OWSM Installation-Configuration on OAM 12.2.1.4

Version 1.0

Contents

1 Environment links

PreProd environment:
Jump Server:172.16.193.55

OAM1 Server:IAM-STG-1003.pap.bka.bund.de or 10.242.107.166

Links:

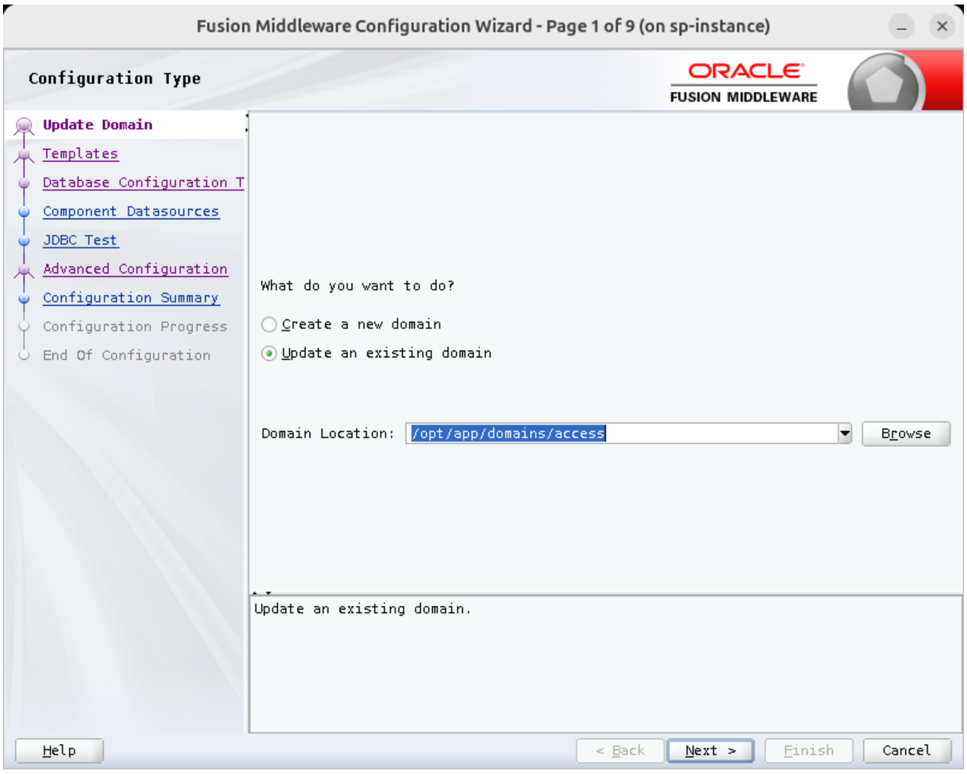
WLS Console:https://iam.stage.iaas.psp.extrapol.de/console/login/LoginForm.jsp
EM Console:https://iam.stage.iaas.psp.extrapol.de/em
OAM Console:https://iam.stage.iaas.psp.extrapol.de/oamconsole/faces/login.jspx
ODSM Console: https://access.extest.bka.extrapol.de:7400/odsm/faces/odsm.jspx

2 OWSM installation on OAM

OAM servers is by default not installed with Oracle WSM Policy Manager. In order to leverage OWSM policies WebLogic schema needs to be extended with “Oracle WSM Policy Manager” feature.

2.1 Domain extension

1. Change directory to $FMW_HOME/oracle_common/common/bin (For example: /opt/oracle/product/fmw/12.2.1/oracle_common/common/bin)
2. Start script **config.sh**
3. On the **Configuration Type** window select “Update an existing domain”. And select “Domain Location” where we want to install OWSM.



What do you want to do?

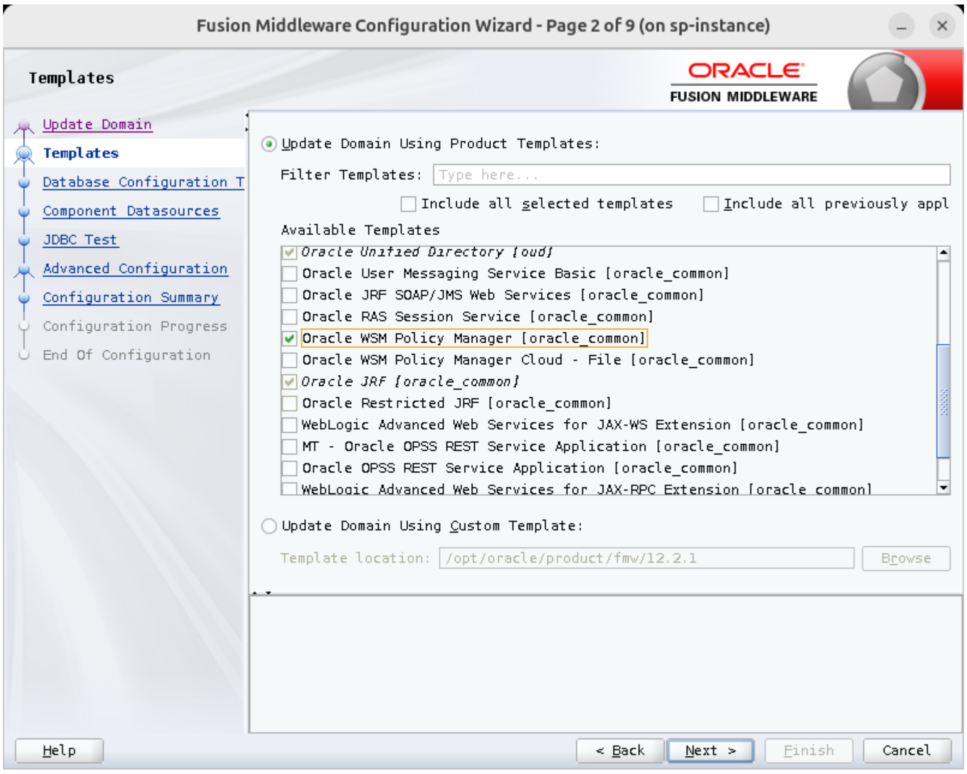
○ Create a new domain

● Update an existing domain

Domain Location: /opt/app/domains/access

Update an existing domain.

4. On the **Templates** window select “Oracle WSM Policy Manager”



Templates

● Update Domain Using Product Templates:

Filter Templates: Type here...

