Oracle® Health Sciences Mobile Clinical Research Associate Server

Security Guide Release 1.3

E38752-04

March 2014

1 Introduction

The Oracle Health Sciences Mobile Clinical Research Associate Server (Mobile CRA) mobile application supports the clinical research analyst in conducting site visits. This release provides 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. Oracle recommends you 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 enables remote administration. For more information, refer to the section "Removing the Listener Password" of *Oracle® Database Net Services Reference 11g Release 2 (11.2)*.

For more information, refer to the Oracle 11gR2 Database Security Guide.

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 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, Create Job, Create Synonym, Create View, Select Any Table, Unlimited Tablespace

• 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, Oracle recommends 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. 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. 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. 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* 12*c 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 1-13

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:

- 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**.

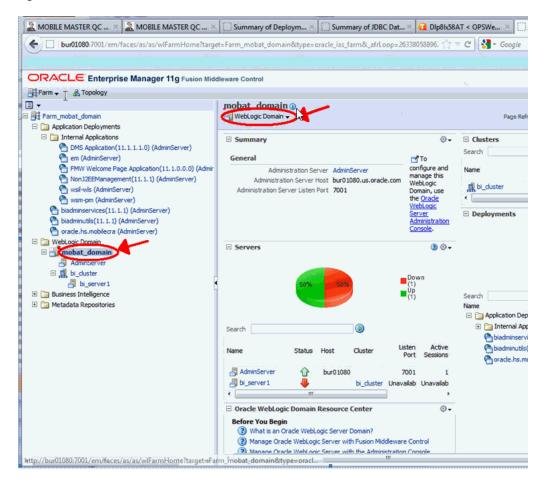


Figure 1 server_domain Screen

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

🤽 MOBILE MASTER QC ... × 📓 MOBILE MASTER QC ... × 🖸 Summary of Deploym... × 🗍 Summary of JDBC Dat... × 🚹 Dlp8b58AT < OPSWe... 🗲 📋 🖢 🕼 🖕 😓 🖕 burð1080/7001/em/faces/as/as/wiFarmHome?target=Farm_mobat_domain&type=oracle_jas_farm&_afrLoop=26338058896; 🏠 🗸 🧭 🛃 😪 Google ORACLE Enterprise Manager 11g Fusion Middleware Control Farm 🗸 📔 🚠 Topology - 🗉 mobat_domain () WebLogic Domain 🗸 E 📴 Farm_mobat_domain Page Re 🖃 🚞 Application Deployments Home 🖃 🚞 Internal Applications ·. C DMS Application (11.1.1.1.0) (AdminServer) Control em (AdminServer) To configure and manage this Logs WebLogic Domain, use the Oracle WebLogic Server Administration FMW Welcome Page Application(11.1.0.0.0) (Admir NonJ2EEManagement(11.1.1) (AdminServer) orade.com Port Usage 🚰 wsm-pm (AdminServer) biadminservices(11.1.1) (AdminServ biadminutls(11.1.1) (AdminServer) oracle.hs.mobilecra (AdminServer) 0 . biadminservices(11.1.1) (AdminServer) Application Deployment Web Services 🖃 🪞 WebLogic Domain Security Credentials 🖻 📑 mobat_domain Metadata Repositories AdminServer IDBC Data Sources Security Provider Configuration 🗉 🧸 bi_duster System MBean Browse bi_server1 Application Policies 🗉 🫅 Business Intelligence Bear Accesse (pe minute WebLogic Server Administration Console 🗄 🛅 Metadata Repositories Application Roles General Information System Policies 0.0 bi_server1 ы Unavaila Audit Policy . 1 Audit Store Oracle WebLogic Domain Resource Center . **Before You Begin** (?) What is an Oracle WebLogic Server Domain? (2) Manage Oracle WebLogic Server with Fusion Middleware Control (2) 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 A # 1 10

Figure 2 Credentials Submenu

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 / Applications can use the Credential Store, a single, consolidated service provider to store and manage their credenti

Ï	🕂 Create Map	🕂 Create Key	/ Edit	💥 Delete	Credential Key Nam	e			
	Credential			Туре	Descriptio	n			
	🕀 💼 orade.bi	i.enterprise							
	🕀 📄 orade.bi	i.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 is 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		
Кеу Туре	oracle.hs.mobilecra notificationService.Credential Password	You can enter a dif
* User Name * Password	ns_user	
* Confirm Password Description		· · ·
Description		
		.::
		OK Cancel

