CA CloudMinder™

Upgrade Guide

1.52

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

As the CA CloudMinder hosting administrator, you perform the upgrade procedures in the order that is used in this guide:

1. Locate Backup Files (see page 8).
2. Install the Right Hotfix (see page 8)
3. Upgrade the SiteMinder Policy Server and CSP console (see page 13).
4. Upgrade the Secure Proxy 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. The upgrade creates a copy of the applicable properties.sh file in /opt/CA/config. However, it contains no passwords. Be sure to create your own backup copy before starting the upgrade.

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 SiteMinder Policy Server
- CSP console
- Secure Proxy 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 Policy servers, back up the properties file for each server.

Install the Right 1.51 Hotfix

Before you upgrade CA CloudMinder, install the latest hotfix package that applies to CA CloudMinder 1.51. The hotfix includes support for disaster recovery. Even if you do not require this feature, each system in your installation requires the hotfix. However, actual configuration of disaster recovery is optional.

If you intend to create a disaster recovery site, you have two options:

- Configure disaster recovery using the hotfix that is supplied for CA CloudMinder 1.51 *before* you upgrade. That hotfix includes a *Disaster Recovery Guide* with complete instructions.
- Configure disaster recovery using the hotfix that is supplied for CA CloudMinder 1.52 *after* you upgrade. The CA CloudMinder 1.52 bookshelf includes a *Disaster Recovery Guide* with complete instructions.

Review the Support Matrix

Be sure that you have all the software that is identified in the Product Support Matrix for CA CloudMinder 1.52 on the main page of the bookshelf.

Product ISO Images

You receive instructions for downloading CA CloudMinder files when you receive your license.

To help ensure that the files download successfully, consider the following notes:

- Use Download Manager to download the files.
- Check the MD5SUM and size for each file after you download them.

CA CloudMinder 1.52	ISO File Name	MD5SUM	File Size
CA Business Intelligence r3.3 for Linux - DVD	DVD06213531E.iso	2276e0786505e7ad3504b3a6ca77c864	5,415,825,408
CA CloudMinder 1.52 Cloud Components (DVD 1 of 2)	DVD11092655E.iso	825cd4207f479672912a07cb4b4ba092	3,117,498,368
CA CloudMinder 1.52 Cloud Components (DVD 2 of 2)	DVD11092847E.iso	4f50a4e36196af0d396dcdd6feca0a9c	2,909,419,520
CA CloudMinder 1.52 On-premise Components	DVD11161206E.iso	216f0ebca9980336f3b6e451e489b7ad	1,784,479,744

Steps to Address OAuth Security Vulnerability

A Gateway with OAuth installed may be vulnerable to unauthorized access due to the following issues:

- OAuth SAML token grant type does not check signer of bearer token
- OAuth validation and storage endpoints do not validate TLS client certificate

Important! No known exploitations of this vulnerability have occurred at sites running the affected software.

Note: OAuth policies may be vulnerable if the SAML token grant type policy branches are present, regardless of whether they are actually used.

Affected Product Versions

Important! CA CloudMinder 1.5x must be considered affected by this vulnerability.

All currently released versions of the OAuth Toolkit and CA Mobile API Gateway are affected:

- OAuth Toolkit installed by CA API Gateway versions before 8.2
- MAG Policies installed by CA Mobile API Gateway versions before 2.2

CA CloudMinder1.5x uses a Gateway version 7.1 with MAG version 2.0.1.

Solution

A two-part solution exists, involving the following components:

- OAuth SAML Token Grant Type
- Validation with Storage Endpoints

OAuth SAML Token Grant Type

The Gateway in CA CloudMinder 1.5x does not utilize the SAML grant type. Therefore, you add a "Stop Processing" assertion at the top of a specific policy to ensure that the vulnerable policy branch is never successfully executed.

Perform the following steps for each tenant:

1. In the Gateway Policy Manager or webadmin, open the policy that is named: **<PREFIX> MAG-<version>/Policy Fragments/grant_types/OTK grant_type=SAML**
2. Disable support for the SAML Token grant type by inserting a "**Stop Processing**" assertion at the top of the policy.
3. Save and activate the changes.

Validation with Storage Endpoints

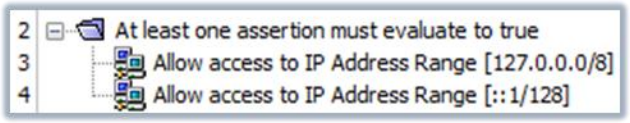
The Gateway in CA CloudMinder 1.5x uses some of the storage and validation endpoints that are affected by the vulnerability of lacking TLS certificate validation. Because the endpoints in question only need to be accessible by the Gateway itself, you can mitigate the vulnerability by only allowing local access.