□ Include all selected templates □ Include all previously appl

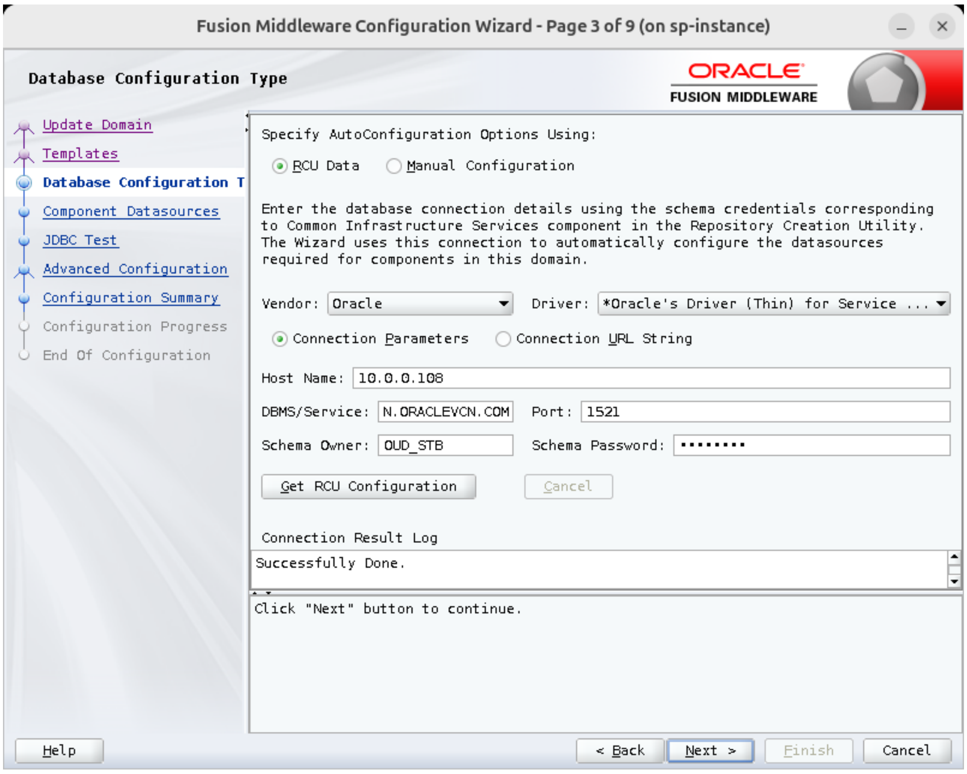
Available Templates

- ☑ *Oracle Unified Directory [oud]*
- □ Oracle User Messaging Service Basic [oracle_common]
- □ Oracle JRF SOAP/JMS Web Services [oracle_common]
- □ Oracle RAS Session Service [oracle_common]
- ☑ Oracle WSM Policy Manager [oracle_common]
- □ Oracle WSM Policy Manager Cloud - File [oracle_common]
- ☑ *Oracle JRF [oracle_common]*
- □ Oracle Restricted JRF [oracle_common]
- □ WebLogic Advanced Web Services for JAX-WS Extension [oracle_common]
- □ MT - Oracle OPSS REST Service Application [oracle_common]
- □ Oracle OPSS REST Service Application [oracle_common]
- □ WebLogic Advanced Web Services for JAX-RPC Extension [oracle_common]

○ Update Domain Using Custom Template:

Template location: /opt/oracle/product/fmw/12.2.1

5. On the **Database Configuration Type** window select “Get RCU Configuration”. When result is Successfully Done. Click on the Next button.



Database Configuration Type

Specify AutoConfiguration Options Using:

● RCU Data ○ Manual Configuration

Enter the database connection details using the schema credentials corresponding to Common Infrastructure Services component in the Repository Creation Utility. The Wizard uses this connection to automatically configure the datasources required for components in this domain.

Vendor: Oracle Driver: *Oracle's Driver (Thin) for Service ...

● Connection Parameters ○ Connection URL String

Host Name: 10.0.0.108

DBMS/Service: N.ORACLEVCN.COM Port: 1521

Schema Owner: OUD_STB Schema Password: ••••••••

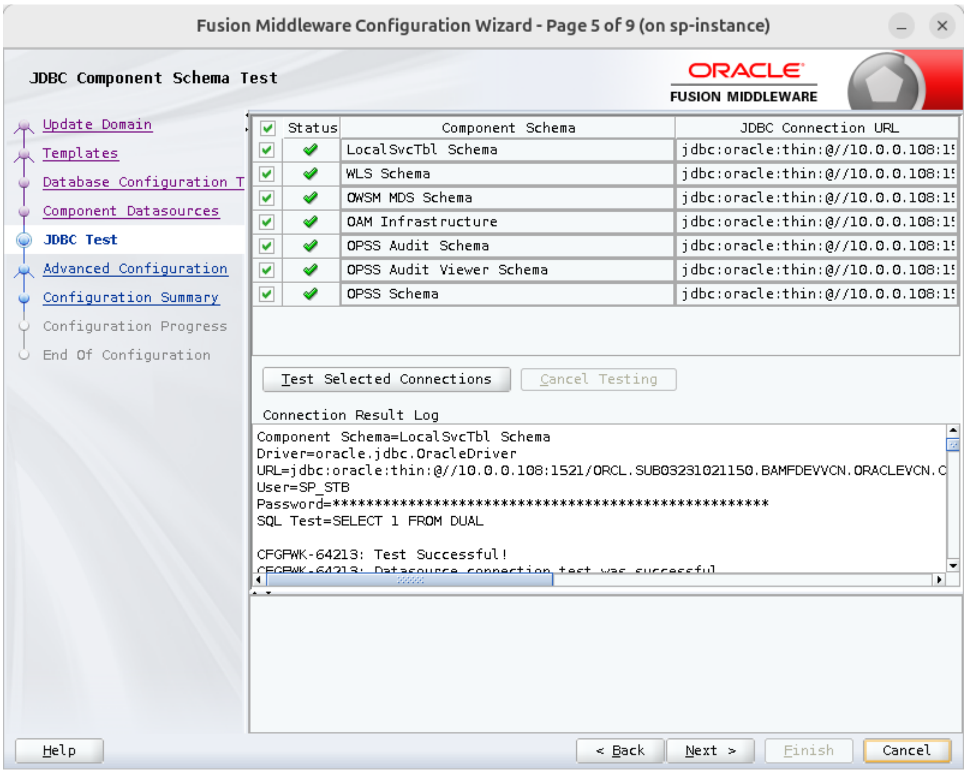
Connection Result Log

```
Successfully Done.
```

```
Click "Next" button to continue.
```

6. On the **Component Datasources** window click on the Next button.

7. On the JDBC Test window chcek if all went fine and then click Next button.



Fusion Middleware Configuration Wizard - Page 5 of 9 (on sp-instance)

