CA CloudMinder™

Upgrade Guide

1.51

CA Technologies Product References

This document references the following CA Technologies products:

- CA CloudMinder™ Identity Management
- CA CloudMinder™ Advanced Authentication
- CA CloudMinder™ Single Sign-On
- CA Directory
- CA IdentityMinder™
- CA AuthMinder™
- CA RiskMinder™
- CA SiteMinder®
- CA SiteMinder® for Secure Proxy Server
- CA Layer 7

Contents

Chapter 1: Upgrade Prerequisites

This document provides instructions for hosting administrators who are upgrading the latest version of CA CloudMinder.

This section contains the following topics:

Overview of Upgrade Steps

Note the following information before you begin the upgrade process:

- You back up all tasks in the User Console before starting the upgrade.
- The upgrade determines the roles and tasks that are available in all tenant environments.

As a CA CloudMinder hosting administrator, you upgrade each component in your deployment in the following order:

1. Locate Backup Files (see page 8).
2. Back Up User Tasks (see page 9).
3. Review the Upgrade Order (see page 11)
4. Upgrade the Oracle Database (see page 12)
5. Upgrade CA Directory. (see page 12)
6. Upgrade the Provisioning Server and the CA IAM Connector Server. (see page 14)
7. Upgrade the SiteMinder Policy Server and CSP console (see page 16).
8. Upgrade the Secure Proxy Server. (see page 19)
9. Upgrade the Identity Management Server. (see page 20)

Locate Backup Files

You need copies of the /tmp/properties.sh files from the previous installation before you start the upgrade. These files contain passwords and other critical information.

This guide directs you to change a few properties, such as the Java property, in the new properties files. Otherwise, values in the new files must match properties of the installed environment including passwords. Errors can cause loss of the environment.

If you have not backed up the properties.sh files, find a secure remote location to store these files. Do not create backup versions in the /tmp directory, as this directory is volatile. Back up the properties.sh file on the following servers:

- CA Directory server
- Provisioning Server
- CA IAM Connector Server
- CA SiteMinder Policy Server
- Secure Proxy Server
- Identity Management Server

Important! If you have more than one server of any type, back up the properties file on each system. For example, if you have two Directory servers, back up the properties file for each server.

Back Up User Tasks

You must back up all tasks in the Identity Management Management Console. The following procedure allows you to back up and export the tasks, upgrade the environment, and re-import the tasks.

Follow these steps:

1. Click Environments in the Management Console.
2. Select the environment that you want to export.
3. If you want the export operation to display validation and deployment information for managed objects and their attributes, select the Enable Verbose Log Output field on the Environment Properties page before you export the environment.

   Note: Selecting this field can cause significant performance issues during the import.
4. Click the Export button.
5. Save the ZIP file to a location that is accessible to the production system.
6. Click Finish.

   The environment information exports to a ZIP file that you can import into another environment.

Chapter 2: Upgrade Procedures

Before beginning the upgrade, be sure you have met the prerequisite steps (see page 7) to avoid losing information.

This section contains the following topics:

Review the Upgrade Order

Once you have located your backup files and you have backed up user tasks, you are ready to upgrade CA CloudMinder components. Upgrade the components in the following order, which is the order that is used in this guide.

1. Oracle Database

   Note: CA CloudMinder 1.51 supports PostgreSQL as a database. To use PostgreSQL, perform a new installation.

2. CA Directory Server
3. CA Provisioning Server
4. CA IAM Connector Server
5. CA SiteMinder Policy Server
6. CSP console
7. Secure Proxy Server
8. Identity Management Server
9. Layer 7 gateway

Note: When you have a primary and secondary server, upgrade the primary server first.

Database Upgrade

If you continue to use Oracle for CA CloudMinder, Oracle requires an upgrade for Workpoint.

