Oracle® Tuxedo System and Applications Monitor Plus

Configuration Guide

Release 22c
F96525-04
July 2026

ORACLE

Oracle Tuxedo System and Applications Monitor Plus Configuration Guide, Release 22c

F96525-04

Primary Author: Priya Pathak

Contributing Authors: Tulika Das

Contributors: Maggie Li

Contents

3 Configuring OIDC for Oracle TSAM Plus Manager with Keycloak and WebLogic

Preface

This guide describes how to configure Oracle Tuxedo System and Applications Monitor Plus (Oracle TSAM Plus). It includes configuration procedures for Oracle TSAM Plus Agent and Oracle TSAM Plus Manager, including manager security settings for authentication and authorization.

This guide also describes how to configure OpenID Connect (OIDC) for Oracle TSAM Plus Manager with Keycloak and WebLogic Server. It includes procedures for preparing the OIDC provider, capturing required configuration values, enabling or disabling OIDC support, and verifying authentication and role-based access.

1

Configuring Oracle TSAM Plus Agent

This chapter contains the following topics:

1.1 Oracle TSAM Plus Agent Overview

The Oracle TSAM Plus Agent handles all Tuxedo-side back-end logic. It includes the following sub-components:

- Standalone TSAM Plus Agent components working in conjunction with the Oracle TSAM Plus Manager:
  - Oracle TSAM Plus Framework: The framework is the data collection engine. It is an independent layer working between Tuxedo infrastructure and other TSAM Plus components. This module is responsible for runtime metrics collection, alert evaluation and monitoring policy enforcement.
  - Oracle TSAM Plus Plug-in: An extensible mechanism invoked by the Oracle TSAM Plus Framework. The Oracle TSAM Plus Agent provides default plug-ins to send data to the LMS (Local Monitor Server), and then to the Oracle TSAM Plus Manager. The plug-in allows custom plug-in to be hooked to intercept the metrics. The default plug-in communicates with the LMS through shared memory. The application is not blocked at the metrics collection point.
    You can develop your own plug-ins for additional data processing. A customized plug-in can be linked to an existing plug-in chain, or replace the default plug-in.
  - Local Monitor Server (LMS): The LMS is an Oracle Tuxedo system server. The Oracle TSAM Plus default plug-in sends data to the LMS. The LMS then passes the data to the Oracle TSAM Plus Manager in over HTTP protocol. LMS is required on each Tuxedo machine if the node needs to be monitored.
  - **accrpt**: A utility to analyze accounting and chargeback information generated by `-a` option in `servopts(5)`.
- JMX agent, which works in conjunction with the Enterprise Manager for Oracle Tuxedo to enable you to monitor and manage Oracle Tuxedo applications through the JMX interface and furthermore, through the Oracle Enterprise Manager Cloud Control.
- Oracle Tuxedo Scripting tool, a command-line scripting environment that you can use to manage and monitor Tuxedo domains.

1.2 Configuring Standalone TSAM Plus Agent

1.2.1 Prerequisites

To effectively and correctly use the Oracle TSAM Plus Agent, note the following prerequisites:

- TSAM Agent must be enabled.
- You can enable it during Tuxedo installation, or after installation by running `$TUXDIR/bin/regtsam.sh`.

- The system clocks for all monitored Tuxedo machines and the Oracle TSAM Plus Manager are synchronized. A uniform time server is recommended.
- Set each Tuxedo domain to a unique `DOMAINID` in the `UBBCONFIG` file.

1.2.2 Adding LMS to UBBCONFIG

Local Monitor Server (LMS) performs the following tasks:

- Acts as a data proxy server between Oracle TSAM Plus agent framework and Oracle TSAM Plus Manager
- Accepts policy and alert configuration requests from Oracle TSAM Plus Manager and applies them to the Tuxedo domain
- Sends Tuxedo domain configuration to Oracle TSAM Plus Manager

For more information, see LMS in the Oracle TSAM Plus Reference Guide

For more information on Configuring TLS Certificate on Oracle TSAM Plus Agent, see Deployment Guide

To properly deploy the Oracle TSAM Plus Agent, you must add the LMS to each Oracle Tuxedo machine section in the UBBCONFIG file. Following is an example:

LMS Added to UBBCONFIG File

```
...

*MACHINES

MACHINEA

...

*GROUPS

...

LMSGRP LMID=MACHINEA

...

*SERVERS

LMS SRVGRP=LMSGRP SRVID=1 CLOPT="-A -l tsamweb.abc.com:8080/tsam"

...
```

The `-l` option specifies the Oracle TSAM Plus Data Server address which is configured in the Oracle TSAM Plus Manager. As of Tuxedo 22.1.0.0.0, the https protocol is supported by the **-l** option. Here is an example,

```
CLOPT="-A – -l tsamweb.abc.com:8080/tsam"
```

For more information, see the TSAM Plus Server, Command, and API Reference.

Beginning with Tuxedo 22.1.0.0.0, the Oracle TSAM Plus Data Server and Oracle TSAM Plus Manager Console use different port numbers. Refer to the TSAM Plus Deployment Guide for details.

> **Note**
>
> - LMS can also be added to a running Oracle Tuxedo application using TMIB.
> - For https protocol, please refer to WebLogic Server Deployment in the TSAM Plus Deployment Guide.

1.2.2.1 Adding LMS Configuration Automatically

TSAM Plus Agent provides a management tool, `tsamadmin`, to add the LMS configurations in the `UBBCONFIG` file automatically. The command format is:

```
tsamadmin autoconfig(ac){-s|--static} {-H|--hostname} hostname:port
```

For example, suppose you run the command:

```
tsamadmin autoconfig -s -H tsamhost.com:7001
```

A new `UBBCONFIG` file is created and the LMS is configured in the new-created group (Group1), as shown below:

```
GROUP1 LMID=SITE1 GRPNO=1

LMS SRVGRP=GROUP1 SRVID=90 CLOPT="-A -- -l tsamhost.com:7001/tsam "
```

For more information about `tsamadmin`, refer to TSAM Plus Management Tool.

1.2.3 Turning Oracle TSAM Plus On and Off

You can use a `tmadmin` command to turn on or turn off Oracle TSAM Plus. The command format is:

```
changemonitor (chmo) [-m lmid] on|off
```

The `-m` parameter specifies the logic machine name where the Oracle TSAM Plus collection is disabled. Without this option, monitoring on all machines is disabled. By default, monitoring is turned on. If monitoring is turned off, all data collection is stopped even if there is a monitoring policy defined.

1.2.4 Configurations for Oracle Tuxedo ART for CICS and Batch Monitoring

To monitor Oracle Tuxedo Application Runtime for CICS, an additional configuration file (`Region-Group.mapping`)is required. You need to put the file in the directory specified by the `KIXCONFIG` environment variable. For more information, see Overview of CICS Runtime

> **Note**
>
> The `KIXCONFIG environment` variable is required for all ART applications.

The following is an example of Region-Group.mapping File Format:

Region-Group.mapping File Format Example

```
[region]
```

```
name= REG1

tuxgroups=APPGRP1,APPGRP2

resources_group=resgroup1,resgroup2


[region]

name= REG2

tuxgroups=APPGRP3,APPGRP4

resources_group=resgroup3,resgroup4
```

Each region has a section in this file. The CICS region is called "name". The `tuxgroups` parameter is followed by the Oracle Tuxedo group name. The `resources_group` parameter is the CICS resource group in this region.

For more information, see Oracle Tuxedo Application Runtime for CICS Reference.

> **Note**
>
> For Oracle Tuxedo Application Runtime for CICS running on Linux, the ARTMON server must be configured in order to enable TSAM Plus monitoring.

If you need to monitor Oracle Tuxedo Application Runtime for Batch ARTJES component, set the `JESMONITOR` environment variable to `yes` before you start the LMS server.

1.2.5 Configurations for JES Security Mode

To integrate TSAM Plus with JES security mode, you need to configure the `UBBCONFIG` file and create TSAM Plus configuration file for TuxJES (`tsamconfig`) and TSAM Plus user mapping file.

1.2.5.1 Configuring UBBCONFIG

In the Tuxedo `UBBCONFIG` file, configure the following:

1. Place the LMS server configurations after lines of the `ARTJESADM` server
2. Add the option `-j <TSAM configuration file for TuxJES>` in LMS CLOPT.

Following is an example of UBCONFIG file:

UBBCONFIG File Example

```
ARTJESADM SRVGRP =ARTGRP SRVID = 1 MIN=1 MAX=1

CLOPT = "-A -- -i jesconfig"

ARTJESCONV SRVGRP =ARTGRP SRVID = 20 MIN=1 MAX=1

CLOPT = "-A --"

ARTJESINITIATOR SRVGRP =ARTGRP SRVID =30

CLOPT = "-A -- -n 20 -d"

ARTJESPURGE SRVGRP =ARTGRP SRVID = 100
```

```
CLOPT = "-A --"

AUTHSVR SRVGRP =ARTGRP SRVID = 200

CLOPT = "-A"

LMS SRVGRP=LMSGRP SRVID=101

CLOPT="-A -- -l <hostname>:<port>/tsam -j tsamconfig"
```

1.2.5.2 TSAM Plus Configuration File for TuxJES

The following lists the key words for the configuration file

Key Words	Description
JES_SYSLOG_SEND	Specify whether to send JES syslog to TSAM Plus Manager. • 0: Do not send syslog (default setting). If 0 is set, SYSLOG is not shown in TSAM Plus manager console. • 1: Send syslog
TSAM_USER_MAPPING_FILE	Specify the path of the TSAM Plus user mapping file, which is used to map the TSAM Plus user to the Tuxedo user and corresponding JES profile.

