Edit Key

Select Map oracle.hs.mobilecra

Key cdaAdapter.ObieeCredential

Type Password

* User Name mobilecra-admin

* Password ••••••

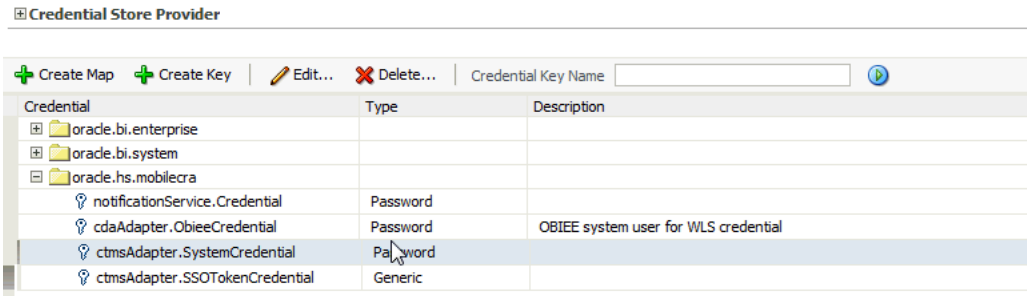
* Confirm Password ••••••

Description

You can enter a diff

11. Click **OK**. The updated **Credentials** screen is displayed.

Figure 8 Credentials Screen



Credential	Type	Description
oracle.bi.enterprise		
oracle.bi.system		
oracle.hs.mobilecra		
notificationService.Credential	Password	
cdaAdapter.ObieeCredential	Password	OBIEE system user for WLS credential
ctmsAdapter.SystemCredential	Password	
ctmsAdapter.SSOTokenCredential	Generic	

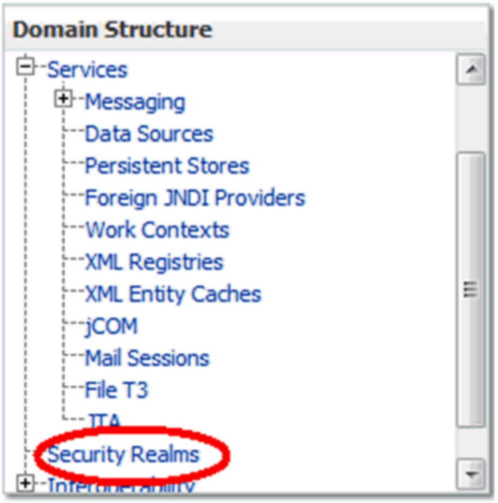
12. Exit the WebLogic server.

7.2 Configuring User-level Security

To configure user-level security using Enterprise Manager, perform the following:

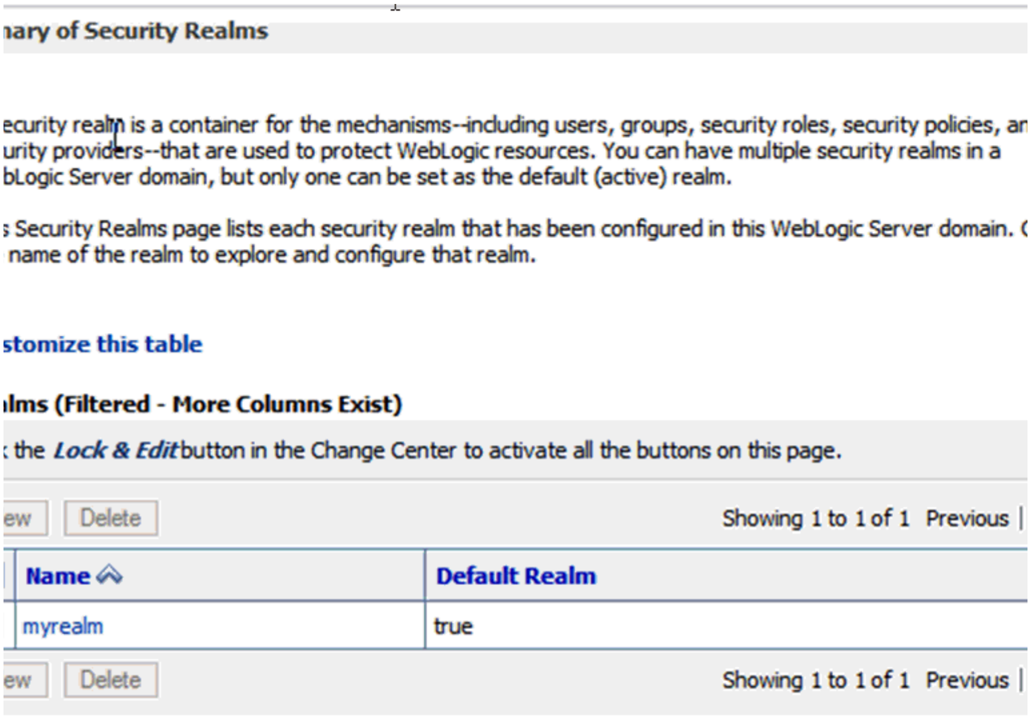
1. Log in to WebLogic Server as admin by entering the URL. For example, `http://server:7001/console`).
2. Click **Lock and Edit** in the **Change Center** panel on the left side.
3. Click **Security Realms** on the **Domain Structure** window.