JDBC Component Schema Test

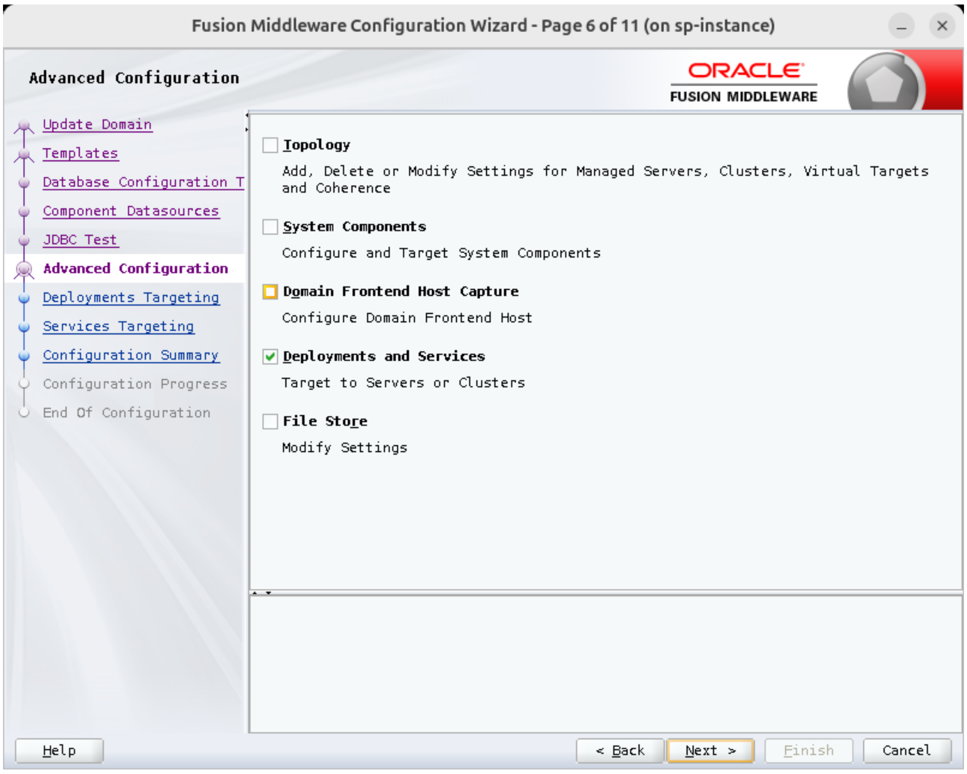
☑	Status	Component Schema	JDBC Connection URL
☑	✓	LocalSvcTbl Schema	jdbc:oracle:thin:@//10.0.0.108:15
☑	✓	WLS Schema	jdbc:oracle:thin:@//10.0.0.108:15
☑	✓	OWSM MDS Schema	jdbc:oracle:thin:@//10.0.0.108:15
☑	✓	OAM Infrastructure	jdbc:oracle:thin:@//10.0.0.108:15
☑	✓	OPSS Audit Schema	jdbc:oracle:thin:@//10.0.0.108:15
☑	✓	OPSS Audit Viewer Schema	jdbc:oracle:thin:@//10.0.0.108:15
☑	✓	OPSS Schema	jdbc:oracle:thin:@//10.0.0.108:15

Connection Result Log

```
Component Schema=LocalSvcTbl Schema
Driver=oracle.jdbc.OracleDriver
URL=jdbc:oracle:thin:@//10.0.0.108:1521/ORCL.SUB03231021150.BAMFDEVVCN.ORACLEVCN.C
User=SP_STB
Password=****************************************************
SQL Test=SELECT 1 FROM DUAL

CFGFWK-64213: Test Successful!
CFGFWK-64213: Datasource connection test was successful
```

8. On **Advanced Configuration** window select **Deployments and Services** click on Next button.



Fusion Middleware Configuration Wizard - Page 6 of 11 (on sp-instance)

Advanced Configuration

□ **Topology**
Add, Delete or Modify Settings for Managed Servers, Clusters, Virtual Targets and Coherence

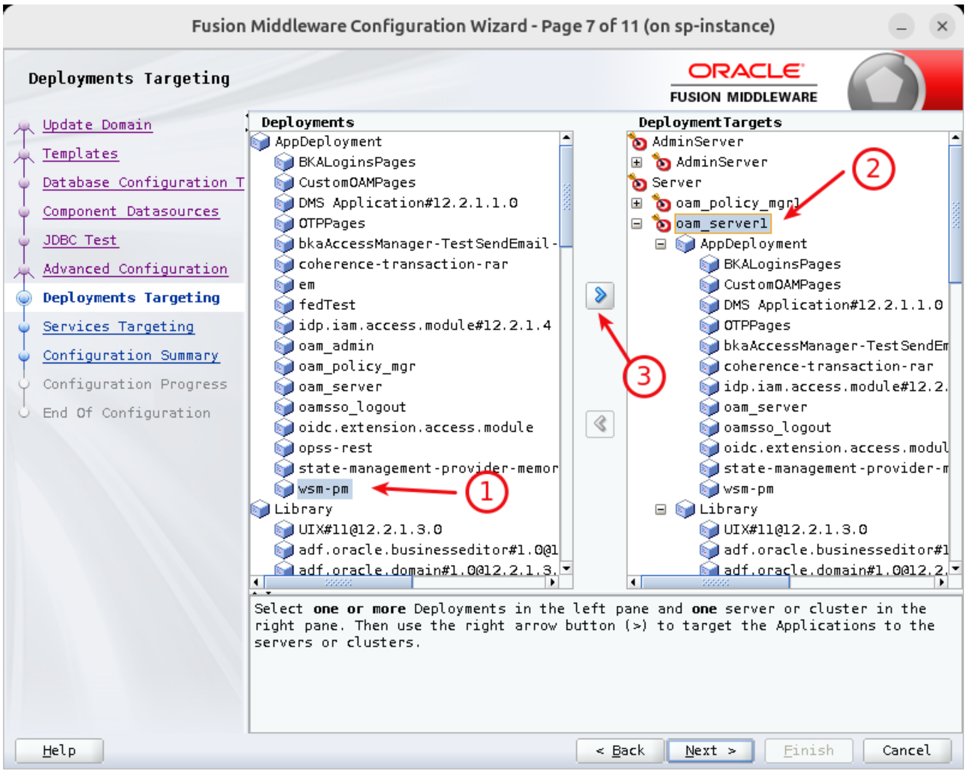
□ **System Components**
Configure and Target System Components

□ **Domain Frontend Host Capture**
Configure Domain Frontend Host

☑ **Deployments and Services**
Target to Servers or Clusters

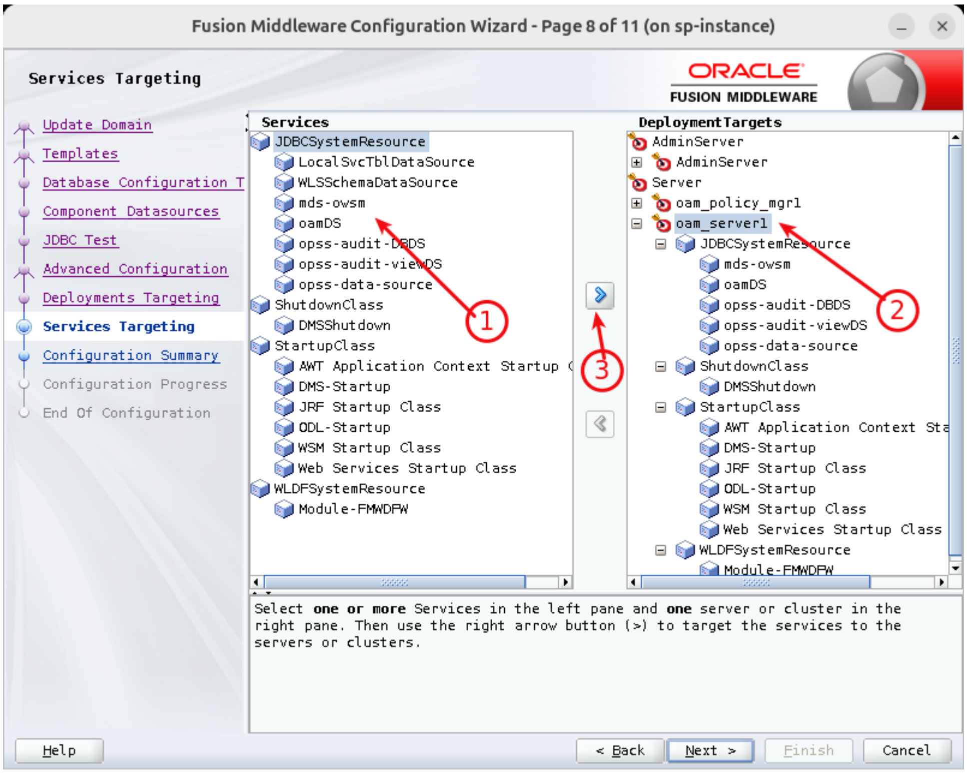
□ **File Store**
Modify Settings

9. On **Deployments Targeting** window select **wsp-pm** from Deployments column and in the Deployments Targets select oam_server1 or oam_cluster. Click on the assign arrow. Click on the Next button