Following is an example of Configuration File for TuxJES:

Configuration File for TuxJES

```
JES_SYSLOG_SEND=1

TSAM_USER_MAPPING_FILE=/home/artbatch/simpjob/tsam_user_profile
```

1.2.5.3 TSAM Plus User Mapping File

This file is used to map the TSAM Plus user to the Tuxedo user and corresponding JES profile.

The file format is:

```
<TSAM user> <Tuxedo user> <JES profile pathname>
```

TSAM Plus User Mapping File Example

```
artbatch tpartbatch /home/artbatch/simpjob/tuxArtProfile

admin tproot /home/artbatch/simpjob/tuxRootProfile
```

> **Note**
>
> The JES profile owner must be the OS user mapped from TSAM Plus user.

1.2.5.4 Running a Sanity Check

You can run a sanity check using the `tsamadmin` command to check if the configurations are properly made and TSAM Plus Agent can communicate with the Manager. The command format is:

```
tsamadmin managercheck(mc)[-s]
```

It checks the following configurations in sequence:

- TSAM Plus agent plug-in is correctly registered in Tuxedo. If the plug-in is not registered yet, `tsamadmin` helps users to register the plug-in.
- LMS server is configured in UBBCONFIG.
- Whether the LMS CLOPT format is valid.
- The TSAM Plus Manager host and port configured in LMS CLOPT can be reached.

If any step fails, the check is terminated and an error report is shown.

For more information about `tsamadmin`, refer to TSAM Plus Management Tool.

1.3 Configuring JMX Agent

1.3.1 Starting the tlisten Process

Before you can use TSAM Plus to monitor the Tuxedo domain targets, you must start the `tlisten` process before starting the Tuxedo domain so that Tuxedo Domain MBeans can register with the JMX agent embedded in the `tlisten` process. For MP domains in particular, you should start `tlisten` for every machine.

The following JDK versions are required to start the embedded JMX agent:

- For AIX: JDK 8 SR4 or later
- For other platforms: JDK 7u85 or later, or 8u60 or later

Before starting `tlisten`, you must set the `tlisten` environment variable `SHLIB_PATH/LIBPATH/LD_LIBRARY_PATH` and include the `libjvm` library path. For windows platforms, you only need to set `JAVA_HOME`. For HP platforms, you need to set `LD_PRELOAD` to include the `libjvm.so` directory.

Environment Variable Setting on Different Platforms

For Linux 64-bit platforms:

```
LD_LIBRARY_PATH=$TUXDIR/lib:$JAVA_HOME/jre/lib/amd64/server:$LD_LIBRARY_PATH;

export LD_LIBRARY_PATH;
```

For AIX 64-bit platforms:

```
LIBPATH=$TUXDIR/lib:$JAVA_HOME/jre/lib/ppc64:${JAVA_HOME}/jre/lib/ppc64/
default:$LIBPATH;

export LIBPATH;
```

For HP 64-bit platforms:

```
LD_LIBRARY_PATH=$TUXDIR/lib:$JAVA_HOME/jre/lib/IA64W/server:$LD_LIBRARY_PATH;

export LD_LIBRARY_PATH;

LD_PRELOAD=$JAVA_HOME/jre/lib/IA64W/server/libjvm.so;

export LD_PRELOAD;
```

> **Note**
>
> `LD_PRELOAD` is only used for `tlisten` to start embedded JMX agent. It should not be set when building Tuxedo applications.

To start `tlisten`, use the following command:

```
tlisten -j rmi://<host>:<rmiport> -l //<host>:<tlistenport>
```

> **Note**
>
> Make sure that the host and port specified by the `-l` option are the same as the `NLSADDR` value specified in the `UBBCONFIG` file.

When the `tlisten` process is started correctly, you can view the message **RMI connector server successfully started** and **Started the embedded JMX agent successfully** in ULOG.

The following functions are added to the `tlisten` process:

- A JMX agent is embedded, and creates a JMX domain for every Tuxedo Domain (SHM mode), or Tuxedo Machine (MP mode), connecting to it. Every MBean in the JMX domain corresponds to a Tuxedo target.
- `tlisten` acts as the Tuxedo-side monitoring and management agent . It receives monitoring and management requests from Enterprise Manager and dispatches these requests to corresponding Tuxedo services.
- `tlisten` creates a Tuxedo context for each JMX connection. If a monitored Tuxedo domain enables authentication and authorization, `tlisten` provides the credentials attained from Enterprise Repository when it attaches a Tuxedo domain.
- If the JMX fetchlet in EM agent sends a metrics request to `tlisten`, `tlisten`:
  - Transforms the request message to an FML32 buffer and forwards the request to the MIB service of the corresponding Tuxedo domain,
  - receives the metrics conveyed in the response buffer and then returns metrics to Enterprise Repository agent. The connection between the JMX fetchlet and the `tlisten` agent are reused across multiple metrics requests for the same Enterprise Repository user.
- `tlisten` also forwards job requests from Enterprise Repository agent to MIB service. Enterprise Repository agent creates a new JMX connection for every job request, and releases the connection after the job finishes. Accordingly, `tlisten` creates a Tuxedo context for each job request.

To start tlisten with SSL enabled, use the following command:

```
tlisten -j rmi://<host>:<rmiport> -l //<host>:<tlistenport> -S -C /path/to/
keystore.jks -P PASSWD_VAR
```

For more information about additional `tlisten` options for JMX monitoring, see TSAM Plus Server, Command, and API Reference.

1.3.2 Configuring the UBBCONFIG File

1.3.2.1 Adding the NETWORK Section

To monitor and manage the Tuxedo domain monitoring targets, you must register the targets in the `tlisten` process by adding the `*NETWORK` section and configuring the `NLSADDR` parameters in the `UBBCONFIG` file for the Tuxedo domain in SHM mode.

1.3.2.2 Adding EXT_MON in the RESOURCES Section

Collection and calculation of certain metrics (such as Service Metrics and IPC Queue Metrics in MIB), consumes CPU time and potentially impacts Oracle Tuxedo performance. Oracle Tuxedo uses the `EXT_MON OPTIONS` parameter in the `UBBCONFIG` file `*RESOURCES` section to allow MIB performance sensitive metrics collection.

If the indicator is specified, all metrics listed in the Tuxedo Targets section are collected in MIB; otherwise, if the indicator is not specified, the following metrics are not collected by Oracle Tuxedo:

- Tuxedo Server Service metrics
- Tuxedo Server IPC Queue metrics
- Tuxedo Bridge IPC Queue metrics

The metrics collection policy changes immediately once you modify this parameter setting.

An SHM UBBCONFIG Sample Supporting Enterprise Manager Monitoring

```
*RESOURCES

IPCKEY 65831

DOMAINID shm

MASTER L1

MODEL SHM

MAXACCESSERS 100

MAXSERVERS 100

OPTIONS EXT_MON

*MACHINES

"<hostname>" LMID = L1

APPDIR = "/testarea/tux/test/jmx/servers"

TUXCONFIG = "/testarea/tux/test/jmx/servers/tuxconfig"

TUXDIR = "/testarea/tux/oracle/tuxedo12c"

*GROUPS

ATMIGRP1 LMID = L1

GRPNO = 10
```

```
*SERVERS

SvrUpdate SRVGRP = ATMIGRP1

SRVID = 100

*SERVICES

*NETWORK

"L1"

NLSADDR="<hostname>:16998"
```

2

Configuring Oracle TSAM Plus Manager

This chapter describes configuration tasks made on Oracle TSAM Plus Manager after you have configured standalone TSAM Plus Agent as described in the first chapter.

This chapter contains the following topics:

2.1 Overview

The Oracle TSAM Plus Manager is the data manipulation and representation component of Oracle TSAM Plus. It is a J2EE application.

The Oracle TSAM Plus Manager provides the following functionality: Communicates with the Oracle TSAM Plus Agent for performance metrics, configuration information and other utility messages. Provides a Web console for Oracle TSAM Plus administration, monitored data presentation and alerts management.

2.2 Configuring Oracle TSAM Plus Data Server

The Oracle TSAM Plus Data Server is the communication interface to Oracle TSAM Plus. It accepts requests from LMS and metrics query requests from a web browser. For each LMS, the URL of the data server must be configured correctly. The format is as follows:

```
CLOPT="-A -- -l host:port/tsam"
```

- the host where the web application is deployed
- `port` is the port number of the Java server.
- `tsam` is the Oracle TSAM Plus URL.

> **Note**
>
> From an HTTP perspective, the Oracle TSAM Plus Agent LMS is the HTTP client, and the Oracle TSAM Plus Manager is the HTTP server. If a firewall is deployed between the Oracle TSAM Plus Manager and Tuxedo applications, the firewall must allow the LMS to issue HTTP requests to the Oracle TSAM Plus Manager.

2.3 Configuring Oracle TSAM Plus Manager

Oracle TSAM Plus Manager provides some global parameters for tuning purposes. They are available at the Data Management/Global Parameters page. For more information, see Oracle TSAM Plus User Guide

2.4 Configuring Security

2.4.1 Authentication

2.4.1.1 Configuring Database Authentication

The default administrator admin is created during deployment.