Follow these steps:

1. To enable on the Oracle database transactions for Workpoint 3.5, execute the following commands, substituting an appropriate value for *Identity Management user*:

   ALTER SYSTEM SET JAVA_POOL_SIZE=120M scope=spfile;
   ALTER SYSTEM SET SHARED_POOL_SIZE=240M scope=spfile;
   create pfile from spfile;
   shutdown immediate;
   startup;
   @$ORACLE_HOME\javavm\install\initjvm.sql;
   @$ORACLE_HOME\javavm\install\initxa.sql;
   grant select,insert,update,delete on DBA_PENDING_TRANSACTIONS to *Identity Management user*;
   grant select,insert,update,delete on DBA_PENDING_TRANSACTIONS to system;

   You can ignore errors such as "ORA-29539: Java system classes already installed." However, you may receive a disconnect message from the database. This error is mostly observed while executing the following command:

   @$ORACLE_HOME\javavm\install\initjvm.sql;

   If you receive this error, continue with the next SQL command:

   @$ORACLE_HOME\javavm\install\initjvm.sql;

2. Restart the database by using the following commands. To avoid downtime in an Oracle RAC installation, restart one database at a time.

   shutdown immediate;
   startup;

CA Directory Upgrade

Upgrade the CA Directory server before you upgrade other servers in your deployment. If you have multiple CA Directory Servers in a high availability environment, upgrade the primary CA Directory first.

Follow these steps:

1. SSH into the system to be upgraded.
2. Navigate to this directory.

   /opt/CA/saas/repo/application/

   If this directory has an upgradeBackupList.sh file, it includes a BACKUP_LIST environment variable. It is an array enclosed in parentheses. This variable defines files that are backed up before the upgrade and restored after the upgrade.

   You can add or remove file names from this list as necessary. Insert the filenames in each set of quotes separated by spaces and inside the parenthesis.
3. Verify that a backup (see page 8) of the /tmp/properties.sh file from the previous version exists.
4. Unzip the new kit for the system being upgraded into the root file system folder. For example, enter the following commands:

   cd /
   unzip –o CAM-DIR_kit-*version*.zip
5. Update the /tmp/properties.sh file in the kit with information from the backup version of properties.sh:
   a. Diff the backup file of the previous install and /tmp/properties.sh by entering the following command:

      diff /serverkit/properties.sh /tmp/properties.sh

      The preceding command assumes that backup files are located in the /serverkit folder.

   b. Make appropriate changes to the /tmp/properties.sh file.

   c. If you have downloaded the Java kit to upgrade Java before the CA CloudMinder upgrade, modify the property "JAVA64_KIT" to use "jdk-6u45-linux-x64.bin" instead of "jdk-6u41-linux-x64.bin" as in this example:

      JAVA64_KIT=/*JDK-Installation-Directory*/jdk-6u4**5**-linux-x64.bin; export JAVA64_KIT
6. Run the upgrade by entering the following commands:

   cd /opt/CA/saas/repo/application/
   ./appliance_local.sh config

Verify the upgrade

Verify all DSAs and DSA services, such as the Dxagent Webservices, are running. Enter the following commands:

```
su – dsa
dxserver status
exit
ps –ef|grep dx
```

Provisioning Server and CA IAM Connector Server Upgrade

After you upgrade the CA Directory server, use the following procedure to upgrade the Provisioning Server, then move to the CA IAM Connector Server system and repeat this procedure.

Follow these steps:

1. SSH into the system to be upgraded.
2. Navigate to this directory.

   /opt/CA/saas/repo/application/

   If this directory has an upgradeBackupList.sh file, it includes a BACKUP_LIST environment variable. This variable defines files that are backed up before the upgrade and restored after the upgrade. You can add or remove file names from this list as necessary.
3. Verify that a backup (see page 8) of the /tmp/properties.sh file from the previous version exists.
4. Unzip the new kit for the system being upgraded into the root file system folder. For example, enter the following commands:

   ```
   cd /
   unzip –o CAM-IMPS_kit-version.zip
   ```
5. Update the **tmp/properties.sh** file in the kit with information from the backup version of **properties.sh**:
   a. Diff the original properties.sh file and the temp/properties file by entering the following command:

      diff -y /serverkit/properties.sh /tmp/properties.sh

   b. Make appropriate changes to the /tmp/properties.sh file as required.

   c. Modify the property "JAVA64_KIT" to use "jdk-6u45-linux-x64.bin" instead of "jdk-6u41-linux-x64.bin" as shown in this example:

      JAVA64_KIT=/*JDK-installation-directory*/jdk-6u4**5**-linux-x64.bin; export JAVA64_KIT

6. Run the upgrade by entering the following commands:

   ```
   cd /opt/CA/saas/repo/application/
   ./appliance_local.sh   config
   ```

Verify the upgrade:

1. Verify that all DSAs are running:

   ```
   su – dsa
   dxserver status
   ```

   The *ProvServerhost*-imps-router should be started.

2. If you are performing this procedure on the Provisioning Server, verify that it is running:

   a. Log in as imps user (su – imps)

   b. cd /opt/CA/IdentityManager/ProvisioningServer/bin

   c. ./imps status

   d. Verify that the message "im_ps is running" appears.

3. If you are performing this procedure on the CA IAM Connector Server, verify that it is running by entering the following commands:

   ```
   su – root
   service im_jcs status
   ```

   The message "jcs is running" should appear.

Provisioning Server Troubleshooting

Symptom:

Install fails with message "MSGMNI kernel parameter set is not sufficient"

Solution:

1. Navigate to the server kit install file:

   /opt/CA/saas/repo/application/local_environment.sh

2. Edit the file as follows.

   Change the line that reads:

   REQUIRED_MSGMNI=" 32"

   to read:

   REQUIRED_MSGMNI=" 33"

3. Re-run the Provisioning Server installation process.

Policy Server and CSP Console Upgrade

After you upgrade the Provisioning Server and CA IAM Connector Server, upgrade the CA SiteMinder Policy Server and the CSP Console.

Note: Repeat these steps to upgrade each SiteMinder Policy Server and the CSP console.

Follow these steps:

1. SSH into the system to be upgraded.
2. Navigate to this directory.

   /opt/CA/saas/repo/application/

   If this directory has an upgradeBackupList.sh file, it includes a BACKUP_LIST environment variable. This variable defines files that are backed up before the upgrade and restored after the upgrade. You can add or remove file names from this list as necessary.
3. Verify that a backup (see page 8) of the /tmp/properties.sh file from the previous version exists.
4. Unzip the new kit for the system being upgraded into the root file system folder. For example, enter the following commands:

   cd /
   unzip –o CAM-SMPS_kit-*version*.zip
5. Update the **/tmp/properties.sh** file in the kit with information from the backup version of properties.sh:
   a. Diff the original properties.sh file and the tmp/properties file by entering the following command:

      diff /serverkit/properties.sh /tmp/properties.sh

   b. Modify the property "JAVA64_KIT" to use "jdk-6u45-linux-x64.bin" instead of "jdk-6u41-linux-x64.bin" as shown here:

      JAVA64_KIT=/*JDK-installation-directory*/jdk-6u4**5**-linux-x64.bin; export JAVA64_KIT
      JAVA32_KIT=/*JDK-installation-directory*/jdk-6u45-linux-xi586.bin; export JAVA32_KIT

   c. Rename the properties starting with _oracle_schema to begin with _db_schema and use values for your database user:

      _db_schema_user=<your db user>; export _db_schema_user
      _db_schema_password=<your db user password>; export _db_schema_password

d. Add these properties at the bottom of file:

```
_oracle_schema_user=$_db_schema_user; export _oracle_schema_user
_oracle_schema_password=$_db_schema_password ; export
_oracle_schema_password
```

6. **Before the next step, be sure that you unset the DISPLAY variable.**

   Important! Unless you unset the DISPLAY variable, the environment will be corrupted.