Figure 9 Domain Structure Window



The **Summary of Security Realms** screen is displayed.

Figure 10   Summary of Security Realms Screen



ıary of Security Realms

ecurity realm is a container for the mechanisms--including users, groups, security roles, security policies, ar urity providers--that are used to protect WebLogic resources. You can have multiple security realms in a bLogic Server domain, but only one can be set as the default (active) realm.

; Security Realms page lists each security realm that has been configured in this WebLogic Server domain. (name of the realm to explore and configure that realm.

stomize this table

ılms (Filtered - More Columns Exist)

ː the *Lock & Edit* button in the Change Center to activate all the buttons on this page.

ew | Delete   Showing 1 to 1 of 1 Previous |

Name	Default Realm
myrealm	true

ew | Delete   Showing 1 to 1 of 1 Previous |

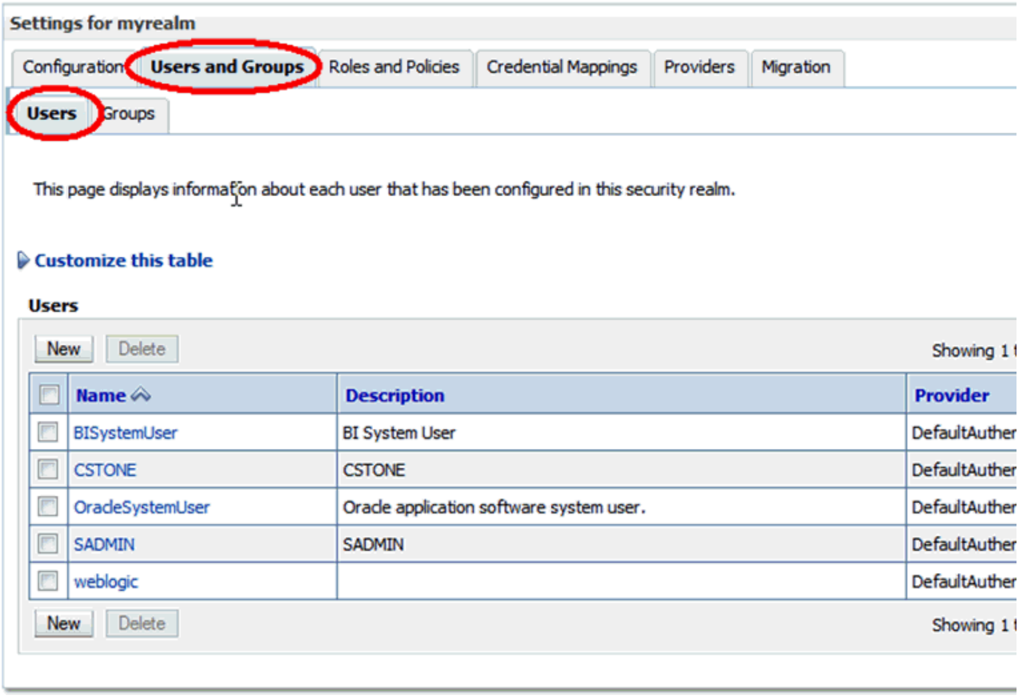
4. Select **myrealm** from the list.

   The settings for the myrealm screen are displayed in the right-side window panel.

5. Click the **Users and Groups** tab and then click the **Users** subtab.

   The list of existing users is displayed.

Figure 11   List of Existing Users



Settings for myrealm

This page displays information about each user that has been configured in this security realm.