You can also add or edit a user from Oracle TSAM Plus monitoring console following these steps:

1. Log in to Oracle TSAM Plus console.
2. From the top menu bar, click **Management** and select **User Management** from the drop-down list.
3. Create, edit or delete a user.

For more information, refer to User Management.

2.4.2 Authorization

TSAM Plus supports role-based authorization.

2.4.2.1 Group Management

You can specify the ID of default groups "Administrator" and "Viewer" during TSAM Plus installation or deployment process. For more information, refer to Set Groups ID in Installing Oracle TSAM Plus Manager Using GUI-Mode Installation and Oracle TSAM Plus Manager Database Server Deployment.

You can also add, edit, or remove groups from Oracle TSAM Plus monitoring console by doing these steps:

1. Log in to Oracle TSAM Plus console.
2. From the top menu bar, click **Management** and select **User Management** from the drop-down list.
3. Click the **Group List** button to enter the Group List menu bar.
4. Specify the group ID when creating a group.

For more information, refer to User Management.

2.4.2.2 Group/User Privileges

Refer to Oracle TSAM Plus Group/User Privileges.

3

Configuring OIDC for Oracle TSAM Plus Manager with Keycloak and WebLogic

This section contains the following topics:

3.1 Overview

You can configure Oracle TSAM Plus Manager to use OpenID Connect (OIDC) authentication instead of local authentication. This setup integrates Oracle TSAM Plus Manager with Keycloak and enables centralized authentication and role-based access control. You must configure Keycloak and the WebLogic OIDC Asserter to establish trust with the identity provider. You can then enable OIDC using the provided script, deploy the application with OIDC options, and restart WebLogic Server. Finally, you can verify login, logout, and access behavior, or disable OIDC to restore local authentication.

Follow this high-level flow:

1. Configure Keycloak
2. Configure the WebLogic OIDC Asserter
3. Enable OIDC support for Oracle TSAM Plus Manager using the automation script
4. Deploy or update the Oracle TSAM Plus Manager application
5. Restart WebLogic and verify login and logout

To enable OIDC in Oracle TSAM Plus Manager, follow the steps below:

- First, configure Keycloak by defining the realm, client, roles, users, and required endpoints such as redirect and logout URLs
- Next, configure the WebLogic OIDC Asserter to integrate with the identity provider
- Then, run `TSAMOIDC_enable.sh` to enable OIDC support
- After that, deploy the application using `TSAMDeploy.sh` with the `-enableOIDC` option
- Then, restart WebLogic Server to apply the changes
- Finally, verify login, logout, and role-based access

To disable OIDC and restore local authentication, follow the steps below:

- First, run `TSAMOIDC_disable.sh`
- Then, redeploy the application using `TSAMDeploy.sh`
- Next, restart WebLogic Server
- Finally, verify that local authentication is restored and working correctly

3.2 Prerequisites

Before starting, ensure the following are available:

- A working Keycloak instance
- A WebLogic Server domain hosting Oracle TSAM Plus Manager
- An Oracle TSAM Plus Manager `EAR` file is available for deployment/update
- Access to deploy Oracle TSAM Plus Manager using `TSAMDeploy.sh`
- Access to the OIDC helper scripts:
  - `TSAMOIDC_enable.sh`
  - `TSAMOIDC_disable.sh`
  - `zip` and `unzip` available on the system PATH
  - Network connectivity between WebLogic and the Keycloak server

For more information on WebLogic OIDC Asserter configuration, see Configuring the WebLogic OpenID Connect Provider

3.3 Configuring Keycloak for Oracle TSAM Plus Manager

This section explains how to configure Keycloak for TSAM using the **Keycloak Admin Console**.

3.3.1 Installing and Starting Keycloak

To install and configure Keycloak, see the Getting Started Guide

> **Note**
>
> - By default, TSAM domain validates the hostname during the TLS handshake. Therefore, when HTTPS is used, the certificate used by Keycloak must include the appropriate Subject Alternative Names (SANs) that match the hostname being accessed.
> - If a self-signed certificate is used, its CA certificate must be imported into the WebLogic Server (WLS) truststore so that the certificate chain can be validated successfully.

After installation, you need to verify the following:

- Keycloak is running
- You can access the **Keycloak Admin Console**
- You can log in using an administrative user
  Example admin console URL:

  ```
  http://<keycloak-host>:<port>/admin
  ```

(or)

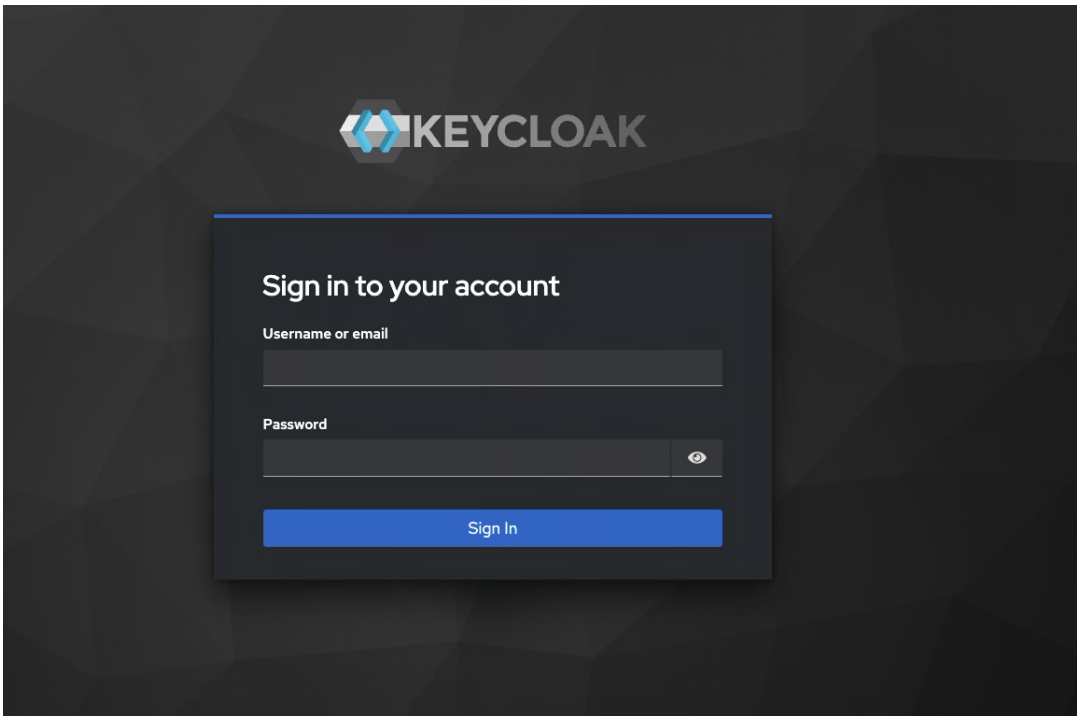
```
https://<keycloak-host>:<port>/admin
```

3.4 Logging in to the Keycloak Admin Console

To log in to the Keycloak Admin Console, follow the steps below:

1. Open the Keycloak Admin Console URL in a browser
2. Sign in with a Keycloak administrator account
3. After login, verify that the admin console home page is visible:

Figure 3-1 Keycloak Admin Console

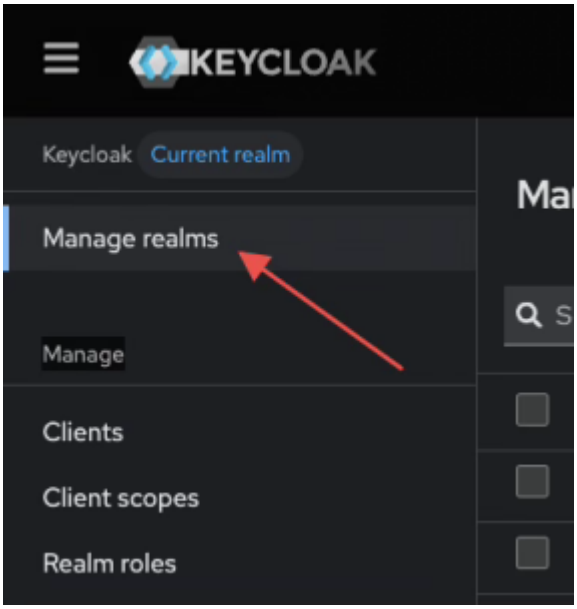


3.5 Creating a Realm for Oracle TSAM Plus Manager

Follow the steps below to create a Realm for Oracle TSAM Plus Manager:

1. In the left navigation, click on **Manage Realms**

Figure 3-2 Manage Realms



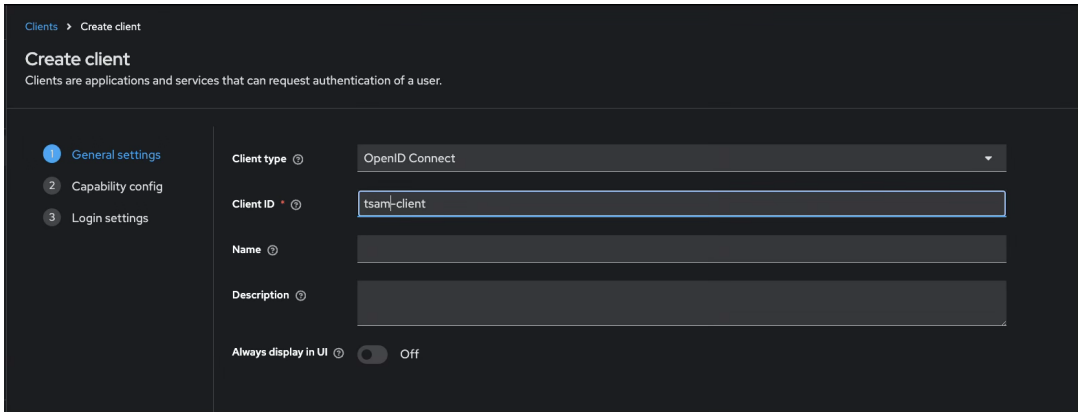
2. Click **Create realm**
3. Enter the realm name. For example, Oracle TSAM Plus Manager
4. Click **Create**

> **Note**
>
> After creating the realm for Oracle TSAM Plus Manager, you need to ensure that the active realm is the newly created `TSAM` realm by clicking on the list of realms.

