ADSS Server Installation / Configuration

Table of Contents

How to configure ADSS Server to use SQL Server with Windows Authentication?

1. At the time of installation select the **Advanced Configuration** option at **Database Configuration** screen and click on **Next**
2. At the next screen of **Advanced JDBC Configuration,** leave the windows **User ID** and **Password** fields empty
3. In the JDBC URL field enter the database server name and database name along with following details:

    a. **Kerberos Authentication**
    *jdbc:jtds:sqlserver://<DATABASE_MACHINE>:1433/<DATABASE_NAME>;**integratedSecurity=true***
    e.g. ***jdbc:jtds:sqlserver://db-machine:1433/adss-db;integratedSecurity=true***

    b. **NTLM Authentication**
    *jdbc:jtds:sqlserver://<DATABASE_MACHINE>:1433/<DATABASE_NAME>;domain=<DOMAIN_NAME>;**useNTLMv2=true***
    e.g. ***jdbc:jtds:sqlserver://db-machine:1433/adss-db;Ascertia;useNTLMv2=true***

4. Click Next button to proceed with the installation wizard.
5. Follow this KB article to register all the instances of ADSS Server under domain user account: HowtoregisterealltheinstancesofADSSServer/SigningHubCoreunderdomainuseraccount?

⚠ The user account should be in administrators group on the ADSS Server machine as well as have necessary read/write privileges on the database created for the ADSS Server.

Moving ADSS Server from a pre-production environment to a production environment

Ascertia recommends that detailed testing of ADSS Server is performed within a test / pre-production environment prior to running ADSS Server in production.
Once testing has completed, ADSS Server administrators are recommended to follow these steps before moving into production:

1. Take a full backup of the pre-production environment, i.e. the test application, the ADSS Server folder as well as logs and the database.
2. If the production environment uses the same database as the pre-production environment (not generally recommended) then consider the following:
    - Archive all test transaction logs (with option '**Delete records from database once archived**') in all ADSS Server services for future reference if required
    - Any test keys/certificates/profiles/clients not required in the production environment should be deleted
    - Any other configurations which may not be required in the production environment should also be removed e.g. CAs registered in the Trust Manager, operators registered in the Access Control etc.

- Once the production environment is up and running, go to the **ADSS Server Console > CRL Monitor > HA Configuration** and remove the pre-production CRL Monitor instance and restart the CRL Monitor
- Go to **ADSS Server Console > Global Settings > High Availability** and remove the pre-production Core and Console instances.

3. If the production environment uses a fresh database then a different approach is recommended - the **Global Settings > Export / Import** options can be used to export all or selected configurations from the pre-production to the production environment to save re-keying of data, effort and errors that this may create.
4. Consider the logging levels required - described under the Advanced Configuration section of this guide.
5. Review all the elements under the Operational Management section of this guide.
6. Notify Ascertia Support of this planned activity with the relevant details (i.e: date and time, Skype/Web-Ex/GoToMeeting remote session etc).

How to configure SigningHub and its ADSS Server to use SQL Server with Windows Authentication?

1. Install ADSS Server using SQL Server authentication.
2. Click here to download a patch that is required to run ADSS Server and SigningHub Core without storing username and password over windows authentication.
3. Unzip the patch and overwrite its content on **[SigningHub-Home]**.
4. Now go to **[SigningHub-Home]/tools/adss-server/conf** directory.
5. Open the **hibernate.cfg.xml** in edit mode and change the values of these elements as shown below:
    - For Windows Authentication (Kerberos)

hibernate.cfg.xml

```
<property
name="hibernate.connection.url">jdbc:jtds:sqlserver://localhost:1433;databa
seName=ADSS-Server-DB;IntegratedSecurity=true</property>
<property name="hibernate.connection.username"></property>
```

Note: User name must be left empty or username property must be removed in case of Windows Authentication (Kerberos)

- For Windows Authentication (NTLM):

hibernate.cfg.xml

```
<property
name="hibernate.connection.url">jdbc:jtds:sqlserver://<DATABASE_MACHINE>:14
33/<DATABASE_NAME>;domain=<DOMAIN_NAME>;;useNTLMv2=true</property>
<property name="hibernate.connection.username">DOMAIN_USER_NAME</property>
```

6. Now go to **[SigningHub-Home]/core/conf** directory.
7. Open the **hibernate.cfg.xml** in edit mode and change the values of these elements as shown below:

hibernate.cfg.xml

```
<property
name="hibernate.connection.driver_class">com.microsoft.sqlserver.jdbc.SQLServerDr
iver</property>
<property
name="hibernate.connection.url">jdbc:sqlserver://localhost:1433;databaseName=SH-D
B;IntegratedSecurity=true</property>
<property name="hibernate.connection.username">db-user</property>
<property name="hibernate.connection.password">password</property>
<property name="hibernate.hbm2ddl.auto">none</property>
```