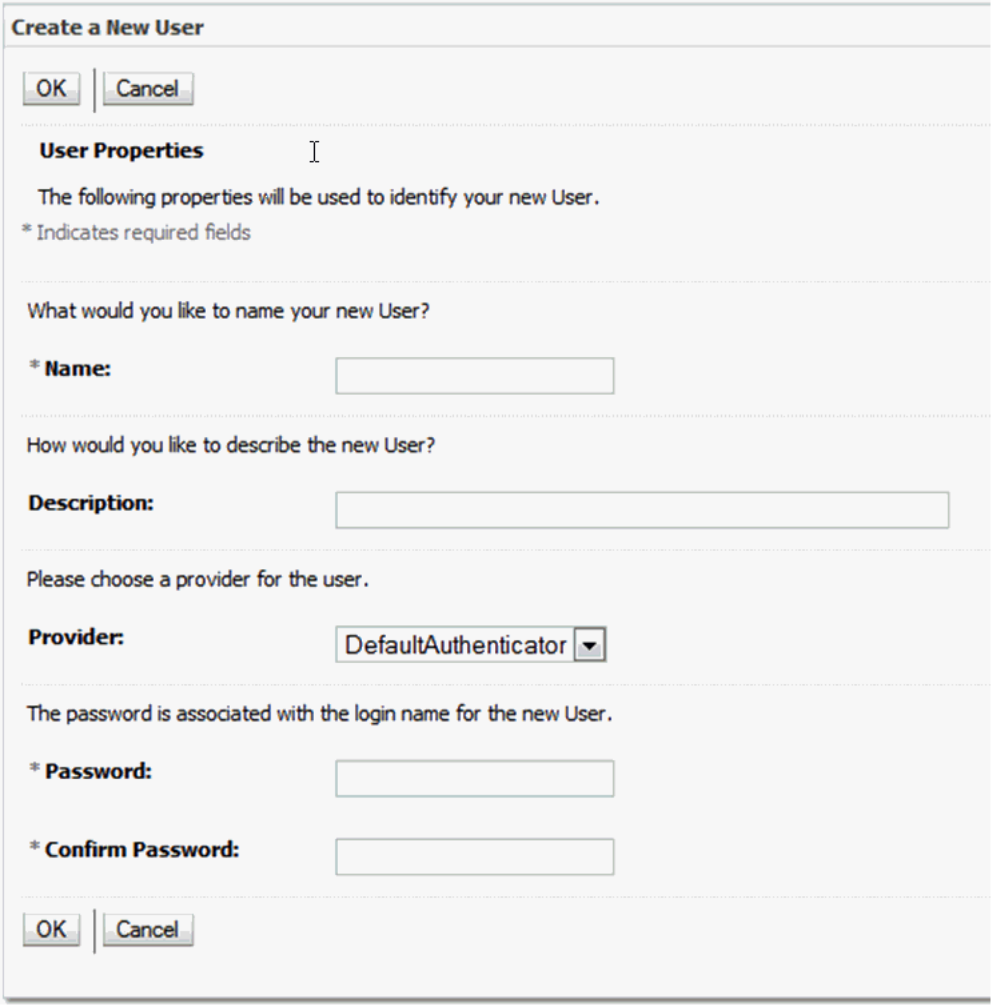
Users

□	Name	Description	Provider
□	BISystemUser	BI System User	DefaultAuther
□	CSTONE	CSTONE	DefaultAuther
□	OracleSystemUser	Oracle application software system user.	DefaultAuther
□	SADMIN	SADMIN	DefaultAuther
□	weblogic		DefaultAuther

6. Click **New** to create a new user.

   The **Create a New User** screen is displayed:

Figure 12 Create a New User Screen



Create a New User

User Properties

The following properties will be used to identify your new User.

* Indicates required fields

What would you like to name your new User?

* Name:

How would you like to describe the new User?

Description:

Please choose a provider for the user.

Provider: DefaultAuthenticator

The password is associated with the login name for the new User.

* Password:

* Confirm Password:

a. Enter the name.

b. Provide the description for the user in the **Description** field.

c. Select the default **Provider**, that is, DefaultAuthenticator.

d. Enter a password of your choice.

e. Re-enter the password in the **Confirm Password** field.

f. Click **OK**.

7. Repeat Step 6 to create another user.

8. Exit the WebLogic server.

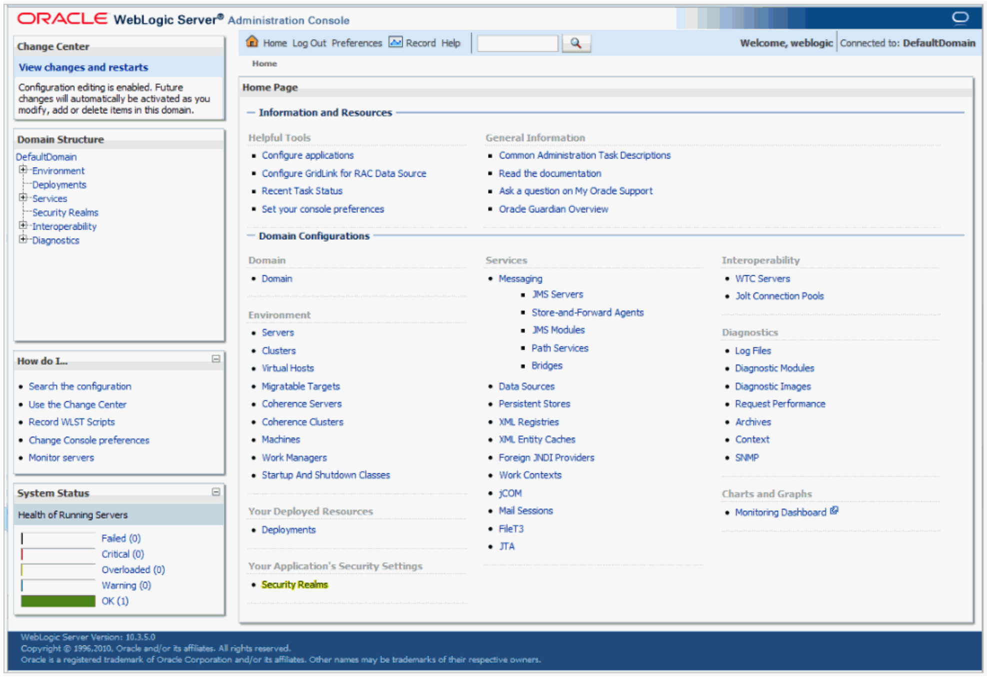
8 Configuring Security for Oracle Health Sciences Mobile Clinical Research Associate