3.6 Creating a Client for Oracle TSAM Plus Manager

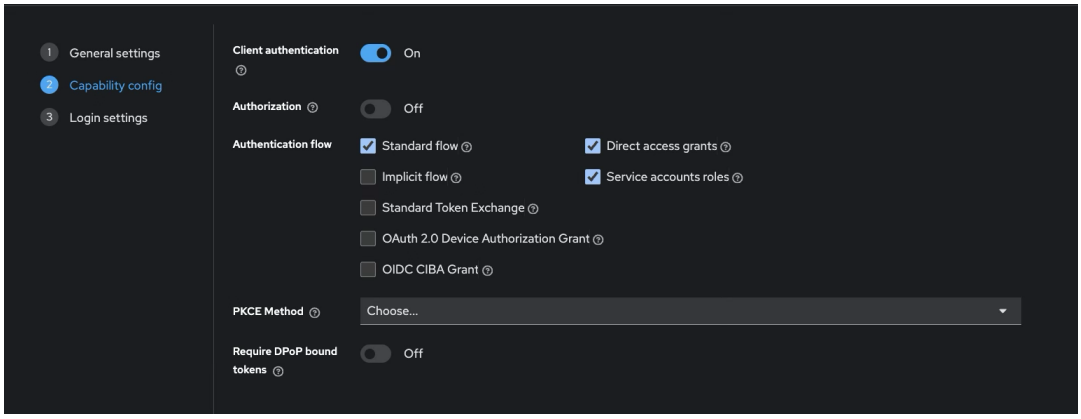
1. In the left navigation, click **Clients**
2. Click **Create client**
3. Enter the client details:
   Recommended Values:

Figure 3-3 Create a Client



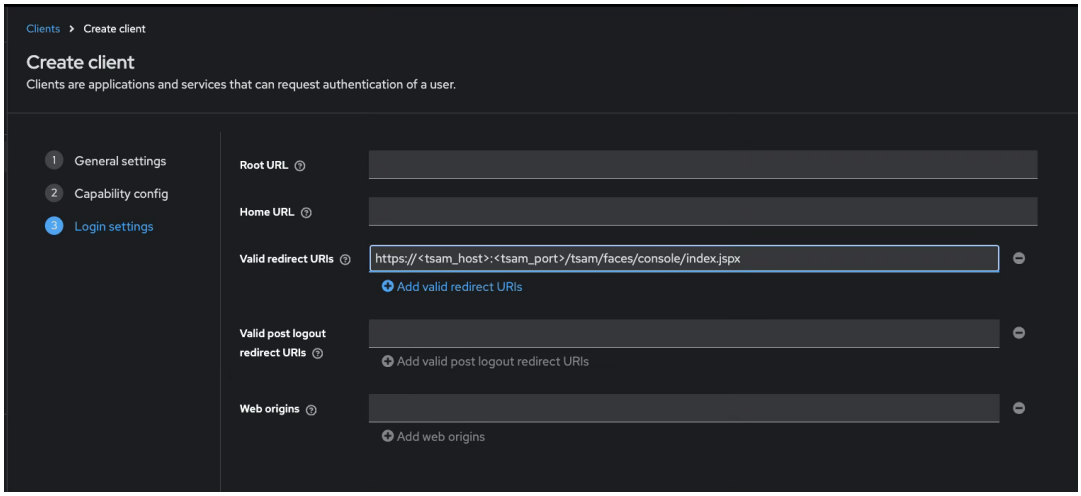
4. Click **Next**
5. Configure the client capability settings as required by your Keycloak version

Figure 3-4 Recommended Values



6. Click **Next** to move onto Log in Settings.
7. Add the Valid redirect URIs in the Log in settings:

Figure 3-5 Valid redirect URIs



8. Save the settings for the client.

After creating the client, note the following details:

- Client ID
- Client Secret

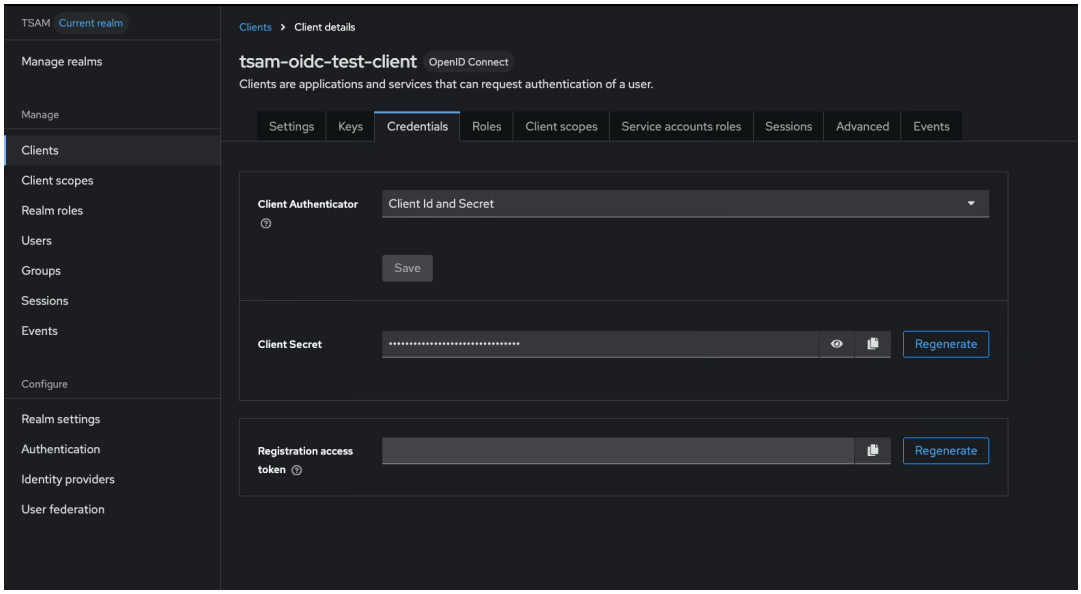
You will need the client secret later to configure OIDC.

3.6.1 Retrieving the Client Secret

Follow the steps below, to retrieve the value of `Client Secret` parameter:

1. Open the newly created Oracle TSAM Plus Manager client
2. Go to the **Credentials** tab
3. Copy the **Client Secret**

Figure 3-6 Client Secret



3.7 Create Client Scope

Create a new client scope that includes WLS OIDC provider required mappers.

Figure 3-7 Keycloak Client Scope

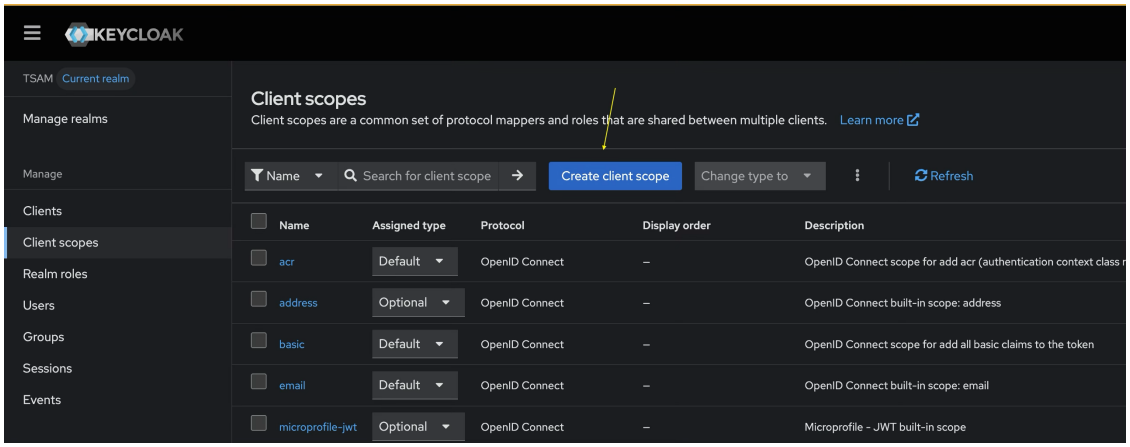
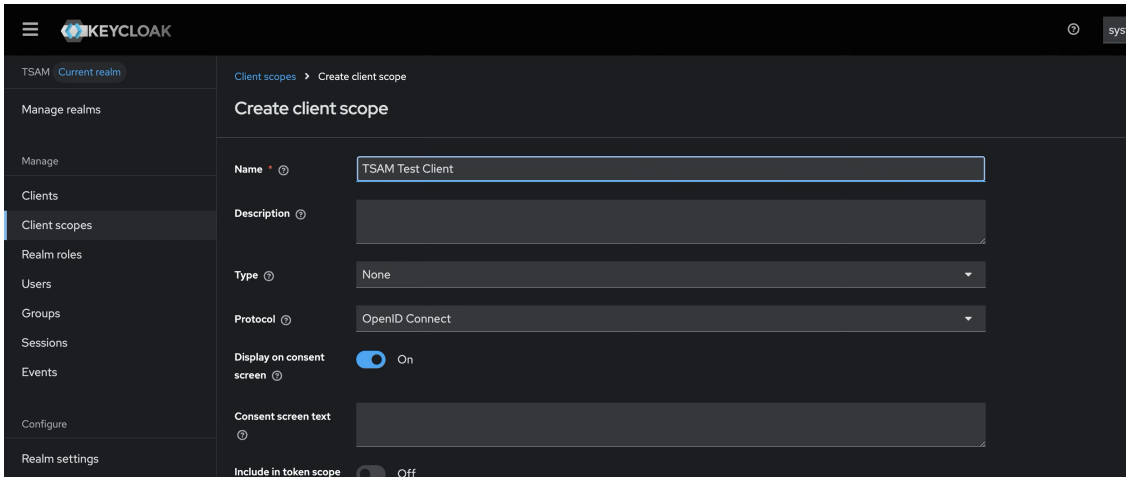