- g. Click OK.
- **8.** Click **Create Key** to create another key. The **Select Map** field is updated with the map name. Now perform the following:
 - **a.** Enter key as ctmsAdapter.systemCredential. This is the CTMS admin user name and the CTMS SSO token password. Mobile CRA uses this information to access CTMS.
 - **b.** Enter type as Password.
 - c. Enter the CTMS super user name and the CTMS SSO token 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	
	ctmsAdapter.SystemCredential	
Type	Password	You can enter a diff
* User Name	SADMIN	
* Password	•••••	
* Confirm Password	•••••	
Description		
		T.::
		1
	· · · · · · · · · · · · · · · · · · ·	OK Cancel

- g. Click OK.
- **9.** Click **Create Key** to create another key. The **Select Map** field is 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

Key	oracle.hs.mobilecra ctmsAdapter.SSOTokenCredential Generic
Description	
* Credential	

- f. Click OK.
- **10.** Click **Create Key** to create another key. The **Select Map** field is 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 Key Type	cdaAdapter.ObieeCredential	You can enter a diff
* User Name	mobilecra-admin	
* Password	•••••	
* Confirm Password	•••••	
Description		
		OK Cancel

h. Click OK.

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 8 Domain Structure Window



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

Figure 9 Summary of Security Realms Screen

nary 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

Ims (Filtered - More Columns Exist)

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

e	w Delete	Showing 1 to 1 of 1 Previous
	Name 🗞	Default Realm
	myrealm	true
e	w 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 10 List of Existing Users

and a wake a literature and Const.	Dalas and Dalains	Condential Manairan	Providers	Marchen	
onfiguration Users and Grou	Ips Roles and Policies	Credential Mappings	Providers	Migration	
Jsers Groups					
This page displays information ab	out each user that has be	en configured in this sea	urity realm.		
			arrey realm		
Customize this table					
Users					
New Delete					Showing
New Delete	Description				Showing Provider
	Description BI System User				Provider
🗖 Name 🌣					Provider DefaultAut
Name BISystemUser	BI System User CSTONE	n software system user.			Provider DefaultAut DefaultAut
Name Name SISystemUser CSTONE	BI System User CSTONE	n software system user.			
Name BISystemUser CSTONE OradeSystemUser	BI System User CSTONE Oracle application	n software system user.			Provider DefaultAut DefaultAut DefaultAut

6. Click **New** to create a new user. The **Create a New User** screen is displayed.

Figure 11 Create a New User Screen

Create a New User								
OK								
User Properties								
The following properties will be * Indicates required fields	used to identify your new User.							
What would you like to name you	ur new User?							
* Name:								
How would you like to describe t	ow 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:								
OK Cancel								

- **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 12 Selecting Security Realms

lange Center	💼 Home Log Out Preferences 🔤 Record Help	Q.	Welcome, weblogic Connected to: DefaultDoma	
iew changes and restarts	Home			
onfiguration editing is enabled. Future langes will automatically be activated as you odify, add or delete items in this domain.	Home Page			
bury, add or delete items in this domain.	Information and Resources			
omain Structure	Helpful Tools	General Information		
faultDomain	 Configure applications 	 Common Administration Task Descriptions 		
Environment	 Configure GridLink for RAC Data Source 	 Read the documentation 		
Deployments Services	 Recent Task Status 	 Ask a question on My Oracle Support 		
Services "Security Realms "Interoperability	 Set your console preferences 	 Orade Guardian Overview 		
"Diagnostics	- Domain Configurations			
	Domain	Services	Interoperability	
	Domain	Messaging	WTC Servers	
		 JMS Servers 	Jolt Connection Pools	
	Environment	 Store-and-Forward Agents 		
	Servers	 JMS Modules 	Diagnostics	
	Clusters	 Path Services 	Log Files	
e do I	Virtual Hosts	 Bridges 	Diagnostic Modules	
Search the configuration	Migratable Targets	Data Sources	Diagnostic Images	
Use the Change Center	Coherence Servers	Persistent Stores	Request Performance	
Record WLST Scripts	Coherence Clusters	XML Registries	Archives	
Change Console preferences	Machines	XML Entity Caches	Context	
Monitor servers	Work Managers	 Foreign JNDI Providers 	SNMP	
	Startup And Shutdown Classes	Work Contexts		
/stem Status 🖂		• jCOM	Charts and Graphs	
ealth of Running Servers	Your Deployed Resources	Mail Sessions	 Monitoring Dashboard [®] 	
-	Deployments	FileT3		
Failed (0) Critical (0)		• JTA		
Overloaded (0)	Your Application's Security Settings			
Warning (0)	Security Realms			
OK (1)				