To configure security for Mobile CRA, perform the following:

1. Log in to the Oracle WebLogic Server Administration Console.

2. Within Server Administration, select **Security Realms**.

Figure 13 Selecting Security Realms



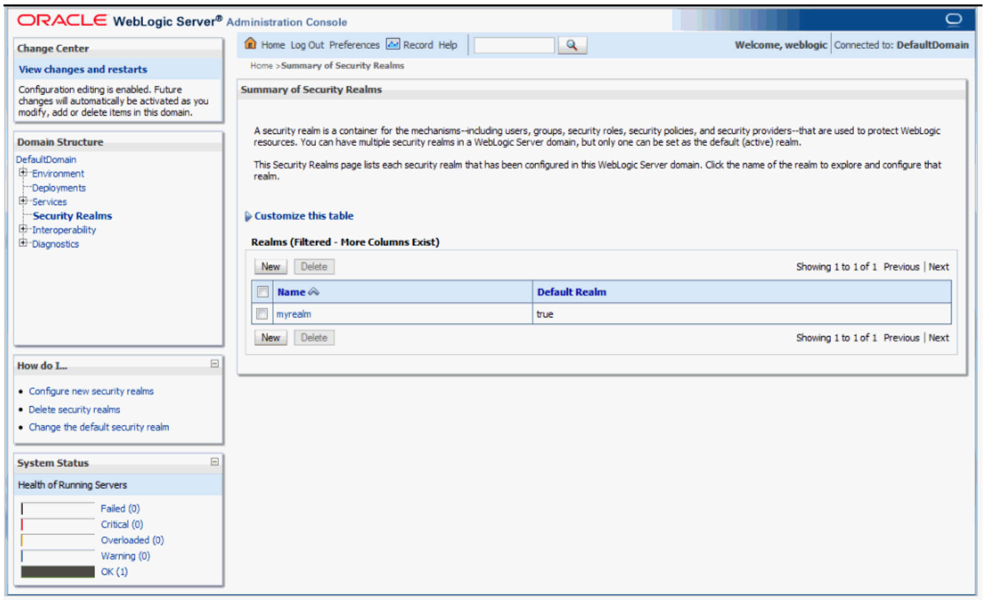
Configuration editing is enabled. Future changes will automatically be activated as you modify, add or delete items in this domain.

WebLogic Server Version: 10.3.5.0
Copyright © 1996,2010, Oracle and/or its affiliates. All rights reserved.
Oracle is a registered trademark of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.

The **Summary of Security Realm** screen is displayed.

3. Select the security realm.

Figure 14 Summary of Security Realm screen


ORACLE WebLogic Server® Administration Console
Change Center
View changes and restarts
Home Log Out Preferences Record Help
Welcome, weblogic Connected to: DefaultDomain
Home >Summary of Security Realms
Summary of Security Realms
Domain Structure
DefaultDomain
Environment
Deployments
Services
Security Realms
Interoperability
Diagnostics
How do I...
Configure new security realms
Delete security realms
Change the default security realm
System Status
Health of Running Servers
Failed (0)
Critical (0)
Overloaded (0)
Warning (0)
OK (1)
Customize this table
New
Delete
Showing 1 to 1 of 1 Previous | Next

Configuration editing is enabled. Future changes will automatically be activated as you modify, add or delete items in this domain.

A security realm is a container for the mechanisms--including users, groups, security roles, security policies, and security providers--that are used to protect WebLogic resources. You can have multiple security realms in a WebLogic Server domain, but only one can be set as the default (active) realm.

This Security Realms page lists each security realm that has been configured in this WebLogic Server domain. Click the name of the realm to explore and configure that realm.

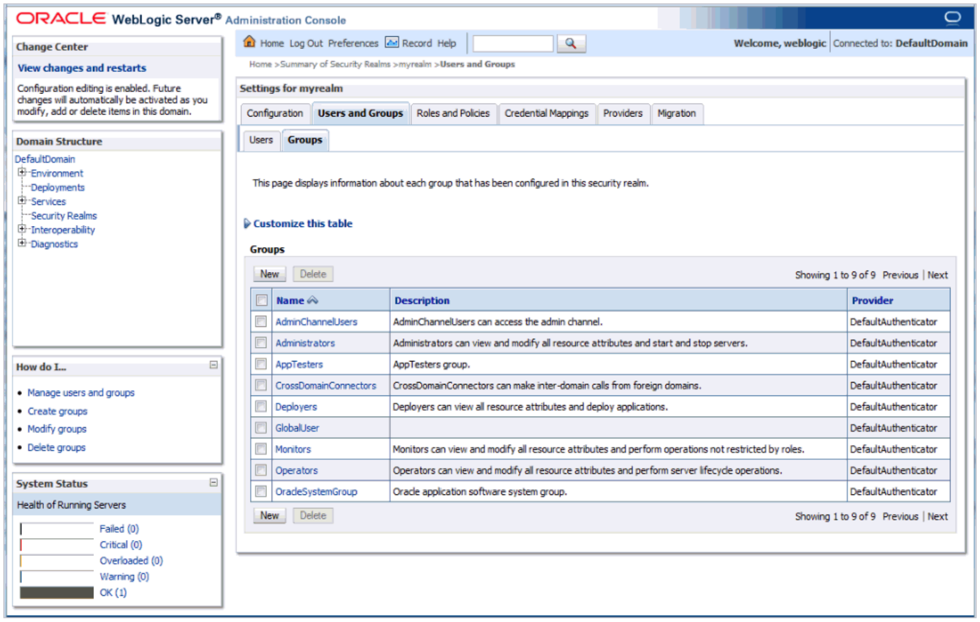
Realms (Filtered - More Columns Exist)