7. Run the upgrade by entering the following commands:

```
cd /opt/CA/saas/repo/application/
./appliance_local.sh    config
```

Tomcat Configuration

After upgrading the Policy Server, Tomcat may fail to start. If it fails, use this procedure.

Follow these steps:

1. Navigate to the following directory:

   /opt/CA/AdvancedAuth/Tomcat/webapps/tenant-services/WEB-INF/classes/resources

2. Edith the following file:

   config.properties

3. Change IM_WEBSERVICE_HOST to the host of the first Identity Management server, if you just upgraded the first Policy Server, or the second Identity Management server if you just upgraded the second Policy Server.

4. Restart Tomcat on the Policy Server that you upgraded as follows:

```
/opt/CA/AdvancedAuth/Tomcat/bin/shutdown.sh
/opt/CA/AdvancedAuth/Tomcat/bin/startup.sh
```

Verify the Upgrade

Follow these steps:

1. Verify dxserver status by executing these commands:

```
su – dsa
dxserver status
```

   Verify that one "*tenantname*-tenant-router started" message exists for each tenant in the environment.

2. Verify that the CSP console is working properly by confirming that the tenant and container tasks exist. Execute the following command:
   ps –ef | grep ui

   You should see a message similar to the following:

   00:00:00 /bin/sh /opt/CA/siteminder/adminui/jboss-as/bin/run.sh

3. Verify that the Policy server is working properly. Execute the following command:
   ps -ef | grep site

   You should see output similar to the following:

   smuser 17067 1 0 06:10 ? 00:00:00 /bin/sh
   /opt/CA/siteminder/adminui/bin/run.sh
   smuser 17095 17067 1 06:10 ? 00:06:15 /opt/java32/bin/java
   -Dprogram.name=run.sh -server
   -Djboss.platform.mbeanserver -Djava.security.policy=workpoint_client.policy
   -Xms256m -Xmx1024m
   -XX:MaxPermSize=256m -XX:ReservedCodeCacheSize=50m
   -Djava.net.preferIPv4Stack=true
   -Djava.endorsed.dirs=/opt/CA/siteminder/adminui/lib/endorsed -classpath
   /opt/CA/siteminder/adminui/bin/run.jar:/opt/java32/lib/tools.jar org.jboss.Main -b
   0.0.0.0 -c default
   root 17533 1 0 06:13 ? 00:00:00 /opt/CA/siteminder/bin/smexec
   root 17534 17533 0 06:13 ? 00:00:26 /opt/java32/jre/bin/java -Xrs
   -Dnete.ps.root=/opt/CA/siteminder -classpath
   /opt/CA/siteminder/lib/smconapi.jar:/opt/CA/siteminder/monitor/smmon.jar
   com.netegrity.smmonagent.SmMonAgentRun
   root 32507 32487 0 15:50 pts/0 00:00:00 grep site

4. Verify that Tomcat is working properly. Execute the following command:
   ps -ef | grep tom

   You should see output similar to the following:
   root 1661 1 0 05:29 ? 00:00:00 automount --pid-file /var/run/autofs.pid
   root 22801 1 0 06:03 ? 00:02:20 /opt/java64/jre/bin/java
   -Djava.util.logging.config.file=/opt/CA/AdvancedAuth/Tomcat/conf/logging.properties
   -Xms256m -Xmx1024m
   -XX:MaxPermSize=256M
   -Djava.util.logging.manager=org.apache.juli.ClassLoaderLogManager
   -Djava.endorsed.dirs=/opt/CA/AdvancedAuth/Tomcat/endorsed -classpath
   /opt/CA/AdvancedAuth/Tomcat/bin/bootstrap.jar:/opt/CA/AdvancedAuth/Tomcat/bin/to
   mcat-juli.jar
   -Dcatalina.base=/opt/CA/AdvancedAuth/Tomcat
   -Dcatalina.home=/opt/CA/AdvancedAuth/Tomcat
   -Djava.io.tmpdir=/opt/CA/AdvancedAuth/Tomcat/temp
   org.apache.catalina.startup.Bootstrap start
   root 32528 32487 0 15:53 pts/0 00:00:00 grep tom