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

3. Select the security realm.

Figure 13 Summary of Security Realm screen

	Administration Console		Q	
Change Center	🔒 Home Log Out Preferences 🔤 Record Help	Q	Welcome, weblogic Connected to: DefaultDomai	
View changes and restarts	Home >Summary of Security Realms			
Configuration editing is enabled. Future changes will automatically be activated as you modify, add or delete items in this domain.	Summary of Security Realms			
Domain Structure	A security realm is a container for the mechanisms resources. You can have multiple security realms in a	ncluding users, groups, security roles, secur a WebLogic Server domain, but only one can	ity policies, and security providersthat are used to protect WebLogic be set as the default (active) realm.	
DefaultDomain Environment Deployments Briservices	hat has been configured in this WebLogic Se	ry we can be set to be actual geory claim.		
Security Realms	Customize this table			
⊕ Diagnostics	Realms (Filtered - More Columns Exist) New Delete		Showing 1 to 1 of 1 Previous Next	
	🔲 Name 😞	Default Realm		
	🗇 myrealm	true		
	New Delete		Showing 1 to 1 of 1 Previous Next	
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)				

The Settings for myrealm screen is displayed.

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

Figure 14 Settings for myrealm Screen

Change Center	(<u></u>	Home Log	Out Preferences 🔤 F	Record Help	٩			Welcome, weblogic	Connected to: DefaultDo
View changes and restarts	Hor	ne >Summa	iry of Security Realms >m	yrealm >Users and Gr	oups				
Configuration editing is enabled. Future		Settings for myrealm							
changes will automatically be activated as you modify, add or delete items in this domain.	Con	Configuration Users and Groups Roles and Policies Credential Mappings Providers Migration							
Domain Structure	Use	rs Gro	ups						
DefaultDomain (+): Environment +): Deployments (+): Services +): Services +): Services (+): Interoperability (+): Diagnostics		This page displays information about each group that has been configured in this security realm.							
			elete					Showin	g 1 to 9 of 9 Previous Nex
		Name		escription					Provider
	E	-			access the admin channe				DefaultAuthenticator
	E		trators Ad	ministrators can view	and modify all resource a	attributes and	d start and sto	p servers.	DefaultAuthenticator
How do I B		AppTes	ters Ap	pTesters group.					DefaultAuthenticator
Manage users and groups	E	CrossDo	omainConnectors Cro	ossDomainConnectors	can make inter-domain o	alls from for	tign domains.		DefaultAuthenticator
Create groups	E] Deploye	ers Dej	Deployers can view all resource attributes and deploy applications.					DefaultAuthenticator
 Modify groups 	E] GlobalU	ser						DefaultAuthenticator
Delete groups	E	Monitor	s Mo	nitors can view and m	odify all resource attribu	tes and perf	orm operation	not restricted by roles.	DefaultAuthenticator
] Operato	ors Op	erators can view and	modify all resource attrib	utes and per	form server li	ecycle operations.	DefaultAuthenticator
System Status B		OradeSystemGroup Oracle application software system group.				DefaultAuthenticator			
Health of Running Servers Failed (0) Critical (0)		Vew D	elete					Showin	g 1 to 9 of 9 Previous Ner
Overloaded (0) Warning (0)	<u> </u>								

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

Figure 15 Create a New Group Screen

Change Center	🔒 Home Log Out Preferences 🔤 Record Help	Welcome, weblogic Connected to: DefaultDomain
- View changes and restarts	Home >Summary of Security Realms >myrealm >Users and Groups	
Configuration editing is enabled. Future changes will automatically be activated as you modify, add or delete items in this domain.	Create a New Group OK Cancel	
Domain Structure	Group Properties	
DefaultDomain TEnvironment Deployments Services	The following properties will be used to identify your new Group. * Indicates required fields	
Security Realms B-Interoperability B-Diagnostics	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.	
How do I	Provider: DefaultAuthenticator	
Create groups		
Modify groups Delete groups	OK Cancel	
Create users		
Manage users and groups		
System Status 🖂		
Health of Running Servers		
Failed (0) Critical (0) Overloaded (0) Warning (0)		

