

Application Server Installation Guide for OPSS - CSF

Oracle FLEXCUBE Universal Banking

Release 14.0.0.0.0

[December] [2017]



Table of Contents

1.	APPLICATION SERVER INSTALLATION GUIDE FOR OPSS - CSF	1-1
1.1	INTRODUCTION	1-1
1.1	.APPLICATION SERVER INSTALLATION FOR OPSS – CSF	1-1
1.2	CREATE OPSS SCHEMAS USING RCU	1-1
1.3	CREATE WEBLOGIC DOMAIN USING DOMAIN TEMPLATES	1-1
1.5	CONFIGURE CREDENTIAL MAP AND KEY	1-2

1. Application Server Installation Guide for OPSS - CSF

1.1 Introduction

Before using CSF(Credential Store Framework), you need to do Application server installation for OPSS(Oracle Platform Security Services) set up.

1.1 .Application Server Installation for OPSS – CSF

1. Create Weblogic Domain with Oracle Enterprise Manager & Oracle JRF templates
2. Extend an existing Weblogic Domain with Oracle Enterprise Manager & Oracle JRF templates
3. Create schemas using RCU

1.2 Create OPSS schemas using RCU

1. Run ./rcu from Oracle_Home/oracle_common/bin
2. Select Create Repository & System load and product load
3. Provide database connection details (sys/sysdba user and password)
4. Select OPSS
5. Provide schema passwords
6. Map table spaces
7. Click on Create button to complete installation.
8. Close

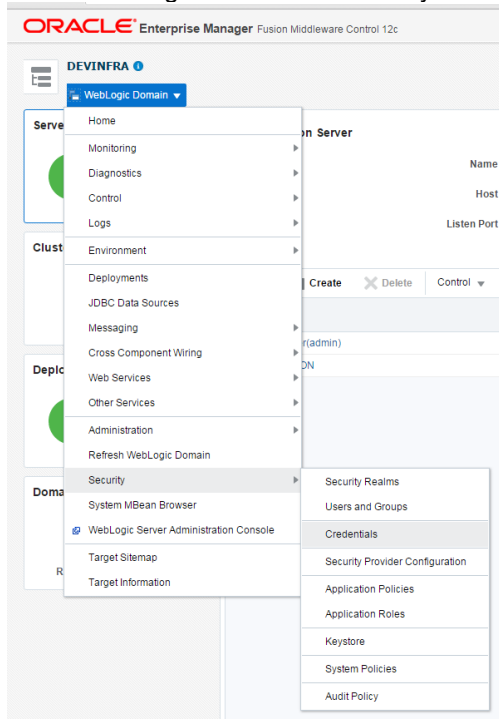
1.3 Create Weblogic domain using domain templates

1. Select Basic Weblogic Server Domain
2. Select Oracle Enterprise Manager
3. Select Oracle JRF
 - a. [once we select Oracle JRF , tool selecting Weblogic Coherence Cluster Extension also]
4. Select application location [select default values]
5. Select admin account
6. Select domain mode & JDK
7. Database configuration Types
 - a. Select RCU data
 - b. Enter database connection details using RCU Service table (STB) schema credentials.
 - c. Check / verify the component data sources
 - d. JDBC test
8. Adv configuration if required
9. Config summary
10. Click on create
11. Next & Finish

