# **Practical Exercise: WSO2 Identity Server as the Key Manager**

Training Objective

In this exercise, the WSO2 Identity Server is used as the Key Manager for the API Manager cluster.

Business Scenario

PizzaShack wants to integrate the WSO2 Identity Server with the APIM using it as the Key Manager to control authentication and authorization.

High-Level Steps

* Configuring the Identity Server as Key Manager
* Configuring the API Manager

Detailed Instructions

**Configuring the Identity Server as Key Manager**

1. Download and install the WSO2 Identity server 6.1.0 from [here](https://wso2.com/identity-and-access-management/#)  
   If you downloaded the archive, extract it. <IS\_HOME> refers to the root folder of the extracted WSO2 IS.
2. Use a port offset of 1 for the WSO2 IS by editing the offset configuration found in <IS\_HOME>/repository/conf/deployment.toml.

| [server]  offset=1 |
| --- |

1. Install, setup and configure WSO2\_AM\_DB and WSO2\_SHARED\_DB databases as illustrated in [Changing the Default Databases](https://apim.docs.wso2.com/en/4.2.0/install-and-setup/setup/setting-up-databases/changing-default-databases/changing-to-mysql/). This particular guide provides you with all the steps on how to install the database, set up database users, create tables using relevant scripts, and apply the drivers which are compatible with the database type.
2. Edit the <IS\_HOME>/repository/conf/deployment.toml file to configure databases relevant to API Manager.

| [database.shared\_db]  type = "mysql"  url = "jdbc:mysql://localhost:3306/wso2shared\_db?useSSL=false"  username = "root"  password = "root" |
| --- |

1. Add the following configurations to <IS\_HOME>/repository/conf/deployment.toml file to configure the Traffic Manager endpoints.

| [[event\_listener]]  id = "token\_revocation"  type = "org.wso2.carbon.identity.core.handler.AbstractIdentityHandler"  name = "org.wso2.is.notification.ApimOauthEventInterceptor"  order = 1  [[resource.access\_control]]  context = "(.)/keymanager-operations/user-info/claims(.)"  secure = true  http\_method = "GET"  permissions = "/permission/admin/manage/identity/usermgt/list"  scopes = "internal\_user\_mgt\_list"  [[resource.access\_control]]  context = "(.\*)/keymanager-operations/user-info/claims/generate"  secure = true  http\_method = "POST"  permissions = "/permission/admin/manage/identity/usermgt/list"  scopes = "internal\_user\_mgt\_list"  [[resource.access\_control]]  context = "(.\*)/keymanager-operations/dcr/register"  secure = true  http\_method = "POST"  permissions = "/permission/admin/manage/identity/applicationmgt/create"  scopes = "internal\_application\_mgt\_create"  [[resource.access\_control]]  context = "(.\*)/keymanager-operations/dcr/register(.\*)"  secure = true  http\_method = "GET"  permissions = "/permission/admin/manage/identity/applicationmgt/view"  scopes = "internal\_application\_mgt\_view"  [[resource.access\_control]]  context = "(.\*)/keymanager-operations/dcr/register(.\*)"  secure = true  http\_method = "DELETE"  permissions = "/permission/admin/manage/identity/applicationmgt/delete"  scopes = "internal\_application\_mgt\_delete"  [[resource.access\_control]]  context = "(.\*)/keymanager-operations/dcr/register(.\*)"  secure = true  http\_method = "PUT"  permissions = "/permission/admin/manage/identity/applicationmgt/update"  scopes = "internal\_application\_mgt\_update"  [[resource.access\_control]]  context = "(.)/keymanager-operations/dcr/register(.)"  secure = true  http\_method = "POST"  permissions = "/permission/admin/manage/identity/applicationmgt/update"  scopes = "internal\_application\_mgt\_update"  [tenant\_context.rewrite]  custom\_webapps = ["/keymanager-operations/"] |
| --- |

1. Configure the event listener endpoint to publish controller events to the Traffic Manager.

| [event\_listener.properties]  notification\_endpoint = "https://<tm.wso2.com>:9443/internal/data/v1/notify"  username = "${admin.username}"  password = "${admin.password}"  'header.X-WSO2-KEY-MANAGER' = "WSO2-IS" |
| --- |

1. Change the default encryption type and remove the keystore.primary configuration.

| [keystore]  userstore\_password\_encryption = "InternalKeyStore"  [system.parameter]  "org.wso2.CipherTransformation" = "RSA/ECB/OAEPwithSHA1andMGF1Padding"  [encryption]  internal\_crypto\_provider = "org.wso2.carbon.crypto.provider.KeyStoreBasedInternalCryptoProvider" |
| --- |

1. Download the [WSO2 IS Connector](https://repo1.maven.org/maven2/org/wso2/km/ext/wso2is/distribution/1.6.8/distribution-1.6.8.zip).
2. Extract the distribution and copy the following JAR files to the <IS\_HOME>/repository/components/dropins directory.

* wso2is.key.manager.core-1.6.8
* wso2is.notification.event.handlers\_1.6.8

1. Add keymanager-operations.war which is in the <wso2is-extensions-1.6.8>/webapps directory to the <IS\_HOME>/repository/deployment/server/webapps directory.
2. Start WSO2 Identity Server.  
   cd <IS\_HOME>/bin/

sh wso2server.sh

**Configuring APIM with IS**

1. Edit the <APIM\_HOME>/repository/conf/deployment.toml file to configure the shared database with IS.

| [database.apim\_db]  type = "mysql"  url = "jdbc:mysql://localhost:3306/wso2am\_db?useSSL=false"  username = "root"  password = "root"  [database.shared\_db]  type = "mysql"  url = "jdbc:mysql://localhost:3306/wso2shared\_db?useSSL=false"  username = "root"  password = "root" |
| --- |

1. Import the Key Manager's public certificate to WSO2 API-M's client-truststore.jks.

Export the public key using the following command from <IS\_HOME>/repository/resources/security/wso2carbon.jks.

keytool -export -alias wso2carbon -keystore wso2carbon.jks -file is\_km\_public.pem

Import the public key using the following command to <APIM\_HOME>/repository/resources/security/wso2carbon.jks.

keytool -import -alias wso2carbonis -file is\_km\_public.pem -keystore client-truststore.jks -storepass wso2carbon

1. Add the following configuration to <APIM\_HOME>/repository/conf/deployment.toml file in order to share the IS LDAP userstore with APIM. Note the port offset in the connection URL.

| #[user\_store]  #type = "database\_unique\_id"  [user\_store]  type = "read\_write\_ldap\_unique\_id"  connection\_url = "ldap://localhost:10390"  connection\_name = "uid=admin,ou=system"  connection\_password = "admin"  base\_dn = "dc=wso2,dc=org" |
| --- |

1. Add below configuration in <APIM\_HOME>/repository/conf/deployment.toml

| [apim.key\_manager]  service\_url = "https://localhost:9444/services/"  type = "WSO2-IS" |
| --- |

1. Start the API Manager Server.

cd <APIM\_HOME>/bin/

sh api-manager.sh

All above instructions are explained in details in <https://apim.docs.wso2.com/en/4.2.0/install-and-setup/setup/distributed-deployment/configuring-wso2-identity-server-as-a-key-manager/>

Expected Outcome

WSO2 Identity Server will act as the primary Key Manager for the WSO2 API Manager.