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

Figure 16 Validate the Creation of the Group

	Adminis	tration C	onsole						Q
Change Center	🕜 н	ome Log (Out Preferences 🔤	Record Help	٩			Welcome, weblogic	Connected to: DefaultDomain
View changes and restarts Configuration editing is enabled. Future changes will automatically be activated as you modify, add or delete items in this domain.	Messa	ges	y of Security Realms >	myrealm >Users and G	oups				
	Settin	gs for m	realm						
Domain Structure DefaultDomain	Confi	guration	Users and Group	s Roles and Policies	Credential Mappings	Providers	Migration		
Environment Deployments	User	s Grou	DS						
B-Services →Security Realms B-Interoperability B-Diagnostics		page disp	,	it each group that has l	een configured in this s	ecurity realm.			
	Gro	ups	leto	Description				Showing 1	to 10 of 10 Previous Next
How do L.		AdminCh	annelUsers A	dminChannelUsers can	access the admin chann	el.			DefaultAuthenticator
		Administ	ators A	dministrators can view	and modify all resource a	attributes and	l start and sto	p servers.	DefaultAuthenticator
Manage users and groups Create groups		AppTest	ers A	ppTesters group.					DefaultAuthenticator
Modify groups		CrossDo	mainConnectors O	rossDomainConnectors	can make inter-domain (alls from fore	sign domains.		DefaultAuthenticator
Delete groups		Deployer	s D	eployers can view all re	source attributes and d	eploy applicat	ions.		DefaultAuthenticator
	[]	GlobalUs	er						DefaultAuthenticator
System Status		mobilecra	a-admin M	lobileCRA Administrator	Group				DefaultAuthenticator
Health of Running Servers		Monitors	м	lonitors can view and m	odify all resource attribu	ites and perfe	orm operations	s not restricted by roles.	DefaultAuthenticator
Failed (0)		Operato	s O	perators can view and	modify all resource attri	outes and per	form server lif	fecycle operations.	DefaultAuthenticator
Critical (0) Overloaded (0)		OracleS)	stemGroup 0	racle application softwa	are system group.				DefaultAuthenticator
Warning (0) OK (1)	N	ew De	lete					Showing 1	to 10 of 10 Previous Next

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

Figure 17 Users Tab

hange Center	- 🔒 H	lome Log	Out Preferences 🔤 I	Record Help	Q			Welcome, weblo	gic Connected to: DefaultDom		
view changes and restarts			ry of Security Realms >m	ryrealm >Users and Gro	ups >Summary of Deploy	ments >Mobii	eCRA_Admin(V2	.0) >Summary of Security	Realms >myrealm >Users and		
Configuration editing is enabled. Future	Gro	Groups									
comporation eating is enabled. Future changes will automatically be activated as you nodify, add or delete items in this domain.	Setti	Settings for myrealm									
	Con	figuration	Users and Groups	Roles and Policies	Credential Mappings	Providers	Migration				
omain Structure	lise	ers Grou	ins								
efaultDomain			4-s								
- Environment - Deployments	т	is nage dis	alays information about	each user that has be	en configured in this sea	urity realm					
D-Services											
Security Realms											
Diagnostics	₽ Cu	istomize	this table								
	Us	ers									
New Delete Showing :							wing 1 to 6 of 6 Previous Next				
	E	Name	~	Description				Provide	r		
		admin						DefaultAu	uthenticator		
	5 6	demo						DefaultAu	uthenticator		
łow do I		mobile-a	idmin	MobileCRA Adn	ninistrator			DefaultAu	uthenticator		
 Manage users and groups] OradeS	ystemUser	Oracle applicat	ion software system use	r.		DefaultAu	uthenticator		
Create users] redsam						DefaultAu	uthenticator		
Modify users Delete users		weblogi		This user is the	default administrator.			DefaultAu	uthenticator		
Delete users		New D	slete					Sho	wing 1 to 6 of 6 Previous Next		
ovstem Status	all										
fealth of Running Servers											
-											
Failed (0)											
Critical (0)											
Overloaded (0) Warning (0)											

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 18 Create a New User Screen