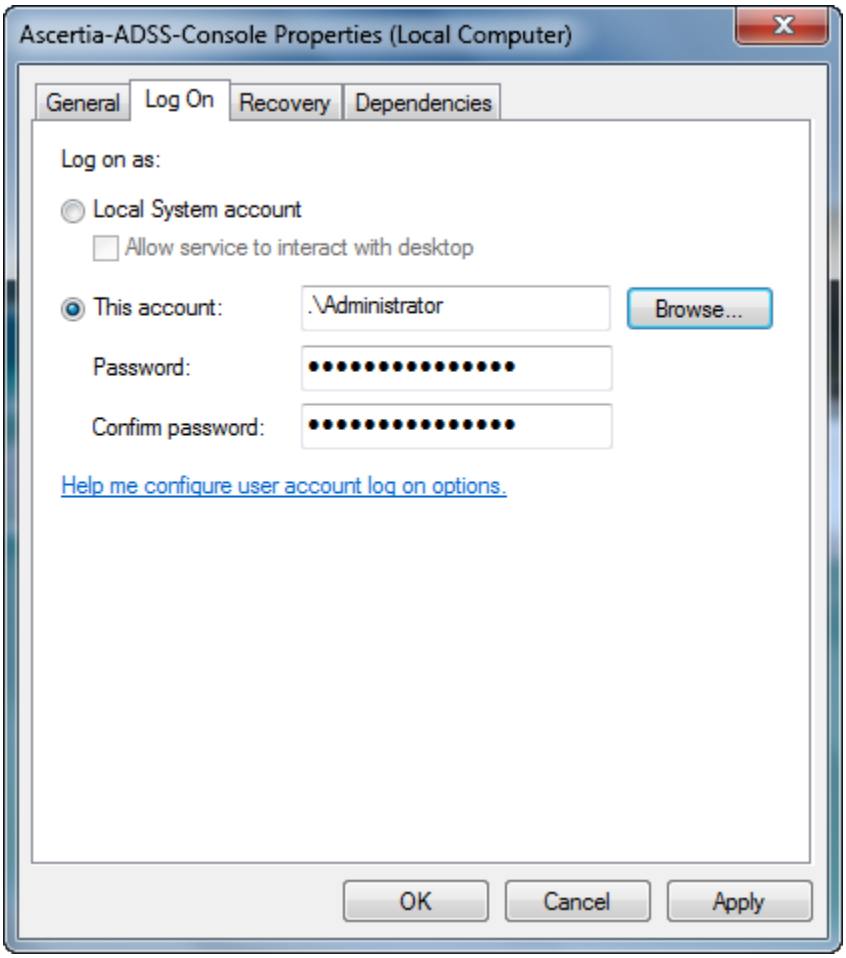
> ⚠ Do not comment or delete the username and password properties from the file - use these values as a dummy username and password otherwise ADSS Server and/or SigningHub will fail to start.

8. Follow this KB article to register all the instances of ADSS Server/SigningHub Core under domain user account: HowtoregisterealltheinstancesofADSSServer/SigningHubCoreunderdomainuseraccount?

How to register all the instances of ADSS Server/SigningHub Core under domain user account?

After the installation of ADSS Server with Windows Authentication, follow these steps to register all the instances of ADSS Server under domain user account:

1. Launch the Windows Services Panel.
2. Stop the ADSS Server Core, Console and Service instances instances.
3. Right click and open the properties for each instance one by one:
    a. Navigate to **Log On** tab
    b. Change the **Log On as** settings from "**Local System account"** to "**This account"**, provide the username and password for the domain user account as shown below:



4. Start (**Ascertia-ADSS-Console**, **Ascertia-ADSS-Core**, **Ascertia-ADSS-Service**) from windows services panel for the changes to take effect.

How to Install ADSS Server with Azure SQL?

1. Extract the ADSS Server package
2. Go to location: **[ADSS-Server-Installation-Dir]\tomcat\bin** and edit these files:

For Linux

- Edit **catalina.sh** file in a text editor and search for the parameter **JAVA_OPTS** and add parameter **-Dcom.sun.net.ssl.enableECC=false** at the end and save the changes as shown below:

catalina.sh

```
JAVA_OPTS="$JAVA_OPTS
-Dorg.apache.catalina.connector.CoyoteAdapter.ALLOW_BACKSLASH=true
-Dorg.apache.tomcat.util.buf.UDecoder.ALLOW_ENCODED_SLASH=true
-Dcom.sun.net.ssl.enableECC=false"
```