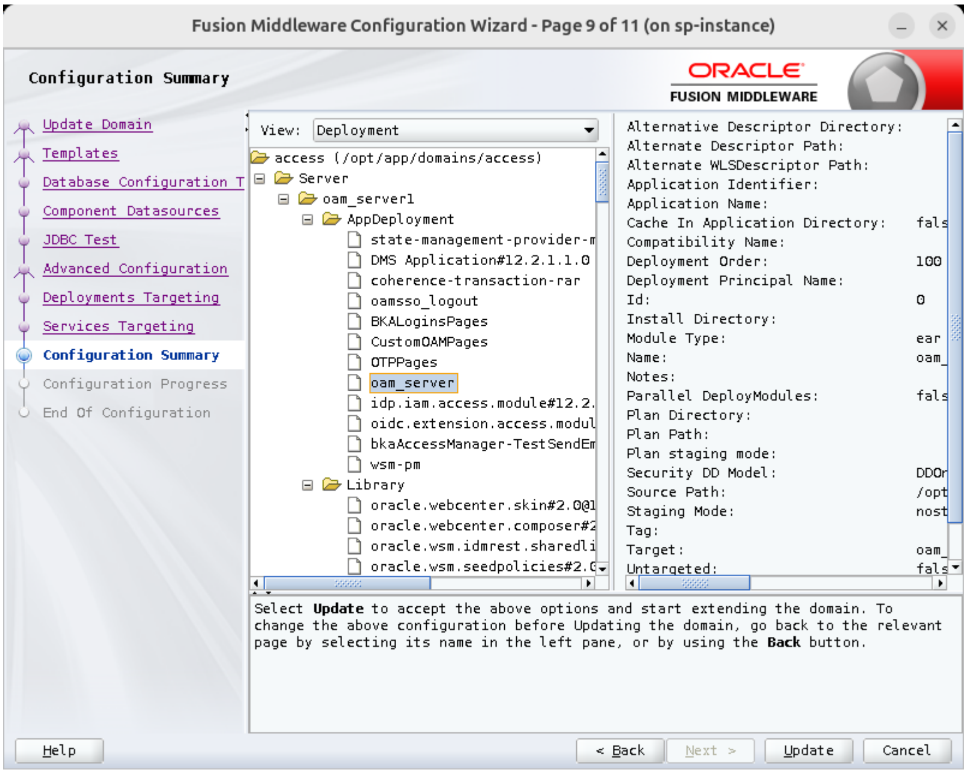
Select **one or more** Deployments in the left pane and **one** server or cluster in the right pane. Then use the right arrow button (>) to target the Applications to the servers or clusters.

10. On **Services Targeting** window select mds-owsm in the Services column. In the Deployment Targets select oma_server1 or oam_cluster. Click on the assign arrow. Click on the Next button.



Select **one or more** Services in the left pane and **one** server or cluster in the right pane. Then use the right arrow button (>) to target the services to the servers or clusters.

11.On **Configuration Summary** window click on Update button.

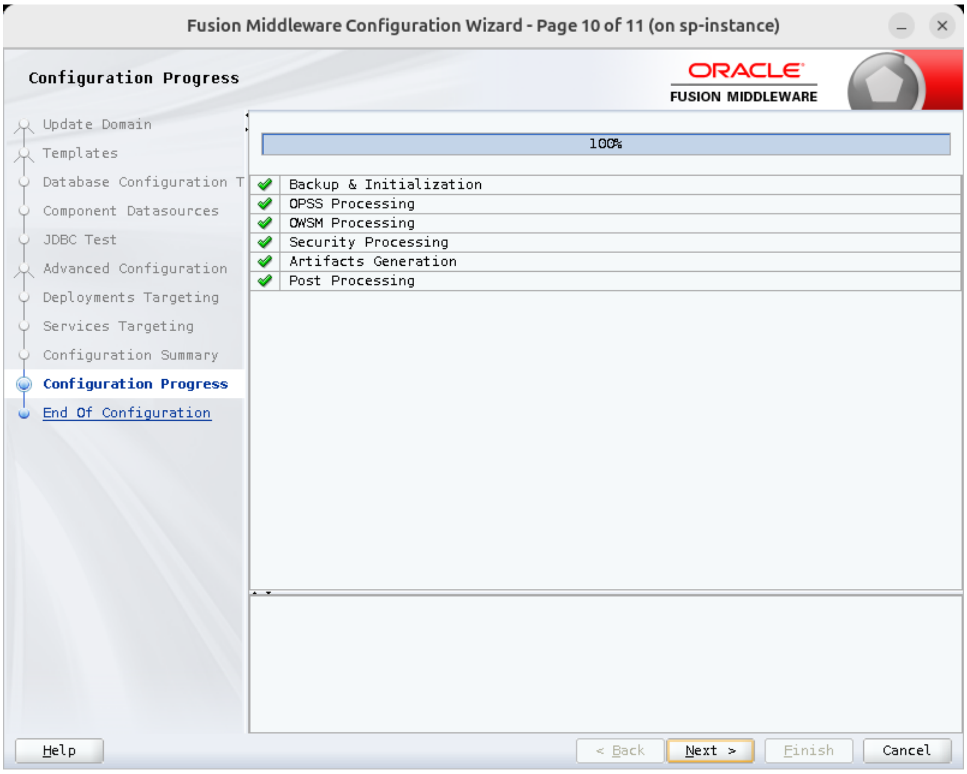


```
access (/opt/app/domains/access)
⊟ Server
  ⊟ oam_server1
    ⊟ AppDeployment
        state-management-provider-m
        DMS Application#12.2.1.1.0
        coherence-transaction-rar
        oamsso_logout
        BKALoginsPages
        CustomOAMPages
        OTPPages
        oam_server
        idp.iam.access.module#12.2.
        oidc.extension.access.modul
        bkaAccessManager-TestSendEm
        wsm-pm
    ⊟ Library
        oracle.webcenter.skin#2.0@1
        oracle.webcenter.composer#2
        oracle.wsm.idmrest.sharedli
        oracle.wsm.seedpolicies#2.0
```

```
Alternative Descriptor Directory:
Alternate Descriptor Path:
Alternate WLSDescriptor Path:
Application Identifier:
Application Name:
Cache In Application Directory:     fals
Compatibility Name:
Deployment Order:                   100
Deployment Principal Name:
Id:                                 0
Install Directory:
Module Type:                        ear
Name:                               oam_
Notes:
Parallel DeployModules:             fals
Plan Directory:
Plan Path:
Plan staging mode:
Security DD Model:                  DDOn
Source Path:                        /opt
Staging Mode:                       nost
Tag:
Target:                             oam_
Untargeted:                         fals
```