Figure 3-8 Keycloak Client Scope



Next, add predefined **upn** and **groups mappers** to the scope.

Figure 3-9 Mappers

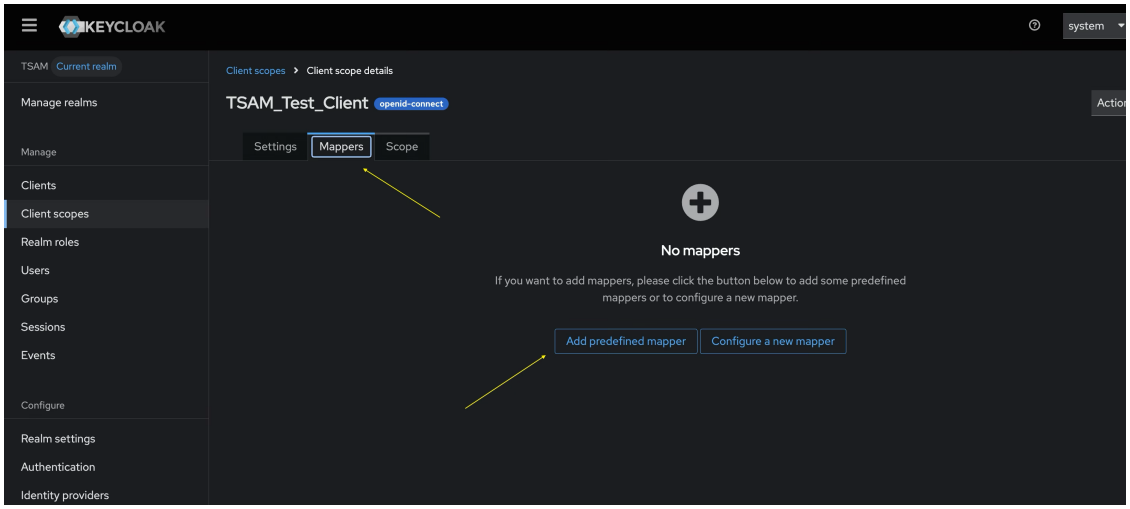


Figure 3-10 Mappers

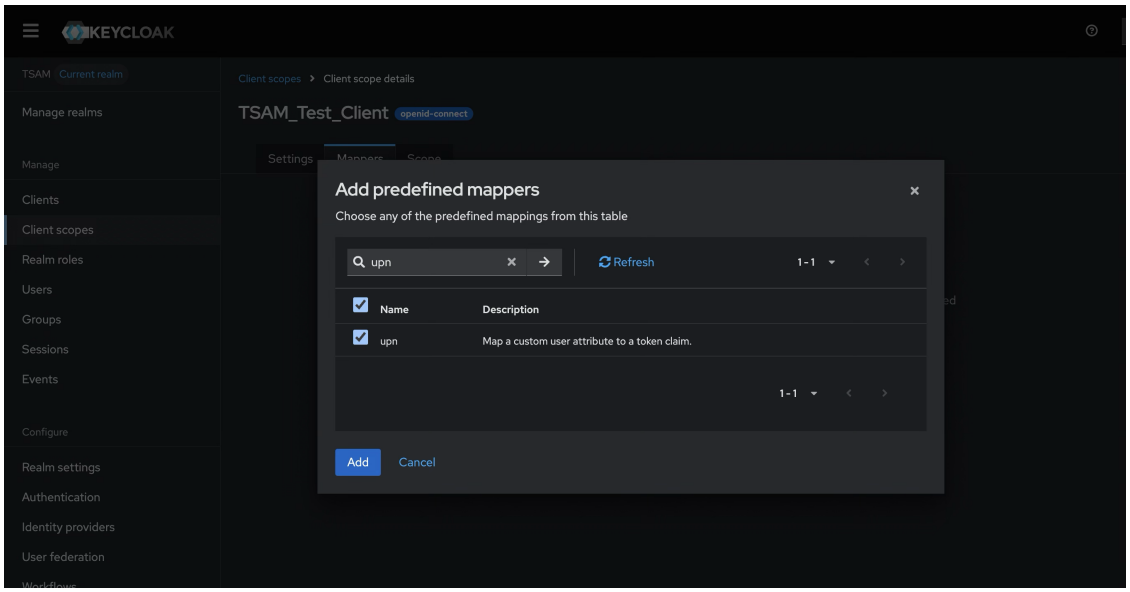
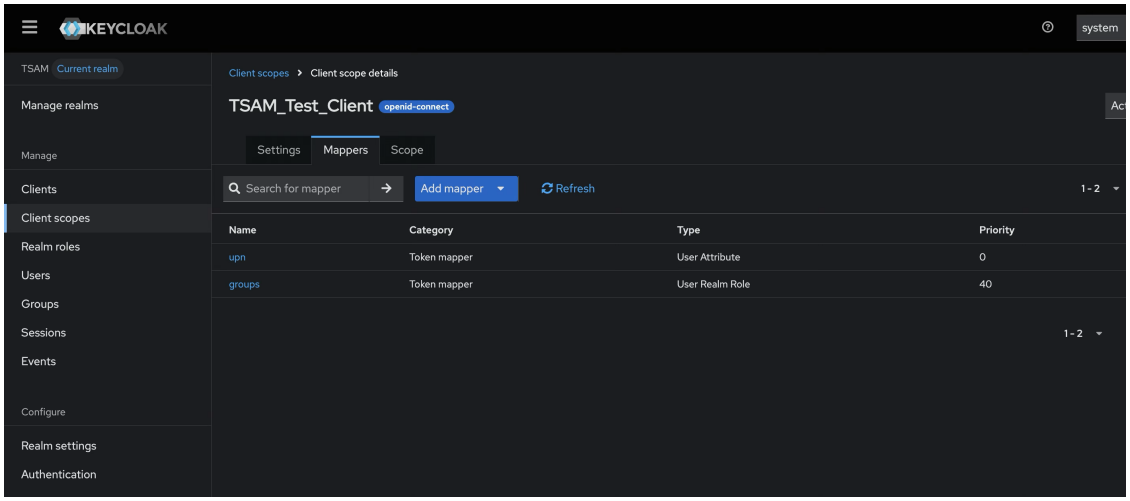


Figure 3-11 Mappers



3.8 Adding a Newly Created Client Scope to a Client

Add Client Scope you have created to the Client with the Assigned Type as "Default".