For Windows

- Edit **catalina.bat** file in a text editor and search for the strings **%JAVA_OPTS% %CATALINA_OPTS%** and add parameter **-Dcom.sun.net.ssl.enableECC=false** at the end of each string and save the changes as shown below:

catalina.bat

```
%_EXECJAVA% %JAVA_OPTS% %CATALINA_OPTS% %DEBUG_OPTS%
-Dcom.sun.net.ssl.enableECC=false
-Djava.endorsed.dirs="%JAVA_ENDORSED_DIRS%" -classpath "%CLASSPATH%"
-Dcatalina.base="%CATALINA_BASE%" -Dcatalina.home="%CATALINA_HOME%"
-Djava.io.tmpdir="%CATALINA_TMPDIR%" %MAINCLASS% %CMD_LINE_ARGS%
%ACTION%
goto end
:doSecurity

%_EXECJAVA% %JAVA_OPTS% %CATALINA_OPTS% %DEBUG_OPTS%
-Dcom.sun.net.ssl.enableECC=false
-Djava.endorsed.dirs="%JAVA_ENDORSED_DIRS%" -classpath "%CLASSPATH%"
-Djava.security.manager
-Djava.security.policy=="%SECURITY_POLICY_FILE%"
-Dcatalina.base="%CATALINA_BASE%" -Dcatalina.home="%CATALINA_HOME%"
-Djava.io.tmpdir="%CATALINA_TMPDIR%" %MAINCLASS% %CMD_LINE_ARGS%
%ACTION%
goto end
:doJpda

if not "%SECURITY_POLICY_FILE%" == "" goto doSecurityJpda
%_EXECJAVA% %JAVA_OPTS% %CATALINA_OPTS% %JPDA_OPTS% %DEBUG_OPTS%
-Dcom.sun.net.ssl.enableECC=false
-Djava.endorsed.dirs="%JAVA_ENDORSED_DIRS%" -classpath "%CLASSPATH%"
-Dcatalina.base="%CATALINA_BASE%" -Dcatalina.home="%CATALINA_HOME%"
-Djava.io.tmpdir="%CATALINA_TMPDIR%" %MAINCLASS% %CMD_LINE_ARGS%
%ACTION%
goto end
:doSecurityJpda

%_EXECJAVA% %JAVA_OPTS% %CATALINA_OPTS% %JPDA_OPTS% %DEBUG_OPTS%
-Dcom.sun.net.ssl.enableECC=false
-Djava.endorsed.dirs="%JAVA_ENDORSED_DIRS%" -classpath "%CLASSPATH%"
-Djava.security.manager
-Djava.security.policy=="%SECURITY_POLICY_FILE%"
-Dcatalina.base="%CATALINA_BASE%" -Dcatalina.home="%CATALINA_HOME%"
-Djava.io.tmpdir="%CATALINA_TMPDIR%" %MAINCLASS% %CMD_LINE_ARGS%
%ACTION%
goto end
:end
```

- Edit the **service.bat** file in a text editor and search for the parameter **--JvmOptions** and **++JvmOptions** one by one, add parameter **;-Dcom.sun.net.ssl.enableECC=false** at the following location for both of them and save the changes

service.bat

```
"%EXECUTABLE%" //US//%SERVICE_NAME% --JvmOptions
"-Dorg.apache.catalina.connector.CoyoteAdapter.ALLOW_BACKSLASH=true;-D
org.apache.tomcat.util.buf.UDecoder.ALLOW_ENCODED_SLASH=true;-Dcatalin
a.base=%CATALINA_BASE%;-Dcatalina.home=%CATALINA_HOME%;-Djava.endorsed
.dirs=%CATALINA_HOME%\endorsed;-Dcom.sun.net.ssl.enableECC=false"
--StartMode jvm --StopMode jvm

"%EXECUTABLE%" //US//%SERVICE_NAME% ++JvmOptions
"-Dorg.apache.catalina.connector.CoyoteAdapter.ALLOW_BACKSLASH=true;-D
org.apache.tomcat.util.buf.UDecoder.ALLOW_ENCODED_SLASH=true;-Djava.io
.tmpdir=%CATALINA_BASE%\temp;-Djava.util.logging.manager=org.apache.ju
li.ClassLoaderLogManager;-Djava.util.logging.config.file=%CATALINA_BAS
E%\conf\logging.properties;-Dcom.sun.net.ssl.enableECC=false" --JvmMs
%6 --JvmMx %7
```

3. Go to **[ADSS-Server-Installation-Dir]/setup** directory and run the **install.bat/sh** file by right clicking and choosing **Run as administrator** option
4. On the **ADSS Server Installation Type** dialog, select the required option
5. Select the appropriate ADSS Server license file
6. Select the database type **Azure SQL**
7. Provide the credentials for the restored database on Azure SQL
8. Continue with the installation and click the Finish button to complete the installation. More detailed instructions can be found in section 3.1.4 of the ADSS Server installation guide.