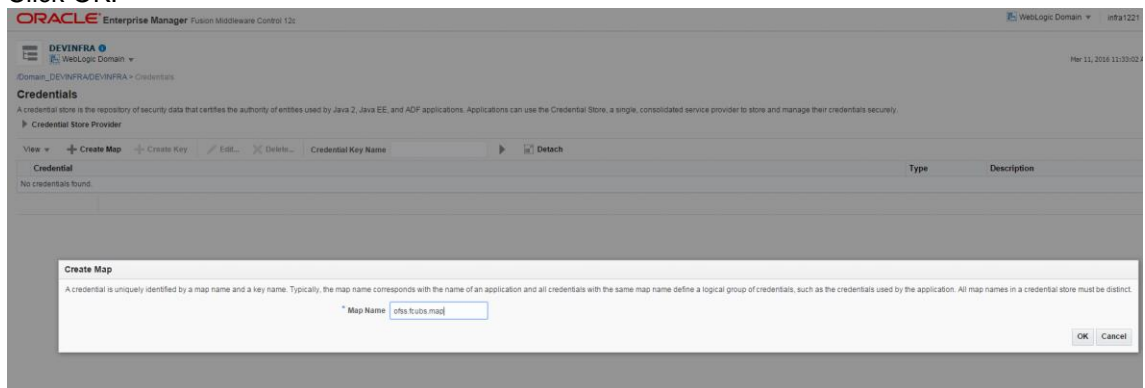
Refer: http://www.oracle.com/webfolder/technetwork/tutorials/obe/fmw/wls/12c/12_2_1/02-03-002-CreateJRFEMDomain/createjrfemdomain.html#overview

1.5 Configure credential MAP and KEY

1. Copy the fcubscommonscsf.jar from INSTALLER/SOFT/LIBRARY/ofss to \$DOMAIN_HOME/lib
2. Update the setDomainEnv.sh file (\$MW_HOME/user_projects/domains/mydomain/bin directory) by appending the above jar file path –
EXTRA_JAVA_PROPERTIES="{EXTRA_JAVA_PROPERTIES} -Dfcubs.csf.path=\${DOMAIN_HOME}"
3. Configure security via em console
4. Select Weblogic Domain -> Security -> Credentials. Click Create Map