5. Verify that Riskfort is working properly. Execute the following command:
   ps -ef | grep rf

You should see output similar to the following:

```
nobody    1960     1  0 05:29 ? 00:00:00 /usr/sbin/dnsmasq --strict-order
--bind-interfaces
--pid-file=/var/run/libvirt/network/default.pid --conf-file= --except-interface lo
--listen-address
192.168.122.1 --dhcp-range 192.168.122.2,192.168.122.254
--dhcp-leasefile=/var/lib/libvirt/dnsmasq/default.leases
--dhcp-lease-max=253--dhcp-no-override
root     21679     1  0 06:13 ?        00:00:00 /opt/CA/AdvancedAuth/sbin/arrfwatchdog
/opt/CA/AdvancedAuth/sbin/arrfserver
root     21680 21679  0 06:13 ?        00:00:00 /opt/CA/AdvancedAuth/sbin/arrfserver
root     32537 32487  0 15:53 pts/0    00:00:00 grep rf
```

6. Verify that Webfort is working properly. Execute the following command:
   ps -ef | grep wf

   You should see output similar to the following:

```
root     21718     1  0 06:13 ?        00:00:00 /opt/CA/AdvancedAuth/sbin/arwfwatchdog
/opt/CA/AdvancedAuth/sbin/arwfserver.real
root     21721 21718  0 06:13 ?        00:00:01
/opt/CA/AdvancedAuth/sbin/arwfserver.real
root     32546 32487  0 15:54 pts/0    00:00:00 grep wf
```

Secure Proxy Server Upgrade

After you upgrade the CA SiteMinder Policy Server, upgrade the CA Secure Proxy Server.

Follow these steps:

1. Verify that a backup of the /tmp/properties.sh file from the previous version exists.
2. SSH into the system to be upgraded.
3. Navigate to this directory.

   /opt/CA/saas/repo/application/

   If this directory has an upgradeBackupList.sh file, it includes a BACKUP_LIST environment variable. This variable defines files that are backed up before the upgrade and restored after the upgrade. You can add or remove file names from this list as necessary.
4. Unzip the new kit, for the system being upgraded into the root file system folder:

   cd /
   unzip –o CAM-SPS_kit-*version*.zip

5. Update the tmp/properties.sh file in the kit with information from the backup version of properties.sh:

   a. Diff the original properties.sh file and the temp/properties file by entering the following command:

      diff /serverkit/properties.sh /tmp/properties.sh

   b. Make appropriate changes to the /tmp/properties.sh file as required.

6. Run the upgrade by running the following commands:

   ```
   cd /opt/CA/saas/repo/application/
   ./appliance_local.sh   config
   ```

   Note: If your internal and external hostnames are different from SPS, set redirectrewritablehostnames="internalname.ca.com, externalname.ca.com" in /opt/CA/secure-proxy/proxy-engine/conf/server.conf.

Upgrade Verification

1. Putty to the Secure Proxy Server.
2. Enter the following command:

   ps –ef|grep httpd

   You should see a message similar to the following:

   /opt/CA/secure-proxy/httpd/bin/httpd -d /opt/CA/secure-proxy/httpd -k startssl

3. Verify you can log into a tenant environment through the Secure Proxy Server. If you cannot log into a tenant environment, restart the Secure Proxy Server as follows:

   ```
   service S98sps stop
   service S98sps startssl
   ```

Identity Management Server Upgrade

The Identity Management server is the last server that you upgrade. If you have multiple Identity Management servers, upgrade the primary server first.

Before you upgrade the Identity Management server, note the following points:

- During a role definition update, Identity Management and tenants may be inaccessible.
- Do not perform administrative updates when upgrading the Identity Management server.
- Do not upgrade the second Identity Management server until the first server completes with role definition updates.