Ensuring that Linux daemons are started successfully

On some flavors of Linux (e.g. Fedora) ADSS Server daemons are not started by default at boot time. To ensure the three daemons start at boot time, append the following commands in **/etc/rc.local/**:

```
service tomcatd-ADSS-core start
service tomcatd-ADSS-console start
service tomcatd-ADSS-service start
```

Now all of the ADSS Server daemons will start properly after a system reboot.

What causes ADSS Server Windows services and Unix daemons to not register properly during installation?

When ADSS Server services are not registered properly it is usually because the installer process has not been run with using **Administrator (or root)** privileges.
If the ADSS Server is installed but the services are not registered then follow these instructions to register the daemon/services:

For Windows:

1. Go to the folder: **[ADSS Server installation directory]/tomcat/bin/**.
2. Execute the following batch files one by one using **administrator privileges** (right click and then select the option ***Run as administrator***).
    - install_core.bat
    - install_console.bat
    - install_service.bat

For UNIX:

1. Go to the directory: **[ADSS Server installation directory]/tomcat/bin/**.
2. Execute the following script files one by one **using root user privileges**.
    - install_core.sh
    - install_console.sh
    - install_service.sh

NOTE: Very occasionally the ADSS Server Windows services might not register properly because of this issue:

1. Go to the location: **[ADSS Server installation directory]/tomcat/bin/**
2. Open the following script files one by one and ensure the property "**set INSTALL_PATH"** is set to point to the absolute path for the ADSS Server root installation directory e.g. D:/ADSSv5.2/
    - install_core.bat
    - install_console.bat
    - install_service.bat
3. If this property is not correctly set then edit the files and set the correct path of the ADSS Server installation folder
4. If you see permission issues (e.g. access denied message) then temporarily copy these files to a location where you have full permissions to modify the files e.g. your desktop and modify these files
   After modifying them copy and overwrite these files back to their original location, click on OK if a dialog appears asking for administrative rights.
5. Run these modified install scripts one by one and right click select **Run as administrator**
6. Check that the Windows services are now registered within the Windows services panel

Running ADSS Server as a non-root user daemon on UNIX

1. Create a UNIX user and group to own the ADSS Server processes e.g. "adss".
2. **Install** ADSS Server using the root user so that services can be registered.
3. **Stop** the tomcatd-ADSS-core,tomcatd-ADSS-console, tomcatd-ADSS-service instances.
4. Go to the parent folder of ADSS Server installation directory.
5. **Change** the **ownership** of the ADSS Server installation directory i.e. **chown -R adss:adss <ADSS-Server-Installation-Dir>**.
6. Go to **[ADSS-Server-Installation-Dir]/tomcat/bin**.
7. Edit the following files one by one:
    - **tomcatd_console_linux**
    - **tomcatd_core_linux**
    - **tomcatd_service_linux**
8. Search for string **$TOMCAT_START** in the start function and replace it with **su -c "$TOMCAT_START" adss**
9. **Restart** the system to start the ADSS Server daemons using the new owner account

How to move the ADSS Server from one machine to another one?

⚠ This assumes the database server system is not being changed

1. Get the package for the same version of ADSS Server on the new machine.
2. **Extract** the ADSS Server package.
3. **Stop** the existing ADSS Server Windows services or Unix daemons on the old machine.
4. Go to location: **[New-ADSS-Server-Installation-Dir]/setup** directory and run the **install.bat/sh** file by right clicking and choosing **Run as administrator** option.
5. On the **ADSS Server Installation Type** dialog, select the option **I want to install ADSS Server using existing database**.
6. Select the appropriate ADSS Server license file.
7. Select the database type.
8. Provide the credentials for the existing database that contains the ADSS Server configurations.
9. Continue with the installation and click the **Finish** button to complete the installation. More detailed instructions can be found in **section 4.1.4** of the **ADSS Server Installation Guide**.
10. Copy these files from the existing ADSS Server installation directory to the new ADSS Server:
    - *[ADSS Server installation directory]\conf\adss.keystore*
    - *[ADSS Server installation directory]\conf\pkcs11.properties*
    - *[ADSS Server installation directory]\jdk\jre\lib\security\jssecacerts*
11. If there were load balanced instance(s) with the existing installation then add those again by reinstalling on the machine(s) reserved for this purpose. More detailed instructions can be found in **section 4.1.2** of the **ADSS Server Installation Guide**.
12. Now **uninstall** the ADSS Server from the old machine(s).