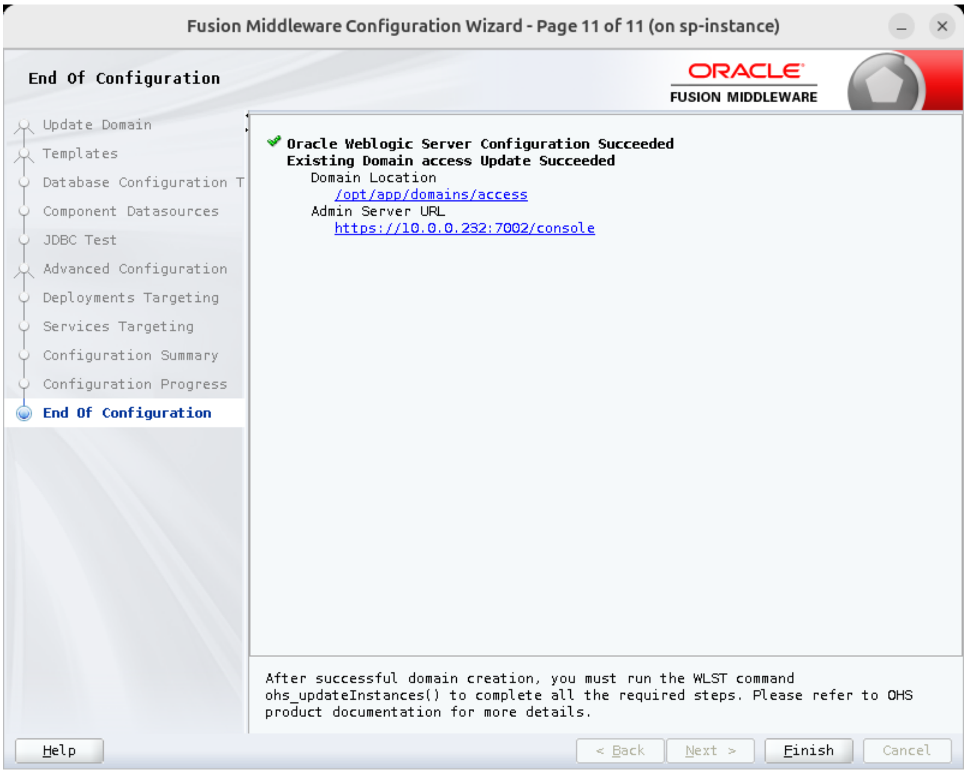
Select **Update** to accept the above options and start extending the domain. To change the above configuration before Updating the domain, go back to the relevant page by selecting its name in the left pane, or by using the **Back** button.

12. On **Configuration Process** click Next button



✓ Backup & Initialization
✓ OPSS Processing
✓ OWSM Processing
✓ Security Processing
✓ Artifacts Generation
✓ Post Processing

13.On **End Of Configuration** window click on the **Finish** button.



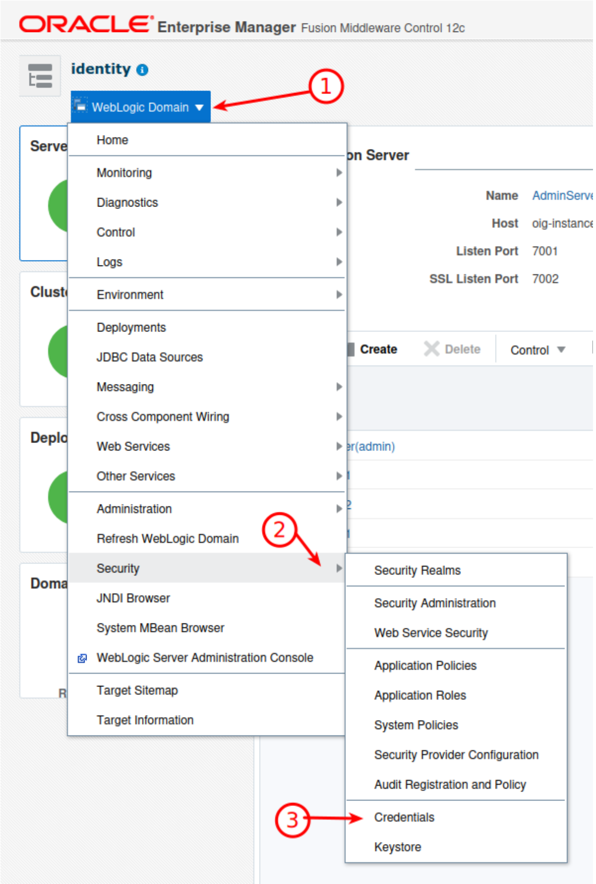
End Of Configuration

```
✓ Oracle Weblogic Server Configuration Succeeded
  Existing Domain access Update Succeeded
     Domain Location
        /opt/app/domains/access
     Admin Server URL
        https://10.0.0.232:7002/console
```

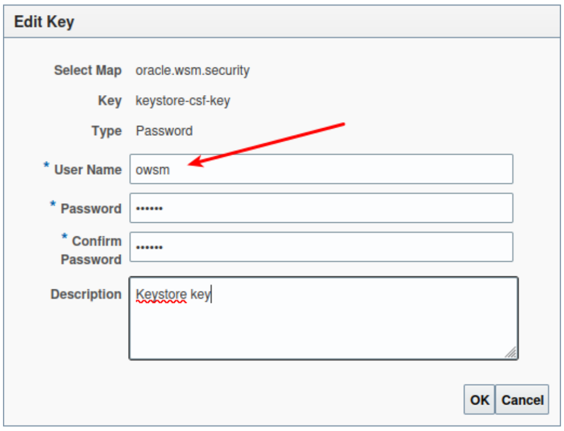
After successful domain creation, you must run the WLST command ohs_updateInstances() to complete all the required steps. Please refer to OHS product documentation for more details.

2.2 Extract OIG certificate used by UMS Server

1. Login as WebLogic Administrator to **OIG** enterprise manager (/em)
2. Click on the WebLogic Domain →Security → Credentials