Change Center Image: An International Program Provided as you modify, add or delete Rems in this domain. Image: An International Provided as you modify, add or delete Rems in this domain. Image: An International Provided As You modify. Image: An Internat	efaultDomain								
Create a New User Create a New User Create a New User Create a New User Obmain Structure Defaultoman Defaultoman Defaultoman The following properties will be used to identify your new User.									
changes will automatically be activated as you modify, add or delete items in this domain. OK Cancel Domain Structure User Properties User Properties DefaulDomain The following properties will be used to identify your new User.									
Dodfy, add or delete items in this domain. OK Cancel Domain Structure User Properties User Properties DefaulDomain The following properties will be used to identify your new User. The following properties will be used to identify your new User.	Create a New User								
DefaulDoman User Properties DefaulDoman The following properties will be used to identify your new User.									
DefaultDomain Brwironment The following properties will be used to identify your new User.	User Properties								
Deployments Indicates required fields Bervices									
Security Realms What would you like to name your new User?	ALL DOUT THE DATE								
Diagnostics * Name: mobile-admin									
How would you like to describe the new User?									
Description: MobileCRA Administrator									
Please choose a provider for the user.									
How do L.									
Modify users The password is associated with the login name for the new User.									
Delete users Create groups * Password:									
Manage users and groups * Confirm Password:									
System Status									
Health of Running Servers OK Cance									
Faled (0)									
Critical (0) Overloaded (0)									
Warning (0)									
OK (1)									

- **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 19 Validate the Creation of the Administrator User

Change Center	Home Log	Out Preferences 🔤 F	Record Help	Q			Welcome, weblogic	Connected to: DefaultDom
View changes and restarts	Home >Summ Messages	ary of Security Realms >m	yrealm >Users and Gro	oups				
Configuration editing is enabled. Future changes will automatically be activated as you modify, add or delete items in this domain.	🖋 User crea	ted successfully						
Domain Structure	Settings for r	nyrealm						
DefaultDomain	Configuration	Users and Groups	Roles and Policies	Credential Mappings	Providers	Migration		
Environment Deployments	Users Gro	ups						
⊕-Services Security Realms ⊕-Interoperability ⊕-Diagnostics	This page de	plays information about	each user that has be	en configured in this sea	curity realm.			
	Vsers	elete	Description				Showing Provider	1 to 6 of 6 Previous Next
How do I	admin						DefaultAuther	nticator
Manage users and groups	🔄 demo						DefaultAuther	nticator
Manage users and groups Create users	mobile-	admin	MobileCRA Adm	inistrator			DefaultAuther	nticator
Modify users	Crade	SystemUser	Oracle applicati	on software system use	er.		DefaultAuther	nticator
Delete users	🗐 redsan						DefaultAuther	nticator
	weblog	ic	This user is the	default administrator.			DefaultAuther	nticator
System Status Health of Running Servers	New)elete					Showing	1 to 6 of 6 Previous Next
Failed (0) Critical (0) Overloaded (0) Warning (0)								

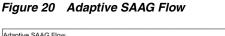
Note: For integration with other security providers, such as Lightweight Directory Access Protocol (LDAP) or Single Sign-On (SSO), see the *Oracle WebLogic Administration Guide*.

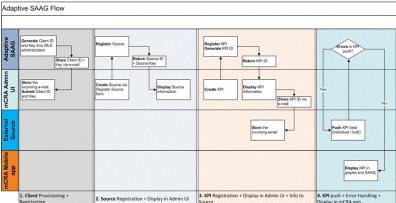
9 Adaptive SAAG Server

The Site At A Glance (SAAG) is a very important feature that helps the CRAs in site-monitoring and keeping themselves abreast with the site performances. Mobile CRA is redesigned to make the SAAG an open feature by exposing APIs using which any system can push in KPI information for the SAAG, once registered into the system. This is called Adaptive SAAG feature.

The following external components use Adaptive SAAG:

- **Client**: Client is an external entity where the application is hosted. Mobile CRA Server can be considered as a Client to Open SAAG Server.
- **Source**: Source is a third party internal or external system to the Client. There are two types of sources supported, KPI and Alert. Each client would be having multiple sources created. These sources provide runtime KPI data and as well as Alert.
- **Users**: Users of the application (Mobile CRA users).





9.1 Configuring Adaptive SAAG Server

To configure the Adaptive SAAG Server, perform the following:

1. Configure Health Sciences Push Notification Service (HSPNS) with key name as oracle.hs.oss.

Refer step 7 of Section 7.1, "Defining Credentials Used by Oracle Health Sciences Mobile Clinical Research Associate".