□	Name	Default Realm
□	myrealm	true

The Settings for myrealm screen is displayed.

4. Select **Users and Groups** and then the **Groups** subtab.

Figure 15 Settings for myrealm Screen


ORACLE WebLogic Server® Administration Console
Home Log Out Preferences Record Help
Welcome, weblogic | Connected to: DefaultDomain
Home >Summary of Security Realms >myrealm >Users and Groups
Change Center
View changes and restarts
Configuration editing is enabled. Future changes will automatically be activated as you modify, add or delete items in this domain.
Domain Structure
DefaultDomain
Environment
Deployments
Services
Security Realms
Interoperability
Diagnostics
How do I...
Manage users and groups
Create groups
Modify groups
Delete groups
System Status
Health of Running Servers
Failed (0)
Critical (0)
Overloaded (0)
Warning (0)
OK (1)
Configuration
Users and Groups
Roles and Policies
Credential Mappings
Providers
Migration
Users
Groups
Customize this table
New
Delete
Showing 1 to 9 of 9 Previous | Next

Settings for myrealm

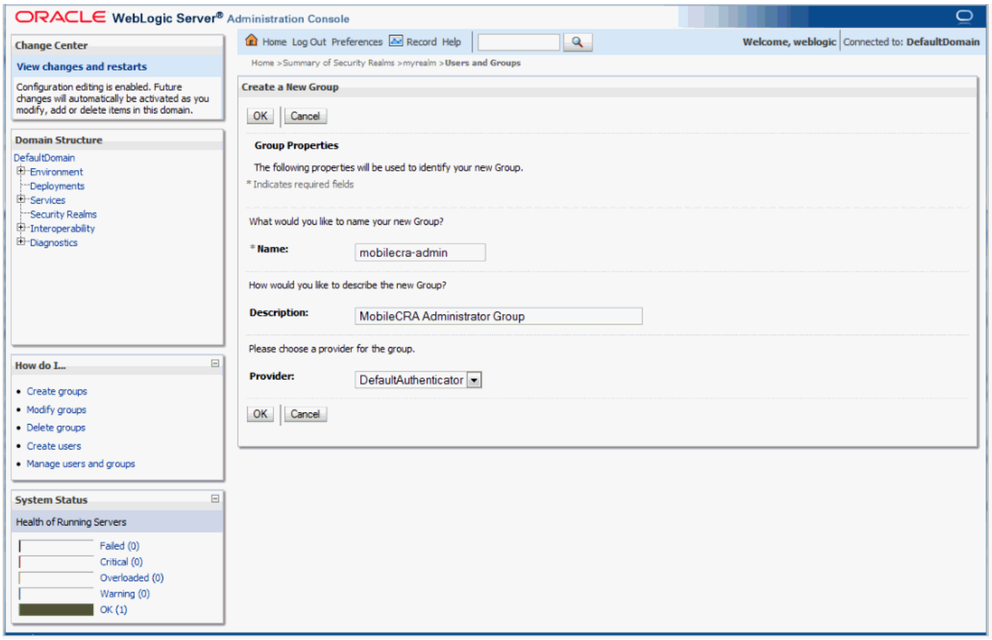
This page displays information about each group that has been configured in this security realm.

Groups

□	Name	Description	Provider
□	AdminChannelUsers	AdminChannelUsers can access the admin channel.	DefaultAuthenticator
□	Administrators	Administrators can view and modify all resource attributes and start and stop servers.	DefaultAuthenticator
□	AppTesters	AppTesters group.	DefaultAuthenticator
□	CrossDomainConnectors	CrossDomainConnectors can make inter-domain calls from foreign domains.	DefaultAuthenticator
□	Deployers	Deployers can view all resource attributes and deploy applications.	DefaultAuthenticator
□	GlobalUser		DefaultAuthenticator
□	Monitors	Monitors can view and modify all resource attributes and perform operations not restricted by roles.	DefaultAuthenticator
□	Operators	Operators can view and modify all resource attributes and perform server lifecycle operations.	DefaultAuthenticator
□	OracleSystemGroup	Oracle application software system group.	DefaultAuthenticator