Figure 3-12 Adding Client Scope to the Client

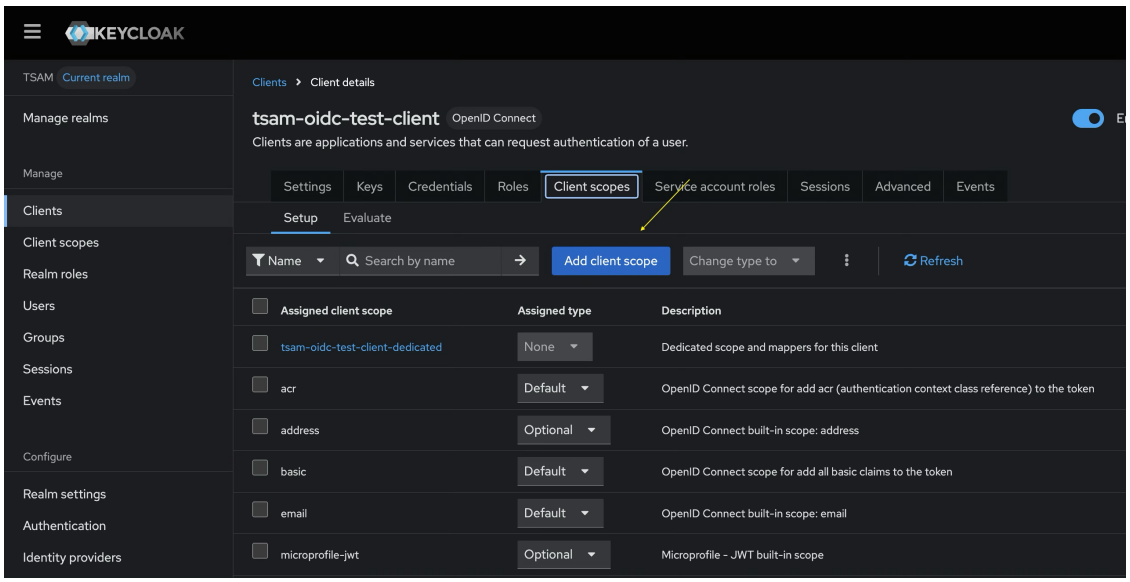
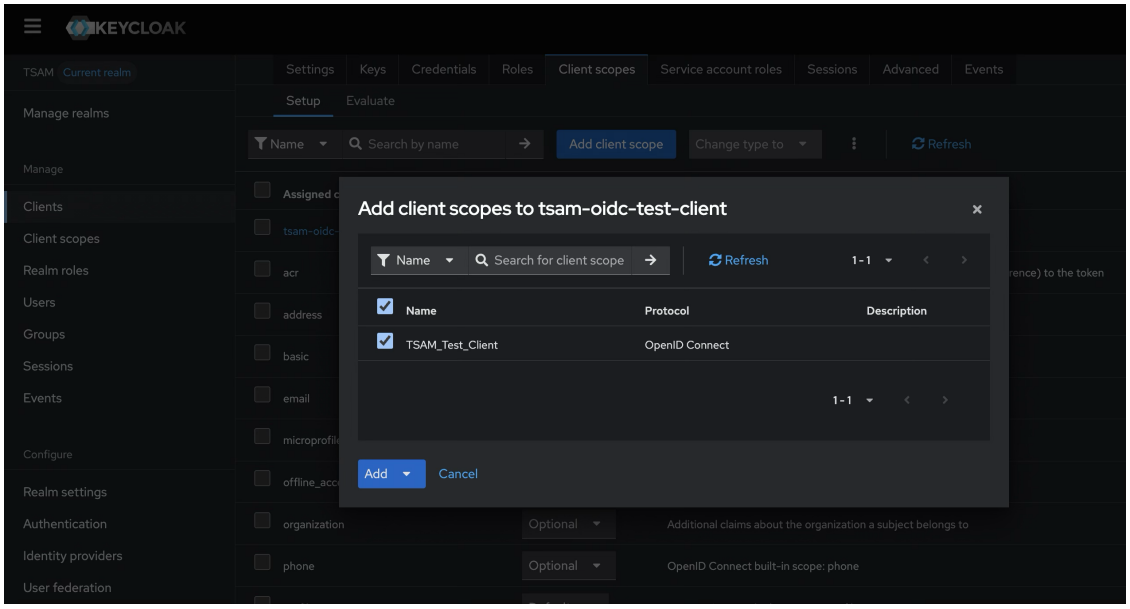


Figure 3-13 Adding Client Scope to the Client



3.9 Configuring Redirect URIs for the Oracle TSAM Plus Manager Client

If the Redirect URI is not configured during the client creation, then you must configure the redirect settings.

1. Open the Oracle TSAM Plus Manager client in Keycloak
2. Go to the client settings page
3. Locate the field for `Valid Redirect URIs`
4. Add the Oracle TSAM Plus Manager application URI

```
https://<tsam-host>:<tsam-port>/tsam/faces/console/index.jspx
```

```
http://<tsam-host>:<tsam-port>/tsam/faces/console/index.jspx
```

> **Note**
>
> - The redirect URI must match the deployed Oracle TSAM Plus Manager URI
> - If the redirect URI does not match, then the login may fail
> - If your environment uses HTTPS, then configure the HTTPS URI
> - If HTTP is explicitly used in QA or test setups, configure the HTTP URI accordingly

3.10 Creating Roles Required by TSAM

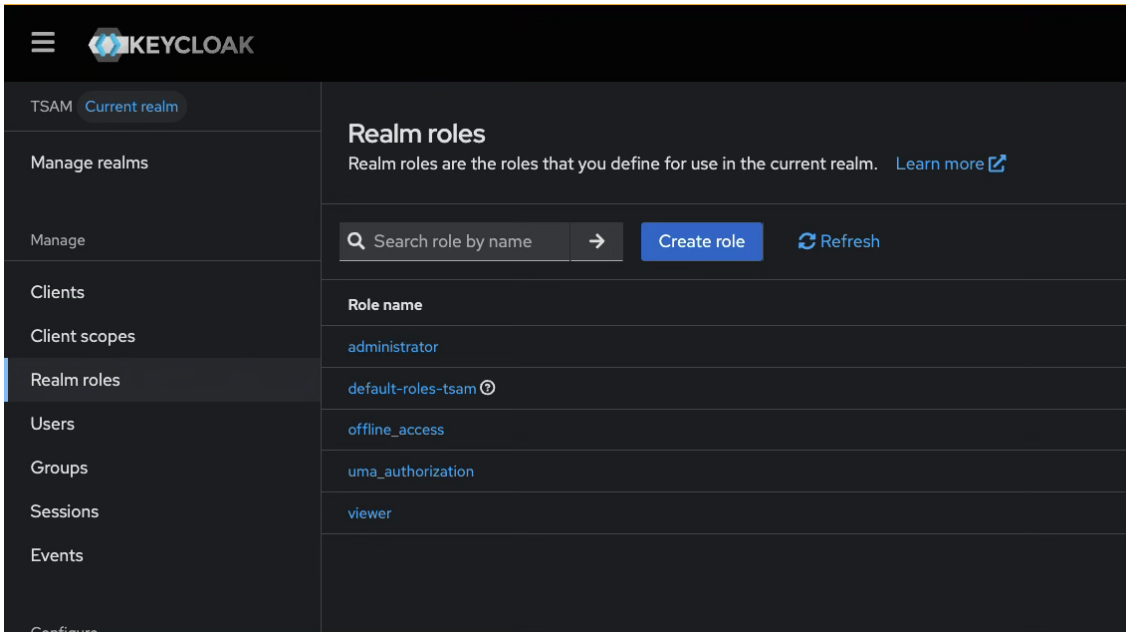
Oracle TSAM Plus Manager requires the following application roles:

- `administrator`
- `viewer`

To create the roles, follow the steps below:

1. In the left navigation, click **Realm roles.**
2. Click **Create role**
3. Enter the role name: `administrator`
4. Save the role.
5. Repeat the same process for: `viewer`

Figure 3-14 Create Roles



3.11 Creating Users in Keycloak

You can create one or more users for Oracle TSAM Plus Manager login. For example:

- `tsamadmin`
- `tsamviewer`

Follow the steps below to create a user in Keycloak:

- In the left navigation, click **Users**
- Click **Add user** or **Create user**

- Enter the username.
- Enter any additional fields required by your environment
- Click **Create**

Figure 3-15 Create user

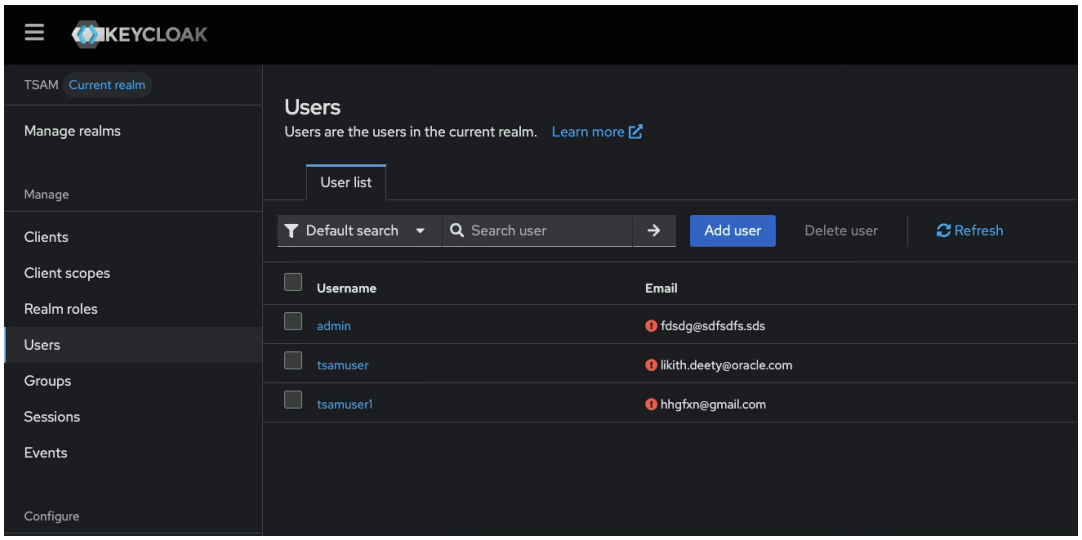
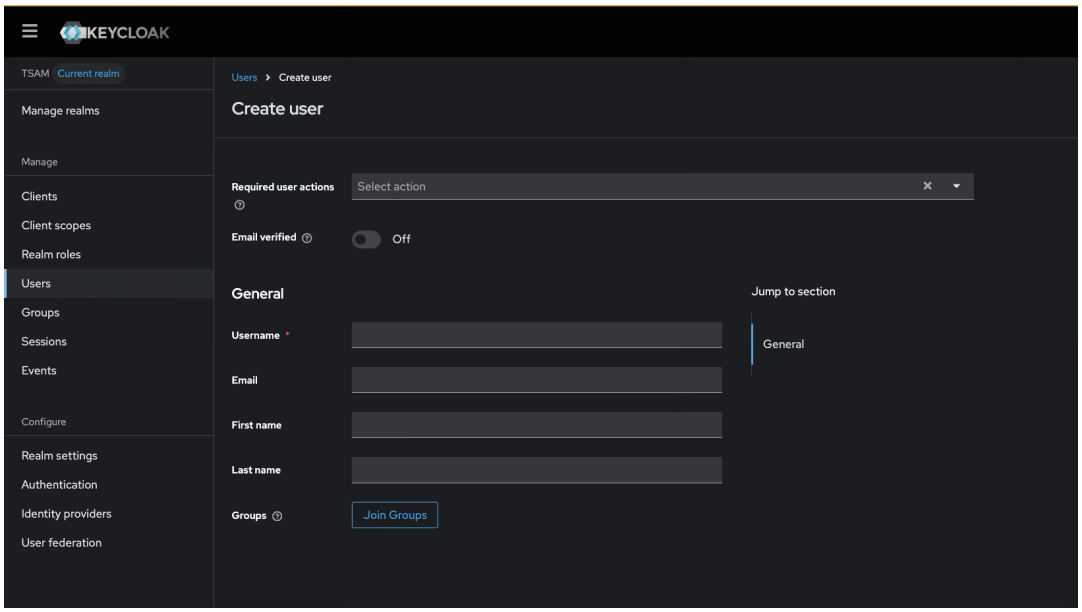