3. Expand map **oracler.wsm.security**
4. Check content of the **keystore-csf-key** (owsm) and **sing-csf-key** (xel).



Edit Key

Select Map oracle.wsm.security

Key keystore-csf-key

Type Password

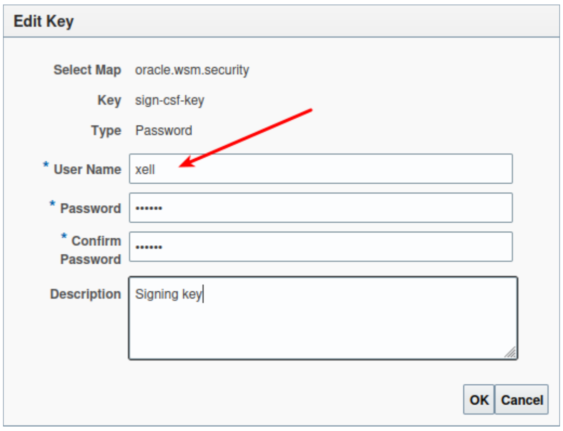
* User Name owsm

* Password ••••••

* Confirm Password ••••••

Description Keystore key

OK Cancel



Edit Key

Select Map oracle.wsm.security

Key sign-csf-key

Type Password

* User Name xell

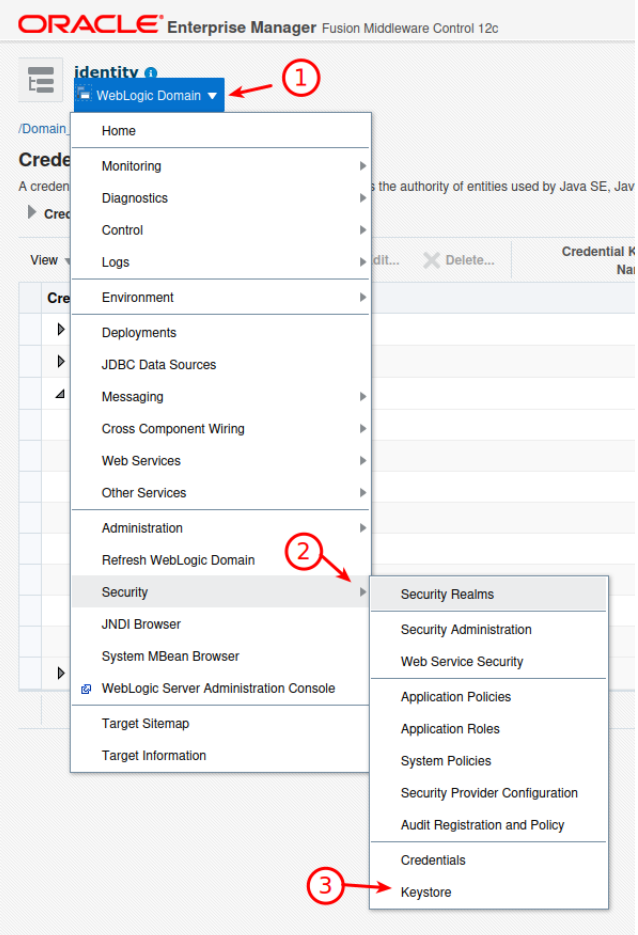
* Password ••••••

* Confirm Password ••••••

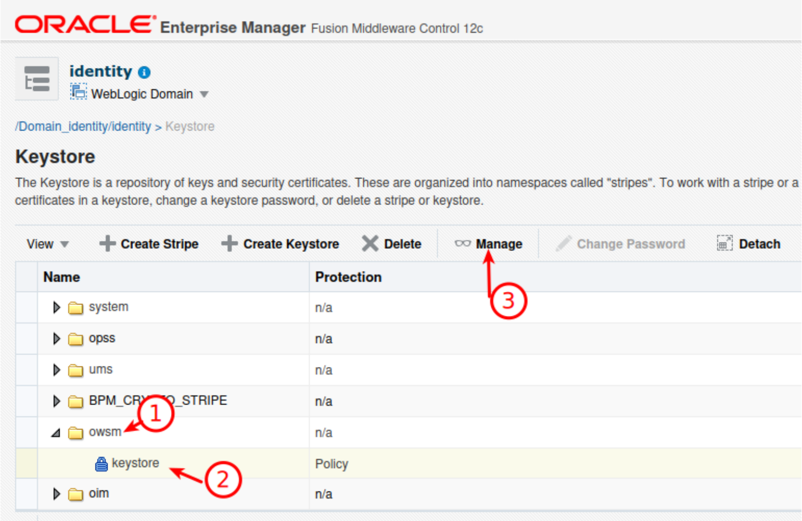
Description Signing key

OK Cancel

5. User Name from **keystore-csf-key** represend stripe name and User Name from **sign-csf-key** represent alias in the keystore.
6. Click on the WebLogic Domain → Security → Keystore



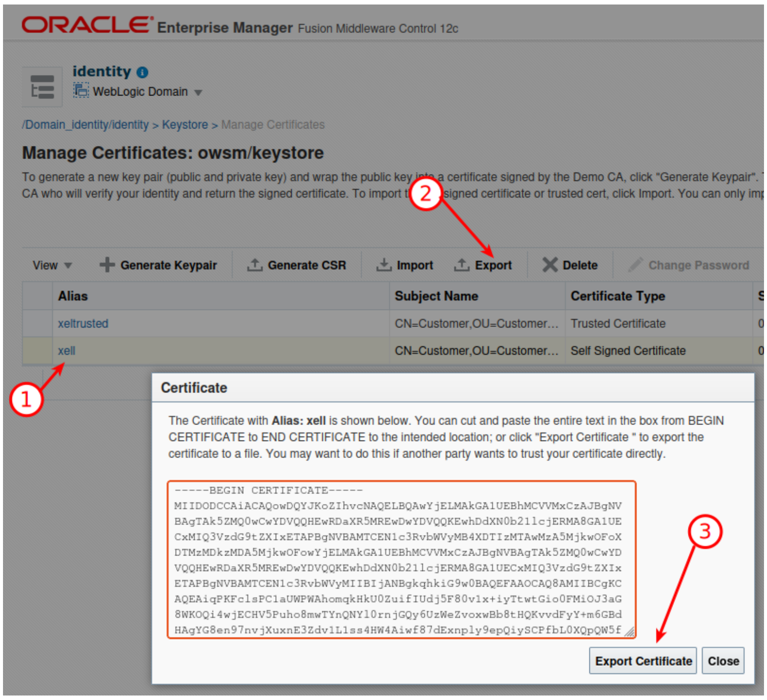
7. Expand owsm, select keystore and click on the Manage button



The Keystore is a repository of keys and security certificates. These are organized into namespaces called "stripes". To work with a stripe or a certificates in a keystore, change a keystore password, or delete a stripe or keystore.

Name	Protection
system	n/a
opss	n/a
ums	n/a
BPM_CRYPTO_STRIPE	n/a
owsm	n/a
keystore	Policy
oim	n/a

8. Export certificate from owsm stripe where alias name is xel



Manage Certificates: owsm/keystore

To generate a new key pair (public and private key) and wrap the public key into a certificate signed by the Demo CA, click "Generate Keypair". T
CA who will verify your identity and return the signed certificate. To import t signed certificate or trusted cert, click Import. You can only imp

Alias	Subject Name	Certificate Type	S
xeltrusted	CN=Customer,OU=Customer…	Trusted Certificate	0
xell	CN=Customer,OU=Customer…	Self Signed Certificate	0

Certificate

The Certificate with **Alias: xell** is shown below. You can cut and paste the entire text in the box from BEGIN CERTIFICATE to END CERTIFICATE to the intended location; or click "Export Certificate " to export the certificate to a file. You may want to do this if another party wants to trust your certificate directly.