Follow these steps:

1. SSH into the system to be upgraded.
2. Navigate to this directory.

   /opt/CA/saas/repo/application/

   If this directory has an upgradeBackupList.sh file, it includes a BACKUP_LIST environment variable. This variable defines files that are backed up before the upgrade and restored after the upgrade. You can add or remove file names from this list as necessary.
3. Verify that a backup (see page 8) of the /tmp/properties.sh file exists.
4. Unzip the new kit for the system being upgraded into the root file system folder. For example, enter the following commands:

   cd /
   unzip –o CAM-Identity Management SERVER_kit-*version*.zip
5. Compare the updated properties.sh with the version of the properties.sh file in the tmp/properties.sh file in the kit.
   a. Diff the properties.sh file that you updated and the tmp/properties file. Enter the following command:

      diff /serverkit/properties.sh /tmp/properties.sh
   b. Make appropriate changes to the backup version of properties.sh file as required.
   c. Modify the property "JAVA64_KIT" to use "jdk-6u45-linux-x64.bin" instead of "jdk-6u41-linux-x64.bin" as shown here:

      JAVA64_KIT=/*JDK-installation-directory*/jdk-6u4**5**-linux-x64.bin; export JAVA64_KIT
   d. Rename the properties starting with _oracle_schema to begin with _db_schema and use values for your database user:

      _db_schema_user=<your db user>; export _db_schema_user
      _db_schema_password=<your db user password>; export _db_schema_password
   e. Add these properties at the bottom of file:

      _oracle_schema_user=$_db_schema_user; export _oracle_schema_user
      _oracle_schema_password=$_db_schema_password ; export _oracle_schema_password
6. Run the upgrade:

   cd /opt/CA/saas/repo/application/
   ./appliance_local.sh config

Verify the upgrade:

1. Verify services are running:
   ps -ef |grep java

   JBoss and the DxAgentService should be running.

2. Verify DSA routers are running
   su – dsa
   dxserver status

   You should see XXX-cam-tenant-router started.

3. For each Identity Management server running JBOSS EAP, perform these steps:

   a. Navigate to this directory

      /opt/boss-eap-5.1.2/jboss-as/server/all/conf/props/

   b. Edit this file to uncomment the "#admin=admin" line.

      jmx-console-users.properties

4. Restart each Identity Management server using JBoss EAP. Execute these commands:

   service im stop
   service im start

5. Restart Tomcat on the Policy Server that you upgraded as follows:

   /opt/CA/AdvancedAuth/Tomcat/bin/shutdown.sh
   /opt/CA/AdvancedAuth/Tomcat/bin/startup.sh

Upgrade Tenant Backup Files

The system has a file named the **upgradeBackupList.sh.** This file contains an array of file names to back up before the upgrade, and then restored after the upgrade. If you have additional files that you want to preserve, you can add or remove file names from this list as necessary.

Follow these steps:

1. Find the variable named BACKUP_LIST, line 391 (It is an array enclosed in parenthesis).
2. Insert the filename(s) in each set of quotes separated by spaces and inside the parenthesis.

Set the Connection Type as Your JDBC Connection

Perform this procedure if SSO reports were enabled before the upgrade. After the upgrade, the Identity Management server SSO Reporting tasks are missing the JDBC connection information. To correct this, set the connection type as your JDBC connection.

The following tasks are SSO reports that you have to modify:

- SSO-Authentications by Authentication Type Report
- SSO-Unique User Authentications Detail Report
- SSO-Unique User Authentications Summary Report
- SSO-Authentications by Auth type per Application Report
- SSO-User Accesses per Application Report
- SSO-User Access Detail Report
- SSO-User Authentication Detail Report

Follow these steps:

1. Log in to the User Console as the CSP administrator.
2. Select Roles and Tasks, Admin Roles, Modify Admin Task.
3. Search for the tasks listed above.
4. Select the Search tab, and then click Browse to locate the search screen for each task. By default, the search screen will be selected in the list.
5. Edit the search screen for the report task: choose your JDBC connection under Connection Object for the Report.
6. Click Submit.