Steps to apply a patch on the ADSS Server

1. Download the patch from the link provided by the Ascertia support staff.

2. Extract it on the file system in a directory separate to the ADSS Server installation directory
3. Note the directories shipped in the patch and take a backup of these directories from the current ADSS Server installation directory
4. Stop the ADSS Sever Core, Console and Service instances from the Windows NT Services Panel / UNIX Daemon
5. Copy the contents of the patch to the ADSS Server installation directory and choose to overwrite all files
6. Start the ADSS Sever Core, Console and Service instances from the Windows NT Services Panel / UNIX Daemon
7. Run the test cases for which the fix was provided and then provide your feedback to the support staff so that they can close the ticket
8. If you notice unexpected results after applying the patch, kindly follow these steps to revert back to last working state of ADSS Server
    a. Stop the ADSS Sever Core, Console and Service instances from the Windows NT Services Panel / UNIX Daemon
    b. Copy the backed up directories in step 2 to the ADSS Server installation directory and choose to overwrite all files
    c. Start the ADSS Sever Core, Console and Service instances from the Windows NT Services Panel / UNIX Daemon

If the ADSS Server is running in load balanced mode, then repeat the above steps to apply the patch on each instance of ADSS Server

ADSS Server is not starting after changing the machine name/IP

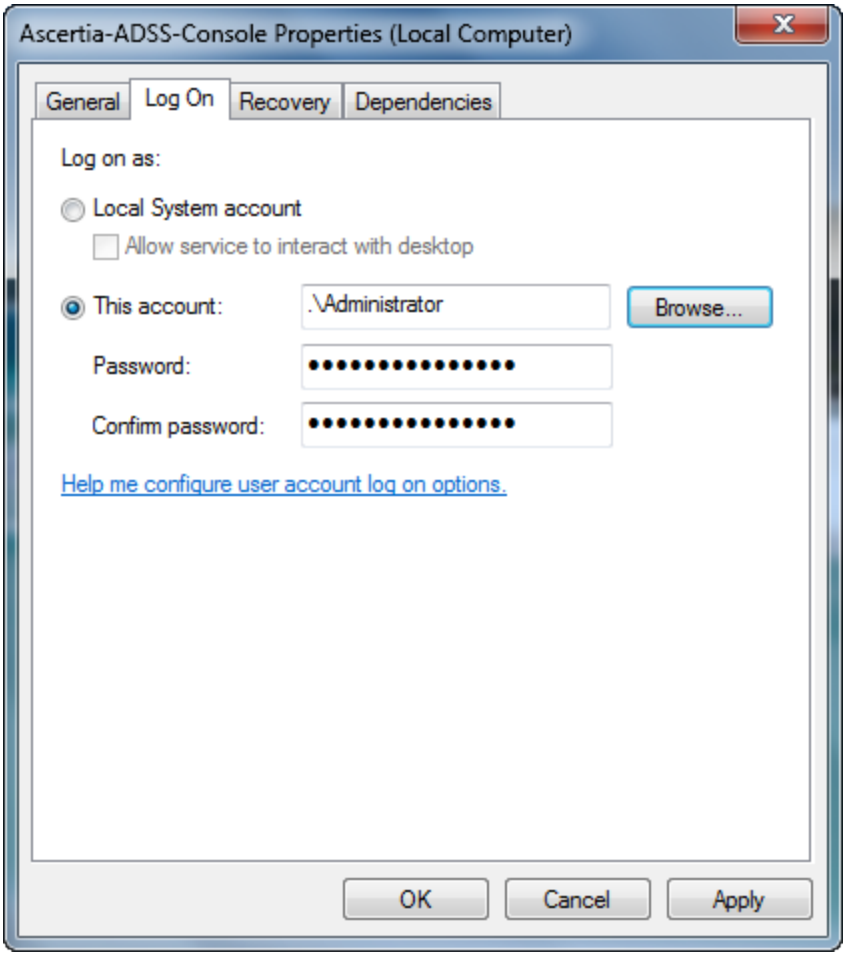
If you have changed the machine name/IP where the ADSS Server is installed then run the following SQL query on the ADSS Server database to update the machine name/IP for the ADSS Server accordingly.

```
UPDATE GlobalSettings SET ParameterValue='localhost/127.0.0.1' WHERE  ParameterId IN
('ADSS_CONSOLE_INSTANCE', 'ADSS_CORE_INSTANCE',
'ADSS_INSTANCES_SYNCHRONIZATION_REQUIRED', 'ADSS_SERVICE_INSTANCE');
UPDATE InstanceHaQueue SET MachineName='localhost';
UPDATE InstanceHaQueue SET ServiceAddress='http://localhost:8773/adss/console/manager'
WHERE InstanceType='CONSOLE';
UPDATE InstanceHaQueue SET ServiceAddress='http://localhost:8770/adss/core/manager'
WHERE InstanceType='CORE';
UPDATE CrlManagerServiceQueue SET MachineName='localhost';
UPDATE CrlManagerServiceQueue SET
ServiceAddress='http://localhost:8777/adss/service/manager';
```