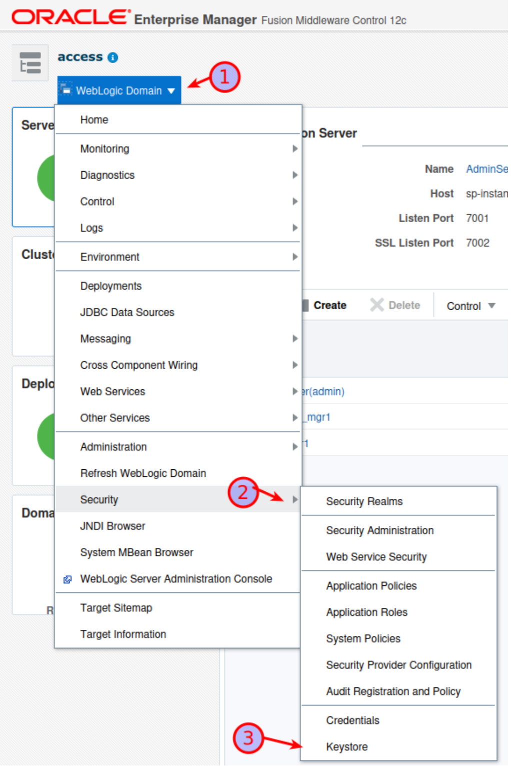
```
-----BEGIN CERTIFICATE-----
MIIDODCCAiACAQowDQYJKoZIhvcNAQELBQAwYjELMAkGA1UEBhMCVVMxCzAJBgNV
BAgTAk5ZMQ0wCwYDVQQHEwRDaXR5MREwDwYDVQQKEwhDdXN0b21lcjERMA8GA1UE
CxMIQ3VzdG9tZXIxETAPBgNVBAMTCEN1c3RvbWVyMB4XDTIzMTAwMzA5MjkwOFoX
DTMzMDkzMDA5MjkwOFowYjELMAkGA1UEBhMCVVMxCzAJBgNVBAgTAk5ZMQ0wCwYD
VQQHEwRDaXR5MREwDwYDVQQKEwhDdXN0b21lcjERMA8GA1UECxMIQ3VzdG9tZXIx
ETAPBgNVBAMTCEN1c3RvbWVyMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKC
AQEAiqPKFclsPC1aUWPWAhomqkHkU0ZuifIUdj5F80v1x+iyTtwtGio0FMiOJ3aG
8WKOQi4wjECHV5Puho8mwTYnQNYl0rnjGQy6UzWeZvoxwBb8tHQKvvdFyY+m6GBd
HAgYG8en97nvjXuxnE3Zdv1L1ss4HW4Aiwf87dExnply9epQiySCPfbL0XQpQW5f
```

9. Export certificate to file or copy it as text to clipboard.

2.3 Import certificate used by UMS server to OAM keystore

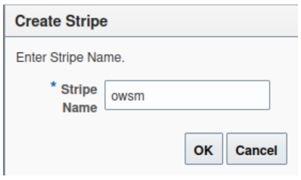
1. Login as WebLogic Administrator to **OAM** enterprise manager (/em)

2. Click on the WebLogic Domain → Security → Keystore



Name AdminSe
Host sp-instan
Listen Port 7001
SSL Listen Port 7002

3. Create Stripe with name **owsm** (Click on the **+Create Stripe** button)

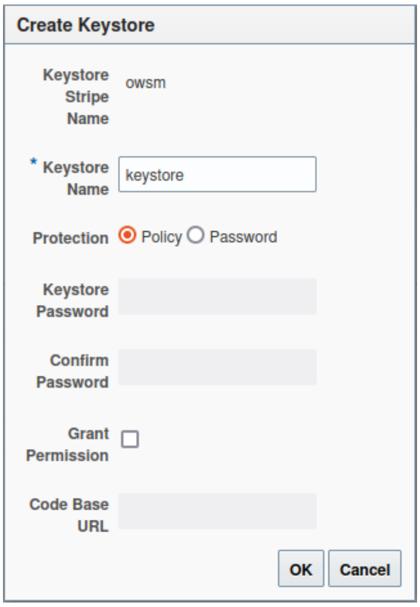


Create Stripe

Enter Stripe Name.

* Stripe Name: owsm

4. Create a keystore with name **keystore** (Click on the **+ Create Keystore**)



Create Keystore

Keystore Stripe Name: owsm

* Keystore Name: keystore

Protection: ● Policy ○ Password

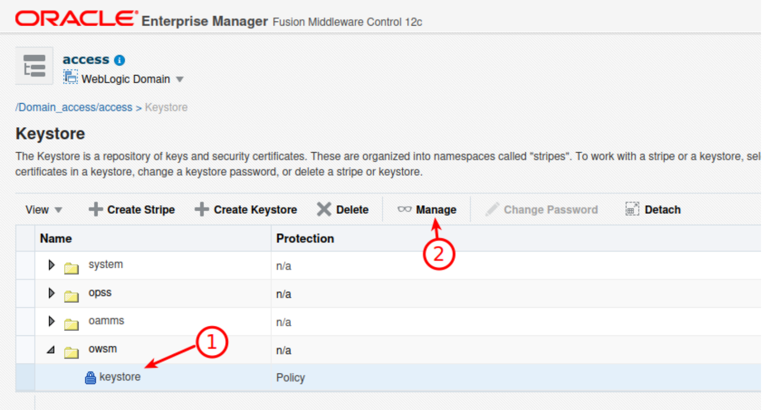
Keystore Password:

Confirm Password:

Grant Permission: □

Code Base URL:

5. Select keystore under owsm stripe and click on the Manage



ORACLE Enterprise Manager Fusion Middleware Control 12c

access
WebLogic Domain

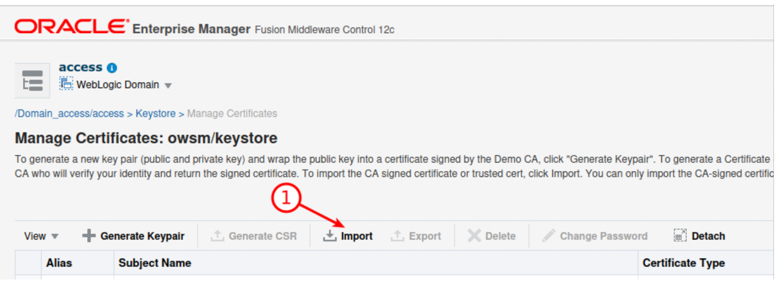
/Domain_access/access > Keystore

Keystore

The Keystore is a repository of keys and security certificates. These are organized into namespaces called "stripes". To work with a stripe or a keystore, sel
certificates in a keystore, change a keystore password, or delete a stripe or keystore.

Name	Protection
system	n/a
opss	n/a
oamms	n/a
owsm	n/a
keystore	Policy

6. Import certificate from OIG server



ORACLE Enterprise Manager Fusion Middleware Control 12c

access
WebLogic Domain

/Domain_access/access > Keystore > Manage Certificates

Manage Certificates: owsm/keystore

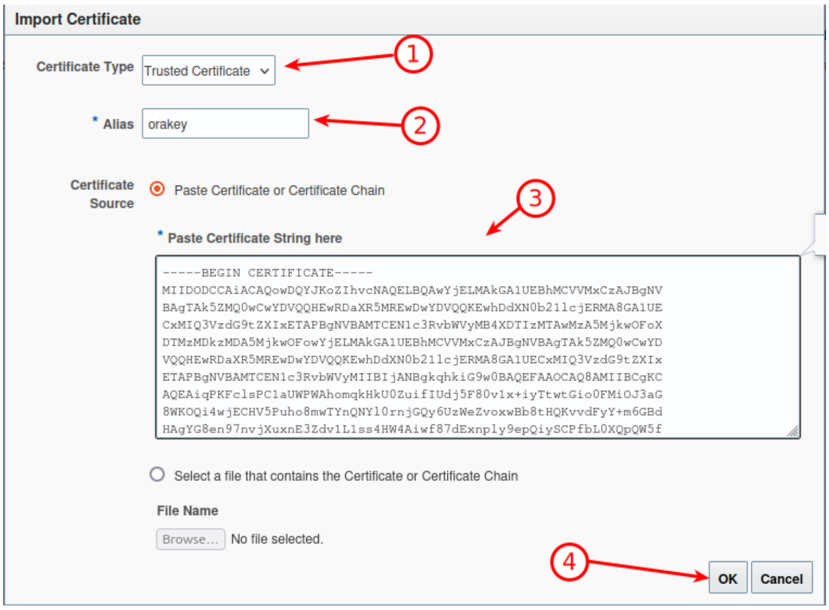
To generate a new key pair (public and private key) and wrap the public key into a certificate signed by the Demo CA, click "Generate Keypair". To generate a Certificate
CA who will verify your identity and return the signed certificate. To import the CA signed certificate or trusted cert, click Import. You can only import the CA-signed certific