Figure 3-16 Create user



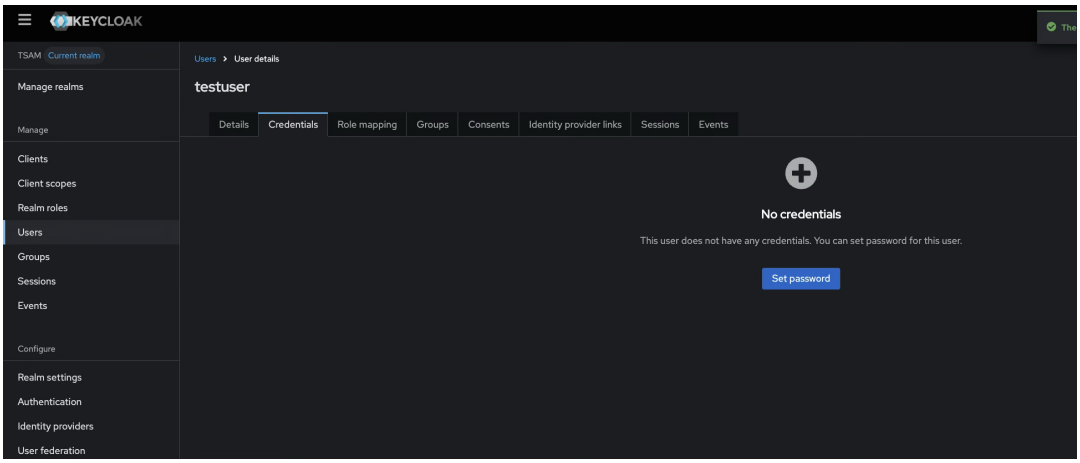
3.12 Setting Password for Each User

After you create users in Keycloak, you need to set a password for each user. Follow the steps below to set the password for each user:

1. Open the user

2. Go to the **Credentials** tab
3. Set a password
4. Optionally disable Temporary if you do not want the user to reset the password at first log in
5. Save the password.

Figure 3-17 Set Password for Each User



3.13 Mapping Roles to Users

You need to assign a role to each user that you have created.

This section contains the following topics:

3.13.1 Mapping the Administrator User Role

To map the administrator user role, follow the steps below:

1. Select the user, for example `tsamadmin`
2. Go to the **Role mapping** tab
3. Click on **Assign Role → Realm roles**
4. Assign the role: **administrator**

3.13.2 Keycloak Verification Checklist

Before proceeding, verify all of the following:

- Keycloak is installed and running
- Admin console is accessible
- Oracle TSAM Plus Manager realm is created
- Oracle TSAM Plus Manager client is created
- Oracle TSAM Plus Manager `client secret` parameter is copied

- Redirect URI is configured
- `administrator` role is created
- `viewer` role is created
- test users are created
- roles are mapped to the correct users

3.13.3 Mapping the Viewer User Role

Follow the steps below, to view the role of a user:

1. Open a user, such as `tsamviewer`
2. Go to the **Role mapping** tab.
3. Click on **Assign Role** → **Realm roles**
4. Assign the role: `viewer`

> **Note**
>
> After mapping the roles, you need to verify the following:
>
> - `tsamadmin` has the `administrator` role
> - `tsamviewer` has the `viewer` role

Figure 3-18 Viewing Role of a User

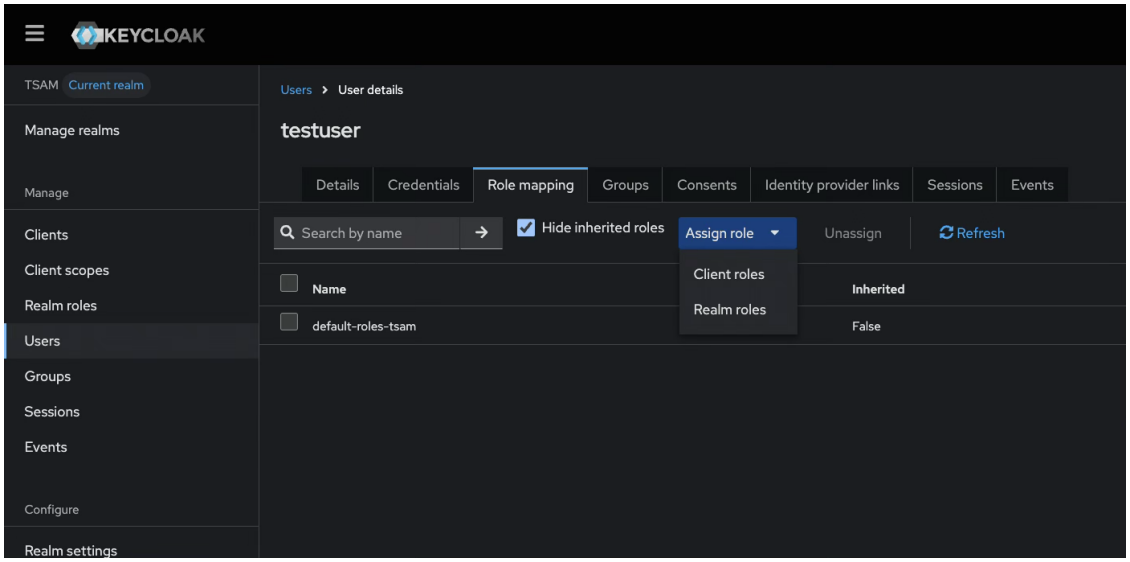
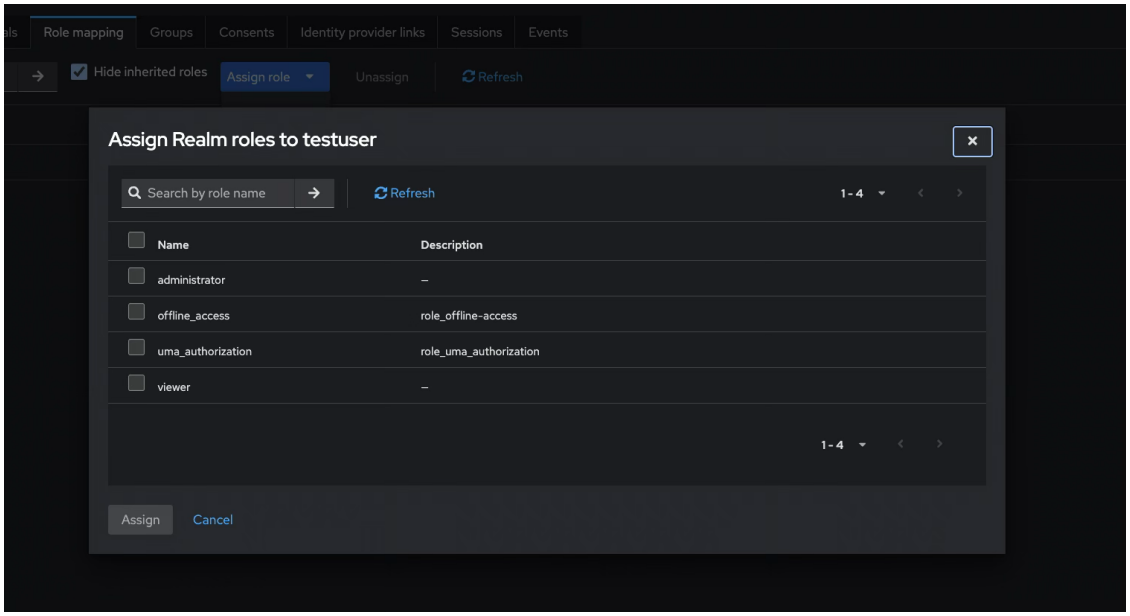


Figure 3-19 Assign Realm Roles to a user



3.14 Capturing the OIDC Values for Oracle TSAM Plus Manager

Before proceeding to the Oracle TSAM Plus Manager and WebLogic configuration, collect the following values from Keycloak:

- Issuer URI
- Client ID
- Client Secret
- Valid Redirect URI

The above values are required when enabling OIDC support for Oracle TSAM Plus Manager.