Replace the **localhost/127.0.0.1** with actual machine name and IP address in the above query e.g. **my-adss-server-machine/190.168.2.1**

ADSS Server is not starting after changing the Log On account password

1. Launch the Windows services panel.
2. Stop the ADSS Server Core, Console and Service instances.
3. Right click and open the properties for each instance one by one.
    - Navigate to **Log On** tab
    - Configure the new password for the Log On account as shown below:



4. Start the ADSS Server Core, Console and Service instances.

How to use HMAC re-computation utility manually after installing/upgrading the ADSS Server?

1. Launch the ADSS Server Console in a web browser and go to location: **Global Settings > System Security**.
2. Click on **Generate OTP** button. System will generate and show the OTP (One Time Password).
3. Now open the Command Prompt/Terminal under administrator/root privileges.
4. Navigate to the **[ADSS Server installation directory]\Setup** directory.
5. Type the following command **bin\compute_hmac.bat** (for Windows) or **bin\compute_hmac.sh** (for Linux) to execute the utility. It will ask for OTP generated in Step 2 to complete the HMAC operation.
6. Provide the generated OTP and press Enter button. Utility will be closed automatically once the operation is completed.

How to change the default parking content of ADSS Server?

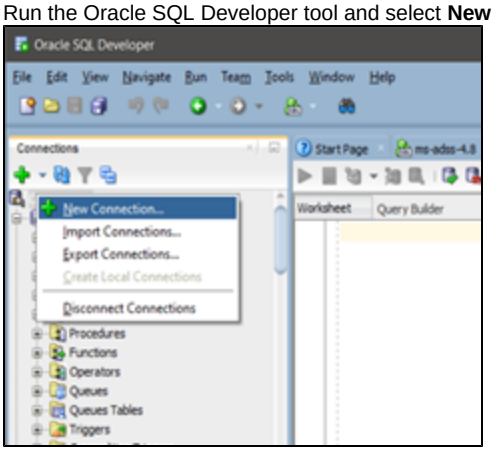
1. Open the **[ADSS Server Installation directory]\service\server\webapps\service\adss.jsp** file
2. Go to line number 102 and change the text according to your needs or if you do not want to show this informtion then comment the code from line number 102 to 134 using comments <!-- -->
3. Save the file and access the URL **http://[server-name]:8777** to see your changes.
4. If you want to change the logo and color scheme of ADSS Server then update the images in **[ADSS Server Installation directory]\service\server\webapps\service\images** directory accordingly. The dimensions of all images must same as for the default images
5. Reload the page to impact changes

- ***If you are running ADSS Server in a load-balanced environment then you need to repeate the above steps on all servers***
- ***You have to change this page every time when you upgrade the ADSS Server to the latest version***

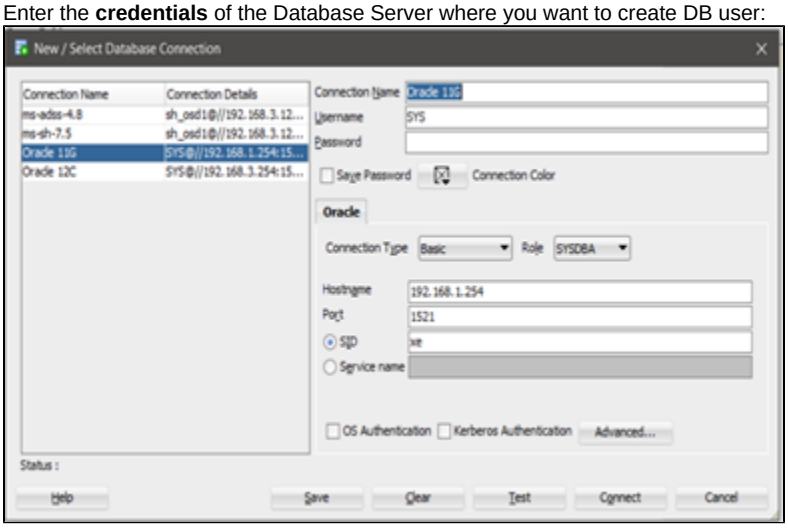
Installing ADSS Server with Oracle Database

To install the ADSS Server with Oracle database, follow these instructions to create the database user using Oracle SQL Developer and configuring it in the ADSS Server:

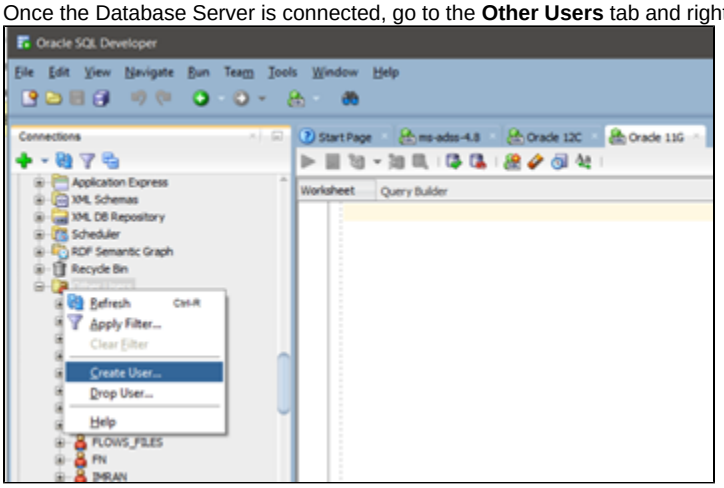
1. Run the Oracle SQL Developer tool and select **New Connection**:



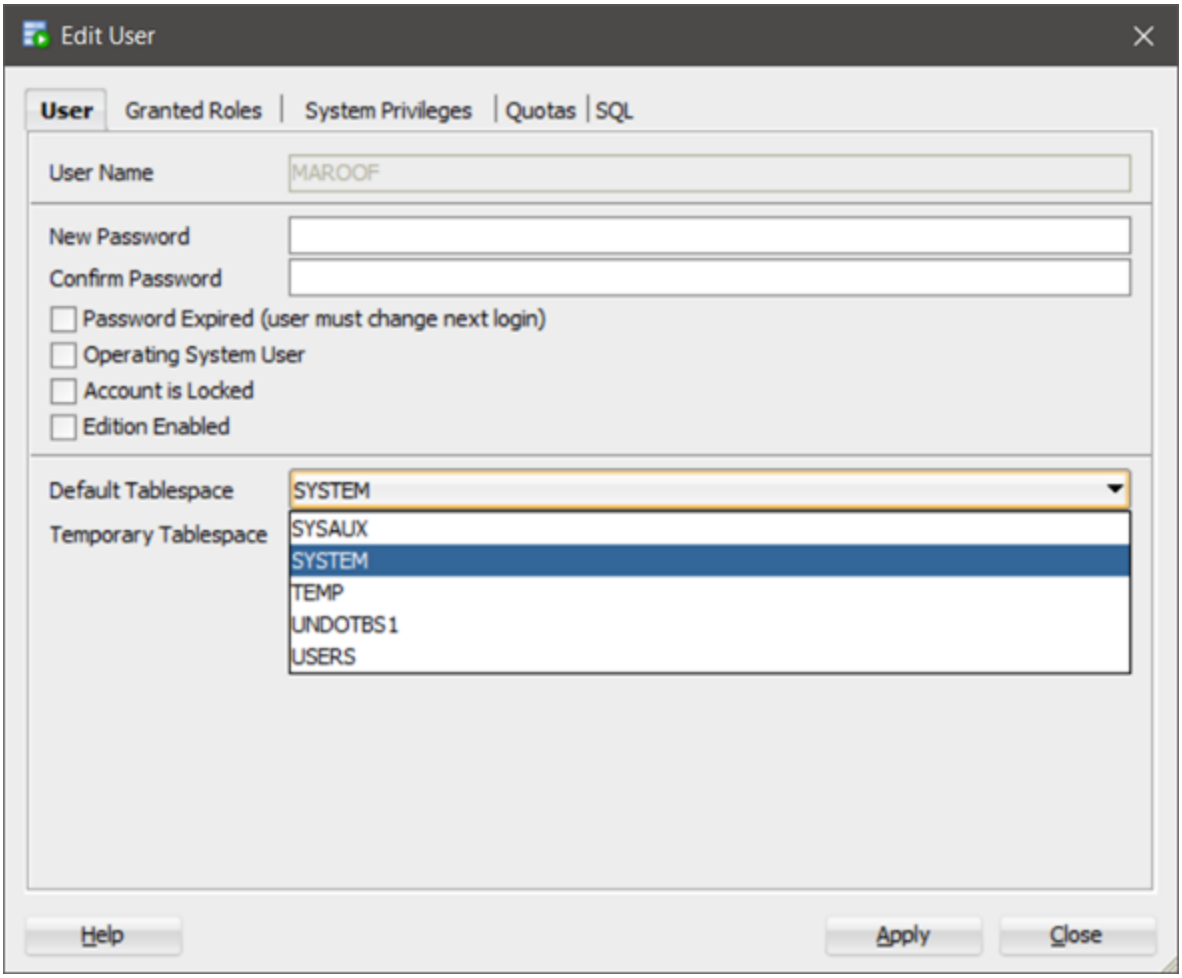
2. Enter the **credentials** of the Database Server where you want to create DB user:



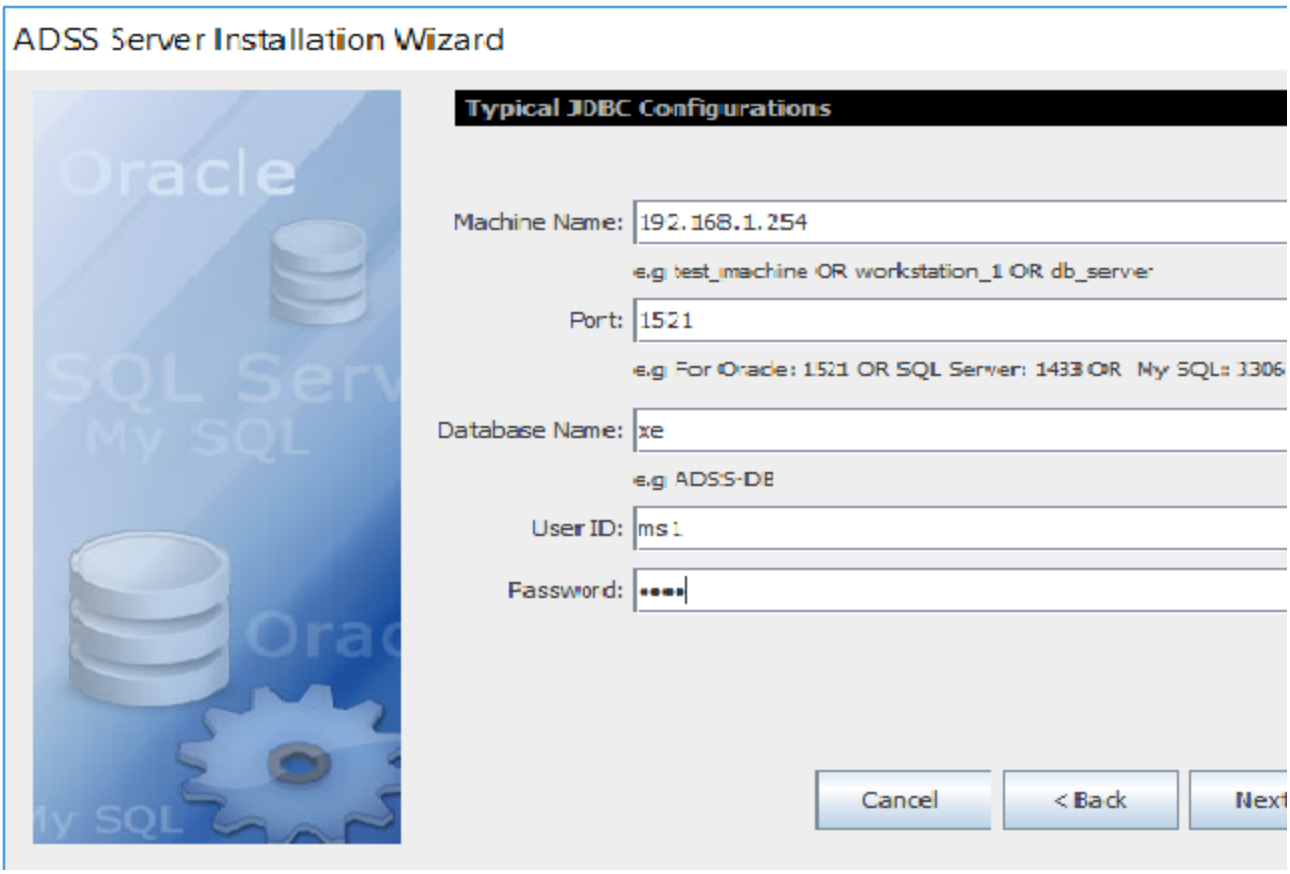
3. Once the Database Server is connected, go to the **Other Users** tab and right click on the label**:**



4. Select **Create User** option from the drop-down menu and provide **User Name**, **Password**, and set the **Default Tablespace** to be **SYSTE M** and **Default Temporary** Tablespace to be **TEMP**



5. Now select the **Granted Roles** tab on the above dialog and select the roles **Connect**, **DBA** and **Resource** privileges.
6. Click **Apply** button to create the user
7. After creating the user, run the ADSS Server installer and navigate to the Database Credentials dialog (it is assumed that you selected the Oracle database on the previous dialog) and enter these credentials as following:



Note that in Database Name, set the SID of the Oracle Database

8. Click **Next** to complete the ADSS Server installation