5. Create a new group with the name `mobilecra-admins` and the description as `Mobile CRA Administrator Group`.

Figure 16 Create a New Group Screen


ORACLE WebLogic Server® Administration Console
Home Log Out Preferences Record Help
Welcome, weblogic | Connected to: DefaultDomain
Home >Summary of Security Realms >myrealm >Users and Groups
Change Center
View changes and restarts
Configuration editing is enabled. Future changes will automatically be activated as you modify, add or delete items in this domain.
Domain Structure
DefaultDomain
Environment
Deployments
Services
Security Realms
Interoperability
Diagnostics
How do I...
Create groups
Modify groups
Delete groups
Create users
Manage users and groups
System Status
Health of Running Servers
Failed (0)
Critical (0)
Overloaded (0)
Warning (0)
OK (1)
OK
Cancel

Create a New Group

Group Properties

The following properties will be used to identify your new Group.

* Indicates required fields

What would you like to name your new Group?

* Name: mobilecra-admin

How would you like to describe the new Group?

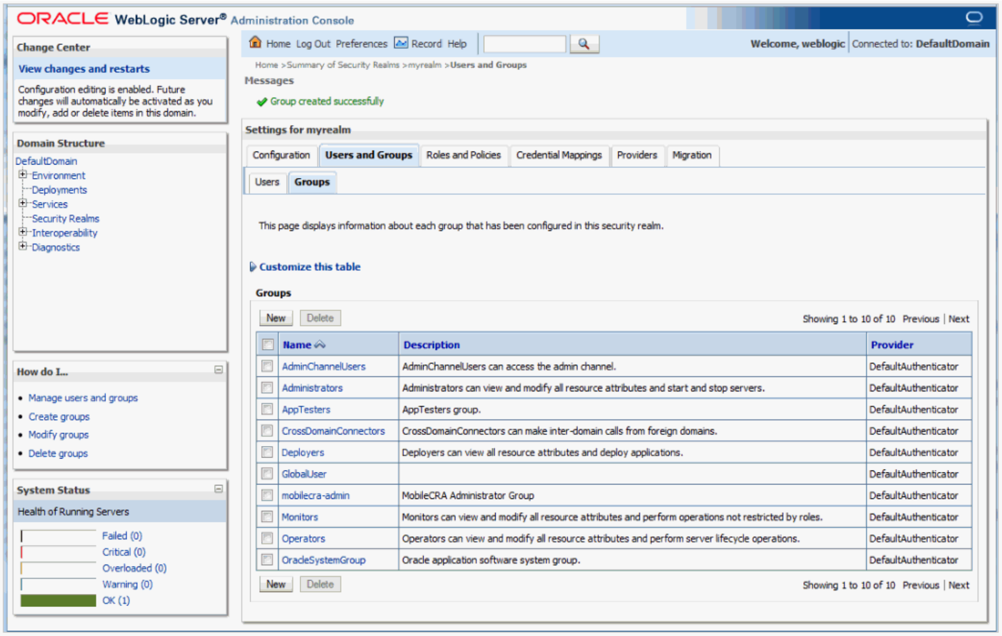
Description: MobileCRA Administrator Group

Please choose a provider for the group.

Provider: DefaultAuthenticator

6. Validate to confirm the administrator group has been successfully created.

Figure 17 Validate the Creation of the Group



ORACLE WebLogic Server® Administration Console

Home Log Out Preferences Record Help

Welcome, weblogic | Connected to: DefaultDomain

Change Center

View changes and restarts

Configuration editing is enabled. Future changes will automatically be activated as you modify, add or delete items in this domain.

Domain Structure

DefaultDomain
- Environment
- Deployments
- Services
- Security Realms
- Interoperability
- Diagnostics

How do I...

- Manage users and groups
- Create groups
- Modify groups
- Delete groups

System Status

Health of Running Servers

Failed (0)
Critical (0)
Overloaded (0)
Warning (0)
OK (1)

Home >Summary of Security Realms >myrealm >**Users and Groups**

Messages

✓ Group created successfully

Settings for myrealm

Configuration | **Users and Groups** | Roles and Policies | Credential Mappings | Providers | Migration

Users | **Groups**

This page displays information about each group that has been configured in this security realm.