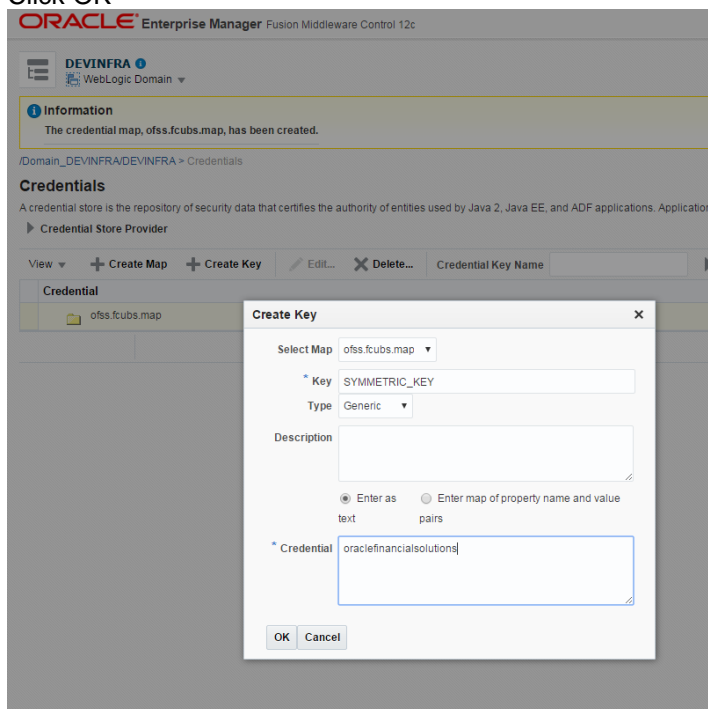


5. Enter the Map Name: ofss.fcubs.map
6. Click OK.

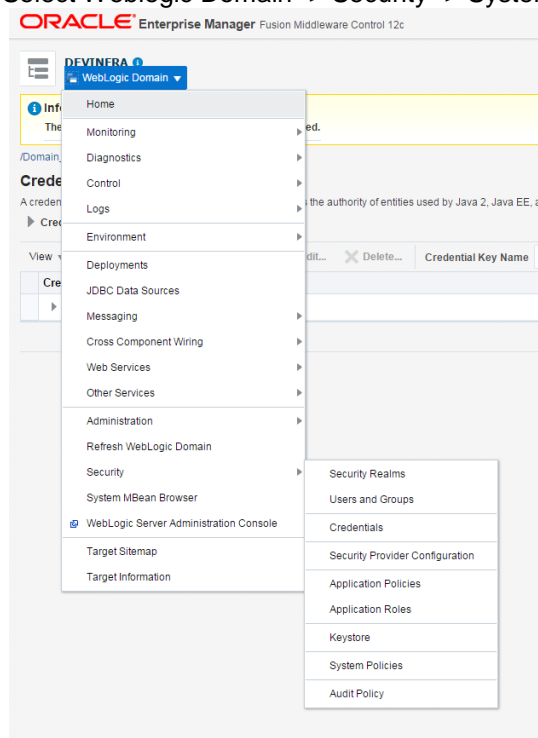


7. Create Key button
8. Enter the details as below
9. Select Map: ofss.fcubs.map

Key: SYMMETRIC_KEY
Type: Generic
Credentials: *oraclefinancialsolutions*
Click OK



10. Select Weblogic Domain -> Security -> System Policies.



11. Click Create

12. Enter Codebase

13. Codebase: file:\${fcubs.csf.path}/lib/fcubsccommonscsf.jar

14. Click Add. select checkbox “Select here to enter details for a new permission”

15. Provide below details

Permission Class: oracle.security.jps.service.credstore.CredentialAccessPermission
Resource Name: context=SYSTEM,mapName=ofss.fcubs.map,keyName=*

Permission Actions: read

ORACLE® Enterprise Manager Fusion Middleware Control 12c

DEVINFRA WebLogic Domain

/Domain_DEVINFRA/DEVINFRA > System Policies > Create System Grant

Create System Grant

There are two different types of system policies supported by application server: principal policy and codebase policy. Principal policy grants permissions and privileges to a list of users or roles. Codebase policy grants permissions and privileges to a specific codebase.

Grant To: Codebase

* Codebase: file:\${fcubs.csf.path}/lib/fcubscommonscaf.jar

Permissions

Add Permission

Select from permissions and resources used in system policies of this domain. Enter search criteria to search for right permissions.

Search

Type: Codebase

Name:

Permission:

Search Results

Name	Type	Permission
No permissions found.		

Select here to enter details for a new permission

* Permission Class: oracle.security.jps.service.credstore.CredentialAccessPermission

Resource Name: context=SYSTEM,mapName=ofss.fcubs.map,keyName=*

Permission Actions: read

16. Click on Ok for Add Permission and System policies.

ORACLE® Enterprise Manager Fusion Middleware Control 12c

DEVINFRA WebLogic Domain

Domain_DEVINFRA/DEVINFRA > System Policies

System Policies

System policies are the system-wide policies applied to all applications deployed to current management domain. You can grant special permissions and privileges to principal or codebase.

To manage users and groups in the WebLogic Domain, use the [Oracle WebLogic Server Security Provider](#).

Policy Store Provider

Search

Select a grant type and enter search keyword for codebase or principal to query system security grants.

Type: Codebase

Name: Includes: caf

View Create... Create Like... Edit... Delete...

Detach

Permissions for Codebase: file:\${fcubs.csf.path}/lib/fcubscommonscaf.jar

Resource Name	Permission Actions	Permission Class
context=SYSTEM,mapName=ofss.fcubs.map,keyName=*	read	oracle.security.jps.service.credstore.Cred...

17. click OK for create System Grant

18. Restart the servers[Admin, Managed servers]



Application Server Installation Guide for OPSS - CSF
[December] [2017]
Version 14.0.0.0.0

Oracle Financial Services Software Limited
Oracle Park
Off Western Express Highway
Goregaon (East)
Mumbai, Maharashtra 400 063
India

Worldwide Inquiries:
Phone: +91 22 6718 3000
Fax: +91 22 6718 3001
<https://www.oracle.com/industries/financial-services/index.html>

Copyright © 2007, 2017, Oracle and/or its affiliates. All rights reserved.

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

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 failsafe, 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.

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.

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.