3.14.1 Example Issuer URL

```
https://<keycloak-host>:<port>/realms/TSAM
```

```
http://<keycloak-host>:<port>/realms/TSAM
```

> **Note**
>
> These values are required when enabling OIDC support for Oracle TSAM Plus Manager.

3.15 Common Keycloak Issues

This section contains the following topics:

3.15.1 Redirect URL Mismatch

If login fails before returning to Oracle TSAM Plus Manager, then check for the following issues:

- Verify the configured redirect URI
- Verify the deployed Oracle TSAM Plus Manager URL
- Verify HTTP vs HTTPS usage

3.15.2 User logs in but access is incorrect

If the user successfully authenticates but does not get the expected Oracle TSAM Plus Manager access, then you need to verify the following parameters:

- Verify the assigned Keycloak roles
- Verify that the role names are correct:
  - `administrator`
  - `viewer`

3.15.3 Wrong Realm or Client Used

If authentication requests go to the wrong realm or client, then you need to verify the following:

- Verify the active Keycloak realm
- Verify the Oracle TSAM Plus Manager client configuration
- Verify the issuer URL used by Oracle TSAM Plus Manager

3.16 OIDC Automation Scripts

Enabling and disabling OIDC support for Oracle TSAM Plus Manager is automated through scripts.

This section contains the following topics:

3.16.1 Enabling Script

`TSAMOIDC_enable.sh` updates `tsam.war` inside `tsam_22c.ear` to enable OIDC, requires zip and unzip, and looks for `oidcAuth.properties` via `-oidcPropertiesFile`. It prompts interactively for any missing required values (`issuer`, `clientId`, `clientSecret`, `redirectUrl`), hides `clientSecret` input, and defaults `inactivityTimeout` to 60 minutes when omitted.

Script Name: `TSAMOIDC_enable.sh`

Description: Enables OpenID Connect authentication for the `TSAM EAR` by updating `tsam.war` with OIDC configuration files and properties.

Usage:

```
./TSAMOIDC_enable.sh -oidcPropertiesFile <path to oidcAuth.properties>
```

- Requires both `zip` and `unzip` on the `PATH`
- Expects `tsam_22c.ear` in the same directory as the script by default
- Creates a temporary workspace for unpacking/repacking the `EAR` and `WAR`
- Requires an `oidcAuth.properties` file as input.
- Missing required values are prompted for interactively.

Required Properties:

The following are the Required properties in `oidcAuth.properties`:

issuer

clientId

clientSecret

redirectUrl

> **Note**
>
> If a required property is missing or blank, then the script prompts for it interactively. `clientSecret` input is hidden.

Optional Properties

The `inactivityTimeout` is the Optional property in `oidcAuth.properties`

- `inactivityTimeout` is in minutes.
- If omitted, then the script adds `inactivityTimeout=60`

> **Note**
>
> If present, then inactivityTimeout must be a positive integer.

Example

```
issuer=https://idp.example.com/realms/tsam
  clientId=tsam-app
  clientSecret=<secret>
  redirectUrl=https://tsam.example.com:7002/tsam/faces/console/index.jspx
  inactivityTimeout=90
```

3.16.2 Disabling Script

Script Name: `TSAMOIDC_disable.sh`

Description: Reverts Oracle TSAM Plus Manager authentication from OpenID Connect back to the default `LocalFirst` mode by restoring the original web and weblogic descriptors and cleaning up OIDC-specific properties.

Usage: `./TSAMOIDC_disable.sh`

> **Note**
>
> - Requires both `zip` and `unzip` on the `PATH`
> - Expects `tsam_22c.ear` in the same directory as the script by default
> - Creates a temporary workspace for unpacking/repacking the EAR and WAR

3.17 Creating OIDC Asserter in WLS

This section contains the following topics:

3.17.1 Deploying a New Oracle TSAM Plus Manager Domain with OIDC Enabled

Run `TSAMDeploy.sh` with `-enableOIDC` while deploying the `TSAM EAR`.

```
./TSAMDeploy.sh \
-WLSAdminUser <admin username> \
-enableOIDC \
-createDataSource \
-dbConnStr <DB connection string> \
-dbUser <DB user> \
-EARFile <path to tsam_22c.ear>
```

3.17.2 Enabling OIDC

When `-enableOIDC` is specified, then the deployment flow creates the OIDC asserter needed for Oracle TSAM Plus Manager OIDC authentication.

This is now the supported mechanism for enabling OIDC during deployment of a new Oracle TSAM Plus Manager domain.

3.17.3 Restarting WebLogic

When OIDC is enabled for the first time in a WebLogic domain, the following changes occur:

- The OIDC Asserter is created.
- The Oracle TSAM Plus Manager EAR is deployed.
- A restart of WebLogic Server is required for the changes to take effect.

> **Note**
>
> A reboot is required the first time the OIDC Asserter is created.

3.17.4 Verifying the OIDC Login

After the reboot:

- Open the Oracle TSAM Plus Manager application
- Confirm that login redirects to Keycloak
- Verify that a user with the `administrator` role can log in successfully
- Verify that a user with the `viewer` role can log in successfully
- Verify that logout works correctly and returns to the configured logout destination

3.18 Enabling OIDC Support on an Existing Oracle TSAM Plus Manager Domain

To enable OIDC on an already deployed Oracle TSAM Plus Manager domain, use the enable script to update the `TSAM EAR` and then redeploy it.

3.18.1 Preparing Files

Make sure the following are available in the same directory:

- `tsam_22c.ear`
- `TSAMOIDC_enable.sh`

3.18.2 Run the Enable Script

Run:

```
./TSAMOIDC_enable.sh -oidcPropertiesFile <path to oidcAuth.properties>
```

Example

```
./TSAMOIDC_enable.sh -oidcPropertiesFile oidcAuth.properties
```

3.18.3 Redeploying the Updated EAR

Deploy the updated `EAR` using the `-enableOIDC` flag:

```
./TSAMDeploy.sh \
-WLSAdminUser <admin username> \
-enableOIDC \
```

```
-createDataSource \
-dbConnStr <DB connection string> \
-dbUser <DB user> \
-EARFile <path to tsam_22c.ear>
```

3.18.4 Restarting WebLogic

Restart the WebLogic Server after deployment is successful.

3.18.5 Verification

Verify the following:

- Oracle TSAM Plus Manager redirects to Keycloak for login
- Admin user login works
- Viewer user login works
- Role-based access works as expected
- Logout works correctly

3.19 Disabling OIDC Support on an Existing Oracle TSAM Plus Manager Domain

To disable OIDC support and return Oracle TSAM Plus Manager to local authentication, use the disable script.

3.19.1 Preparing the Files

Make sure the following files are available in the same directory:

- `tsam_22c.ear`
- `TSAMOIDC_disable.sh`

3.19.2 Run the Disable Script

Run: `./TSAMOIDC_disable.sh`

3.19.3 Redeploy the Updated EAR

Deploy the updated EAR using `TSAMDeploy.sh`.

3.19.4 Verification

Verify that Oracle TSAM Plus Manager now uses local authentication instead of redirecting to Keycloak.

3.20 Troubleshooting

This section helps you identify and resolve common issues encountered during OIDC configuration for Oracle TSAM Plus Manager. It covers problems related to redirect URLs, issuer validation, role mapping, and script execution. Use these checks to verify your configuration and ensure proper integration between Keycloak and WebLogic Server. Follow the guidance to quickly isolate and fix issues affecting authentication and access.

3.20.1 Redirect URL Mismatch

If login fails or Keycloak rejects the request, then verify the following configuration settings:

- The `redirectUrl` value configured in `oidcAuth.properties`
- The Redirect URL configured in Keycloak.
- The Logout URL or Post Logout Redirect URL configured in Keycloak.

All of these values must match the URL of the deployed Oracle TSAM Plus Manager. Any mismatch between these settings and the deployed Oracle TSAM Plus Manager URL can cause login failures or result in Keycloak rejecting the authentication request.

3.20.2 Incorrect Issuer URL

If Oracle TSAM Plus Manager or WebLogic cannot validate the provider, verify the issuer format:

```
https://<keycloak-host>:<port>/realms/TSAM
```

or, if HTTP is being used:

```
http://<keycloak-host>:<port>/realms/TSAM
```

3.20.3 Role Mapping Problems

If users can log in but do not get the expected access:

- ensure Keycloak roles exist
- ensure roles are mapped to users
- ensure role names exactly match:
  - `administrator`
  - `viewer`

3.20.4 Script Preconditions

If the script fails, then verify the following:

- `zip` is installed

- `unzip` is installed
- `tsam_22c.ear` is in the same directory as the script
- the script has execute permission

Example:

```
chmod +x TSAMOIDC_enable.sh TSAMOIDC_disable.sh
```