Alias	Subject Name	Certificate Type

7. OIG certificate can be imported from file or as text in PEM format

   Cerificate Type set to **Trusted Certificate**.

   Alias name must be **orakey**



Import Certificate

Certificate Type: Trusted Certificate

* Alias: orakey

Certificate Source: ● Paste Certificate or Certificate Chain

* Paste Certificate String here

```
-----BEGIN CERTIFICATE-----
MIIDODCCAiACAQowDQYJKoZIhvcNAQELBQAwYjELMAkGA1UEBhMCVVMxCzAJBgNV
BAgTAk5ZMQ0wCwYDVQQHEwRDaXR5MREwDwYDVQQKEwhDdXN0b21lcjERMA8GA1UE
CxMIQ3VzdG9tZXIxETAPBgNVBAMTCEN1c3RvbWVyMB4XDTIzMTAwMzA5MjkwOFoX
DTMzMDkzMDA5MjkwOFowYjELMAkGA1UEBhMCVVMxCzAJBgNVBAgTAk5ZMQ0wCwYD
VQQHEwRDaXR5MREwDwYDVQQKEwhDdXN0b21lcjERMA8GA1UECxMIQ3VzdG9tZXIx
ETAPBgNVBAMTCEN1c3RvbWVyMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKC
AQEAiqPKFclsPC1aUWPWAhomqkHkU0ZuifIUdj5F80v1x+iyTtwtGio0FMiOJ3aG
8WKOQi4wjECHV5Puho8mwTYnQNYl0rnjGQy6UzWeZvoxwBb8tHQKvvdFyY+m6GBd
HAgYG8en97nvjXuxnE3Zdv1L1ss4HW4Aiwf87dExnply9epQiySCPfbL0XQpQW5f
```

○ Select a file that contains the Certificate or Certificate Chain

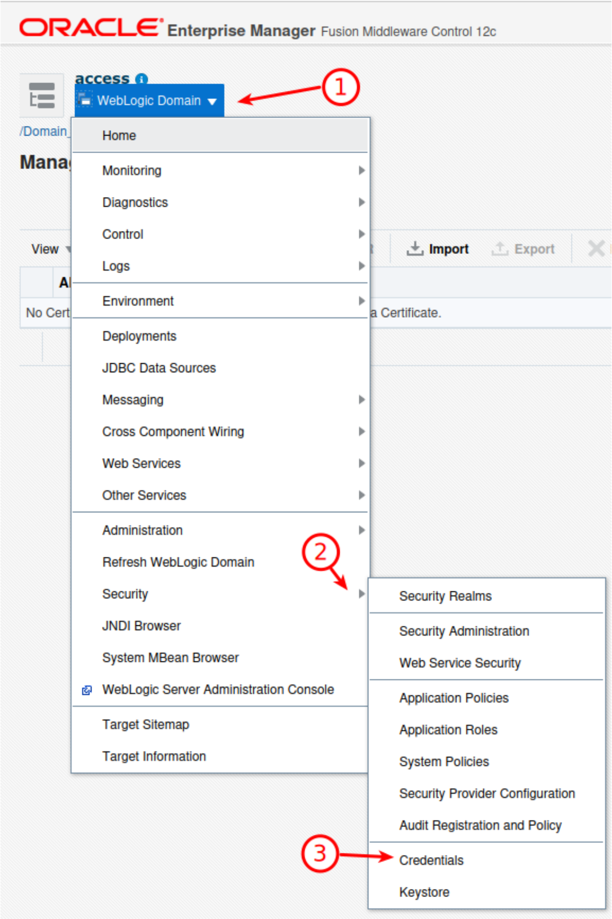
File Name

Browse... No file selected.

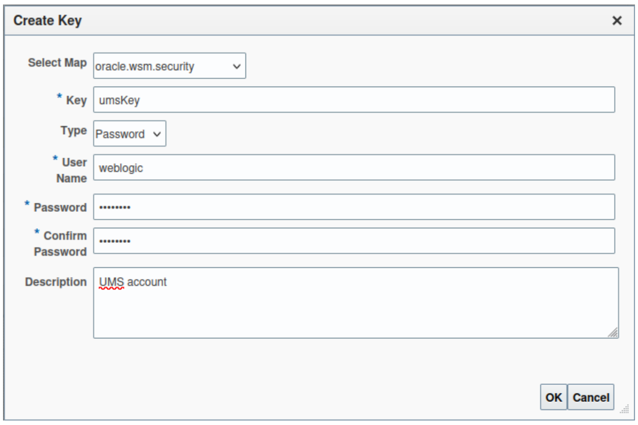
2.4 Create CSF key under oracler.wsm.security

1. Login as WebLogic Administrator to **OAM** enterprise manager (/em)

2. Click on the WebLogic Domain → Security → Keystore



3. Expand map **oracle.wsm.security**.
4. Click on the **+Create Key**. Create Key as **usmKey**. In the User Name nad password provide weblogic username and password.



Create Key ×

Select Map	oracle.wsm.security
* Key	umsKey
Type	Password
* User Name	weblogic
* Password	•••••••••
* Confirm Password	•••••••••
Description	UMS account

NOTE: umsKey from map OAM_CONFIG can be removed, it is not used anymore

3 Redeploy OAM OTPAuthenticationPlugin

OAM plugin OTPAuthenticationPlugin needs to be redeployed on OAM server. Location of this plugin is:

/deployment/oam/0101 authenticationPlugin/lib/OTPAuthenticationPlugin.jar

For more information how to redeploy OAM plugins check oracle documentation:

https://docs.oracle.com/cd/E52734_01/oam/AIAAG/GUID-A22A0F9A-618A-4183-ADD0-2E98C84458FA.htm#AIAAG8130

NOTE: OAM Plugin can’t be redeployed once is used by OAM authentication module. OAM Plugin must be removed from all authentication modules and then can be redeployed.

3.1 Configuration OTPAuthenticationPlugin

In the latest version of the OTPAuthenticationPlugin is a new plugin parameter **UMS_IS_WSS**. Defaule value of this parameter is **false**, in this case basic authentication is used for authentication with UMS service on OIG.

When **UMS_IS_WSS** is set to the **true** OWSM client policy „**oracle/wss11_username_token_with_message_protection_client_policy**“ is used when sending email via UMS service on OIG.