Customize this table

Groups

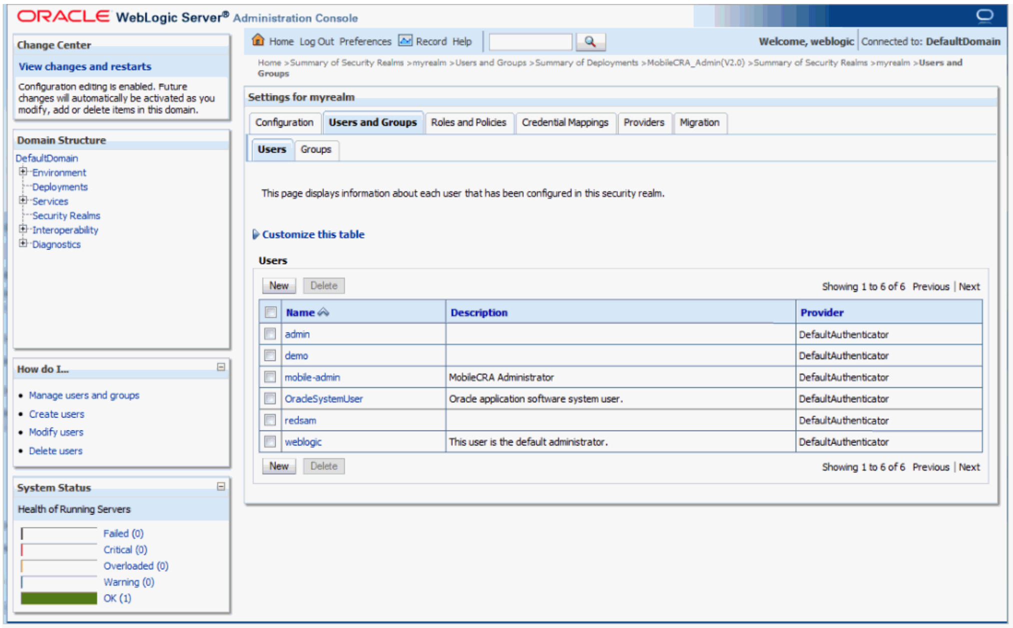
New Delete Showing 1 to 10 of 10 Previous | Next

□	Name	Description	Provider
□	AdminChannelUsers	AdminChannelUsers can access the admin channel.	DefaultAuthenticator
□	Administrators	Administrators can view and modify all resource attributes and start and stop servers.	DefaultAuthenticator
□	AppTesters	AppTesters group.	DefaultAuthenticator
□	CrossDomainConnectors	CrossDomainConnectors can make inter-domain calls from foreign domains.	DefaultAuthenticator
□	Deployers	Deployers can view all resource attributes and deploy applications.	DefaultAuthenticator
□	GlobalUser		DefaultAuthenticator
□	mobilecra-admin	MobileCRA Administrator Group	DefaultAuthenticator
□	Monitors	Monitors can view and modify all resource attributes and perform operations not restricted by roles.	DefaultAuthenticator
□	Operators	Operators can view and modify all resource attributes and perform server lifecycle operations.	DefaultAuthenticator
□	OracleSystemGroup	Oracle application software system group.	DefaultAuthenticator

New Delete Showing 1 to 10 of 10 Previous | Next

7. Select the **Users** tab within the Security section.

Figure 18 Users Tab



ORACLE WebLogic Server® Administration Console

Home Log Out Preferences Record Help

Welcome, weblogic | Connected to: DefaultDomain

Change Center

View changes and restarts

Configuration editing is enabled. Future changes will automatically be activated as you modify, add or delete items in this domain.

Domain Structure

DefaultDomain
- Environment
- Deployments
- Services
- Security Realms
- Interoperability
- Diagnostics

How do I...

- Manage users and groups
- Create users
- Modify users
- Delete users

System Status

Health of Running Servers

Failed (0)
Critical (0)
Overloaded (0)
Warning (0)
OK (1)

Home >Summary of Security Realms >myrealm >Users and Groups >Summary of Deployments >MobileCRA_Admin(V2.0) >Summary of Security Realms >myrealm >**Users and Groups**

Settings for myrealm

Configuration | **Users and Groups** | Roles and Policies | Credential Mappings | Providers | Migration

Users | Groups

This page displays information about each user that has been configured in this security realm.

Customize this table

Users

New Delete Showing 1 to 6 of 6 Previous | Next

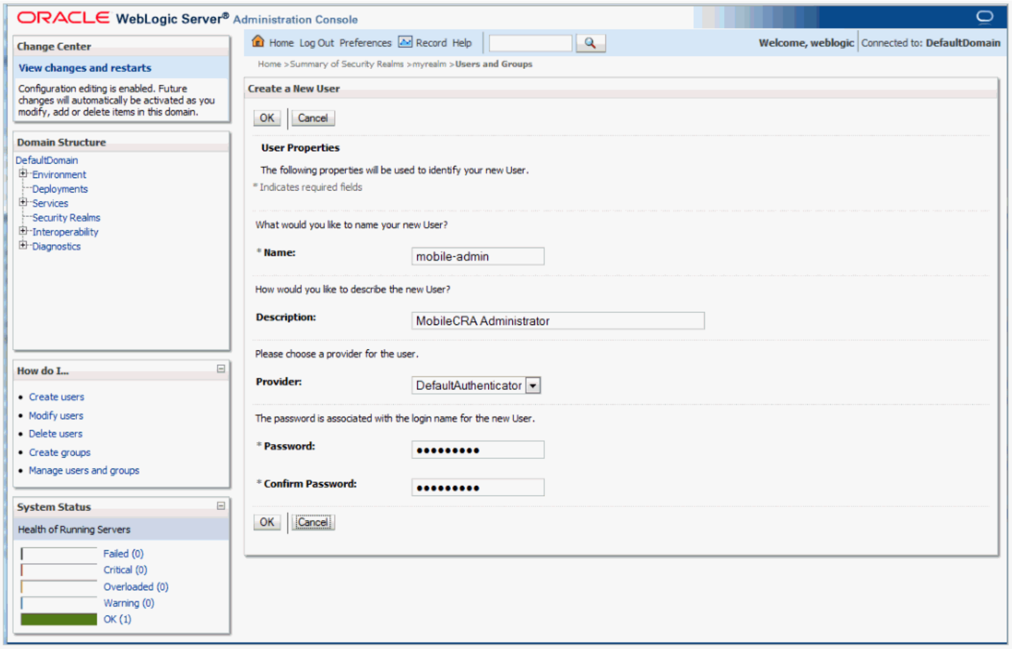
□	Name	Description	Provider
□	admin		DefaultAuthenticator
□	demo		DefaultAuthenticator
□	mobile-admin	MobileCRA Administrator	DefaultAuthenticator
□	OracleSystemUser	Oracle application software system user.	DefaultAuthenticator
□	redsam		DefaultAuthenticator
□	weblogic	This user is the default administrator.	DefaultAuthenticator