Back Up Files for the Next Upgrade

After the upgrade, back up the /tmp/properties.sh file on each server to a secure remote location. Otherwise, the next upgrade overwrites these files. You need these files for upgrades because these files contain password information.

Important! Do not create back-up versions in the **/tmp** directory, as this directory is volatile. Copy the properties.sh files to a remote system.

Back up the properties.sh file on the following servers:

- CA Directory server
- Provisioning Server
- CA IAM Connector Server
- CA SiteMinder Policy Server
- Secure Proxy Server
- Identity Management Server

Important! If you have more than one server of any type, back up the properties file on each system. For example, if you have two Directory servers, back up the properties file for each server.

Upgrade Layer 7 Gateway Server

The upgrade path for the Gateway in going from CA CloudMinder 1.5 to CA CloudMinder 1.51 requires downtime. It requires some steps to be done per cluster node and other steps to be done per existing tenant installation.

Existing tenant Gateway deployments for CA CloudMinder 1.5 are still compatible with other CA CloudMinder 1.51 deployments. Therefore, those deployments can remain unchanged if they do not need PostgreSQL support or changes to the user interface for the 1.51 release.

Use the following procedure to upgrade the Layer 7 Gateway servers.

Upgrade Each Cluster Node

These steps should be executed per cluster node. For example, in a two-node cluster, you perform these steps on each Gateway.

Follow these steps:

1. SSH onto the Gateway.
2. Stop the Gateway process as follows:

   ```
   service ssg stop
   ```

3. Remove the existing MAG RPM as follows:

   rpm –e ssg-mag-2.0-1.noarch

4. Install new MAG RPM:

   rpm –Uvh ssg-mag-cloudminder_1.51-2.0-3.noarch.rpm

5. Start the Gateway process as follows:

   service ssg start

Upgrade Each Tenant Oracle Database

Perform this procedure once per tenant deployment. However, do not repeat this procedure on each cluster node.

Follow these steps:

1. Connect to the existing CA CloudMinder Oracle database as the system user.

   For example, connect as SQL Developer.

2. Open the following file:

   oracle_oidc_upgrade_cm15_cm151.sql.sql

3. Replace all instances of <OTKDB-USERNAME> with a user name you choose.

   Choose a user name that is unique to the current tenant.

4. Save and close the file.

5. Execute the modified version of the script.

6. Click Commit.

Upgrade Each Tenant Policy Deployment

Perform this procedure once per tenant deployment. However, do not repeat this procedure on each cluster node. In the following steps, the existing prefix of the tenant is referred to as <PREFIX>.

Follow these steps:

1. SSH onto the Gateway.

2. Delete existing encapsulated assertions:

   mysql –u root –p ssg –e "delete from encapsulated_assertion where name like '<PREFIX> %'"

3. Log into the Gateway webadmin
4. Delete the existing OAuth folder if it exists as follows:
   a. Find the OAuth root installation folder with name "OAuth <PREFIX>"
   b. Right-click folder and select "Delete Folder"
   c. Confirm the deletion
5. Delete the existing MAG folder:
   a. Find the MAG root installation folder with name "MAG-2.0 <PREFIX>"
   b. Right-click folder and select "Delete Folder"
   c. Confirm the deletion
6. Follow steps for new install from SSO with CloudMinder as an OAuth Authorization Server: *Install OpenID Connect*
   a. Reuse <PREFIX> as installation prefix
   b. Point installation towards the same JDBC connection as previous install
7. Perform the following procedures from the "SSO with CloudMinder as an OAuth Authorization Server" chapter of the *SSO Getting Started Guide* in this sequence:
   - "Update the Authorize Endpoint"
   - "Update the UserInfo Endpoint"
   - "Update the Tenant Web Service Fragment"
   - "Restart Gateways"