- **2.** Configure administrator user on Weblogic console.
- **3.** To configure user-level security using Enterprise Manager, perform the following:
 - **a.** Log in to WebLogic Server as administrator by entering the URL.

For example, http://server:7001/console

- b. Click Lock & Edit in the Change Center panel on the left side.
- c. Click Security Realms on the Domain Structure window.

Figure 21 Domain Structure Window

Domain Structure	
□ Services	
Messaging	
Data Sources	
Persistent Stores	
Foreign JNDI Providers	
Work Contexts	
XML Registries	
XML Entity Caches	н
jCOM	
Mail Sessions	
File T3	
L TTA	
Security Realms	_
Intermeration	1

The Summary of Security Realms screen is displayed.

Figure 22 Summary of Security Realms

ummary of Security Realms		
security providers that are used to	mechanismsincluding users, groups, security roles, security policies, a protect WebLogic resources. You can have multiple security realms in a e can be set as the default (active) realm.	ind
	ecurity realm that has been configured in this WebLogic Server domain.	Click
the name of the realm to explore an	configure that realm.	
Contraction alternation		
Customize this table		
Customize this table Realms (Filtered - More Column	: Exist)	
Realms (Filtered - More Column	FExist) hange Center to activate all the buttons on this page.	
Realms (Filtered - More Column	•	Nex
Realms (Filtered - More Column Click the <i>Lock & Edit</i> button in the C	hange Center to activate all the buttons on this page.	Nex
Realms (Filtered - More Column Click the <i>Lock & Edit</i> button in the C New Delete	hange Center to activate all the buttons on this page. Showing 1 to 1 of 1 Previous	Nex

d. Select **myrealm** from the list.

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

e. Click the Users and Groups tab and then click the Groups subtab.

The list of existing groups is displayed.

Figure 23 List of Existing Groups

	uration Users and Gro	ups Roles and Policies	Credential Mappings	Providers	Migration		
ers	Groups						
usi	page displays information a tomize this table	bout each group that has b	een configured in this se	ecurity realm.			
Ne	w Delete	1				Sho	wing 1 to 9 of 9 Previous Ne
	Name 🗠	Description					Provider
1	AdminChannelUsers	AdminChannelUsers can	access the admin channe	el.			DefaultAuthenticator
	Administrators	Administrators can view a	and modify all resource a	attributes and	start and stop se	vers.	DefaultAuthenticator
	AppTesters	AppTesters group.					DefaultAuthenticator
1			can make inter-domain o	alls from fore	ign domains.		DefaultAuthenticator
1	CrossDomainConnectors	CrossDomainConnectors					
	CrossDomainConnectors Deployers	CrossDomainConnectors Deployers can view all re		eploy applicat	ons.		DefaultAuthenticator
-				eploy applicat	ons.		DefaultAuthenticator DefaultAuthenticator
1	Deployers		source attributes and de			restricted by roles.	
1	Deployers GlobalUser	Deployers can view all re	source attributes and de odify all resource attribu	ites and perfo	rm operations not		DefaultAuthenticator

f. Click New and add a group with name OSSServiceAdmins.

Figure 24 Create a New Group

Create a New Grou	1p		
OK Cancel			
Group Propertie	3		
The following prop	erties will be used to identify your new Group.		
* Indicates required	fields		
What would you like	e to name your new Group?		
* Name:	OSSServiceAdmins		
How would you like	to describe the new Group?		
Description:	OSS Service Administrators		
Please choose a pro	ovider for the group.		
Provider:	DefaultAuthenticator 💌		
OK Cancel			

Note: Provider should be DefaultAuthenticator.

- g. Click Roles and Policies on the Settings for myrealm screen.
- h. Select Realm Roles and then click Roles under Global Roles.
- i. Click New to add a new Role.
- j. Add *OSSServiceAdminRole* and **Save**.

- **k.** Select **User** under **Users and Groups** tab.
- I. Click New and add a new User.

Once the user is created select the user in user list and click user to edit it.

- **m.** Click **Groups** tab to configure group for this user.
- **n.** Under Parents group available, select OSSServiceAdmins Group and click **Save**.

10 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.

11 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=trs if you are hearing impaired.

If this is software or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

This software or hardware and documentation may provide access to or information on content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services.

Oracle Health Sciences Mobile Clinical Research Associate Server Security Guide, Release 1.3 E38752-04

Copyright © 2013, 2014 Oracle and/or its affiliates. All rights reserved.

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.