New Delete Showing 1 to 6 of 6 Previous | Next

The **Create a New User** screen is displayed.

8. Create a new arbitrary or predefined user with the name `mobile-admin` and the description as `Mobile CRA Administrator`.

Figure 19 Create a New User Screen



Configuration editing is enabled. Future changes will automatically be activated as you modify, add or delete items in this domain.

Create a New User

User Properties

The following properties will be used to identify your new User.

* Indicates required fields

What would you like to name your new User?

* **Name:** mobile-admin

How would you like to describe the new User?

Description: MobileCRA Administrator

Please choose a provider for the user.

Provider: DefaultAuthenticator

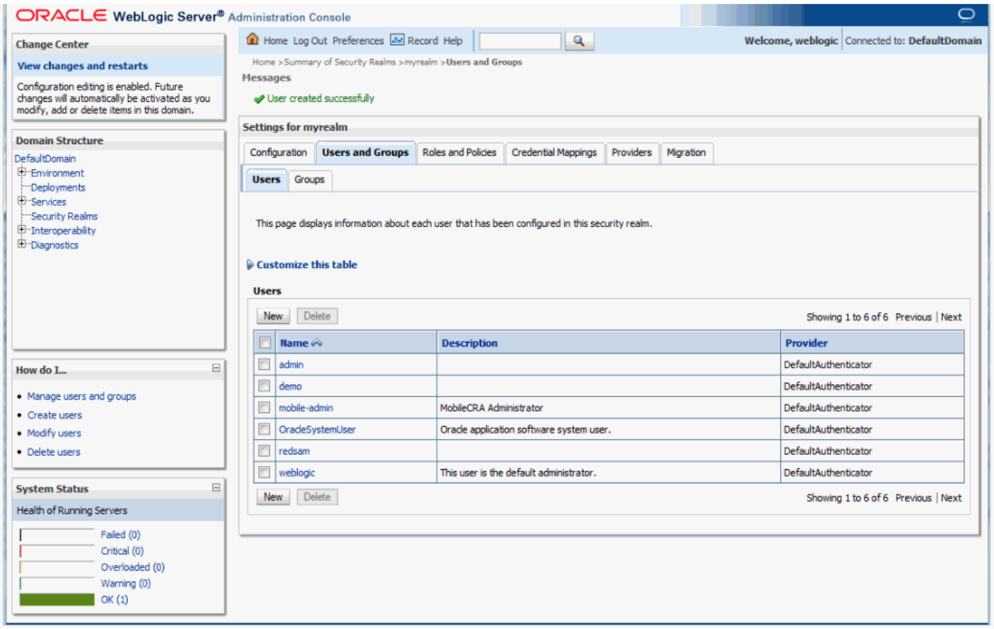
The password is associated with the login name for the new User.

* **Password:** •••••••••

* **Confirm Password:** •••••••••

9. Add the group `mobilecra-admin` to the newly created administrator user.
10. Validate to check if the administrator user has been successfully created.

Figure 20 Validate the Creation of the Administrator User



Configuration editing is enabled. Future changes will automatically be activated as you modify, add or delete items in this domain.

Messages

✓ User created successfully

Settings for myrealm

This page displays information about each user that has been configured in this security realm.

Users

Showing 1 to 6 of 6

□	Name	Description	Provider
□	admin		DefaultAuthenticator
□	demo		DefaultAuthenticator
□	mobile-admin	MobileCRA Administrator	DefaultAuthenticator
□	OracleSystemUser	Oracle application software system user.	DefaultAuthenticator
□	redsam		DefaultAuthenticator
□	weblogic	This user is the default administrator.	DefaultAuthenticator

Showing 1 to 6 of 6

Note: For integration with other security providers, such as Lightweight Directory Access Protocol (LDAP) or Single Sign-On (SSO), see the *Oracle WebLogic Administration Guide*.

9 Protecting Data

Data is vulnerable at many points in any computer system, and many security techniques and types of functionality can be employed to protect it.

10 Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc`.

Access to Oracle Support

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

Oracle Health Sciences Mobile Clinical Research Associate Security Guide, Release 1.0
E38752-01