Perform the following steps for each tenant:

1. Copy the following policy XML snippet from this document:

```
<?xml version="1.0" encoding="UTF-8"?>
<wsp:Policy xmlns:L7p="http://www.layer7tech.com/ws/policy"
xmlns:wsp="http://schemas.xmlsoap.org/ws/2002/12/policy">
    <wsp:All wsp:Usage="Required">
        <wsp:OneOrMore wsp:Usage="Required">
            <L7p:RemoteIpAddressRange>
                <L7p:NetworkMask intValue="8"/>
                <L7p:StartIp stringValue="127.0.0.0"/>
            </L7p:RemoteIpAddressRange>
            <L7p:RemoteIpAddressRange>
                <L7p:NetworkMask intValue="128"/>
                <L7p:StartIp stringValue="::1"/>
            </L7p:RemoteIpAddressRange>
        </wsp:OneOrMore>
    </wsp:All>
</wsp:Policy>
```

2. Search for endpoints within the folder "SecureZone - OVP":
    a. /oauth/validation/v2/client
    b. /oauth/validation/validate/v2/refreshtoken
    c. /oauth/validation/validate/v2/token
    d. /oauth/validation/validate/v2/idtoken
3. Search for endpoints within the folder "SecureZone - Storage":
    a. /oauth/clientstore/*
    b. /oauth/tokenstore/*
    c. /oauth/session/*
4. Within each policy, paste the snippet into the top of the policy. Look for results that are similar to the following graphic:



5. Save and then activate the modified policy.

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. CA SiteMinder Policy Server
2. CSP console
3. Secure Proxy Server

Note: When you have a primary and secondary server, upgrade the primary server first. Then upgrade the Disaster Recovery (DR) site, if you have a DR site.

Policy Server and CSP Console Upgrade

The upgrade of the SiteMinder Policy Server and the CSP console are very similar. The following procedures call out the steps that are needed for only one system.

If you are upgrading a Disaster Recovery site, two extra procedures are included. Perform these procedures in addition to the other procedures.

Policy Server and CSP Console Prerequisites

Repeat these steps to upgrade each SiteMinder Policy Server and the CSP console. These steps identical if you are upgrading a Disaster Recovery site.

Follow these steps:

1. SSH into the system to be upgraded.
2. Install the 32-bit version of the libXrender.so.1 Linux package.
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. Verify that a backup (see page 8) of the /tmp/properties.sh file from the previous version exists. The properties.sh file is replaced when you unzip the kit. Therefore, make a backup now if no backup copy exists.
5. Unzip the Policy Server kit into the root file system folder. For example:

   ```
   cd /
   unzip –o CAM-SMPS_kit-version.zip
   ```
6. Copy the following kits to /root directory.
   - jdk-7u40-linux-x64.tar.gz
   - jdk-7u40-linux-i586.tar.gz
   - UnlimitedJCEPolicyJDK7.zip
   - JBPAPP-8693.zip (If you are using the EAP version of JBoss).
7. If you are following this procedure to upgrade the CSP console, copy the following kit to the /root directory:
   `jboss-eap-5.1.2.zip`
8. 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.sh file by entering the following command:

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

   b. Modify the following properties to match the following lines:

      ```
      JAVA64_KIT=/root/jdk-7u40-linux-x64.tar.gz; export
      JAVA64_KIT
      JAVA32_KIT=/root/jdk-7u40-linux-i586.tar.gz; export
      JAVA32_KIT
      _jce_zip_file=/root/UnlimitedJCEPolicyJDK7.zip; export
      _jce_zip_file
      ```

c. Add the following property:
```
JBOSS_EAP_PATCH="/root/JBPAPP-8693.zip"; export
JBOSS_EAP_PATCH
```

d. If you are following this procedure to upgrade the CSP console, add one more property:

```
JBOSS_KIT="/root/jboss-eap-5.1.2.zip"; export JBOSS_KIT
```

e. Define _ps_ha_hosts.

For a high-availability deployment, do not include the host name on which you are currently installing. Enter the host name where you installed the first SiteMinder Policy Server.

Note: If you have three or more instances of SiteMinder Policy Server, separate the entries with commas. For example: PolicyServer2, PolicyServer3.

If you configured load balancing for the Policy Server at the application tier, set _ps_ha_hosts to the Policy Server load balancer VIP.

Additional Disaster Recovery Prerequisites

You upgrade systems at the Disaster Recovery (DR) site while the Primary site remains active.

- When you start the DR site upgrade, verify that database and systems at the DR site are in standby mode.
- Disable all traffic to the Secure Proxy Server.

Policy Server and CSP console Prerequisites

1. Perform all steps in the prerequisite procedure (see page 13).
2. Verify that the following properties are defined as follows in /tmp/properties.sh.

```
_db_server=Primary-Database-Hostname; export _db_server
_database_name=Primary-Database-Name; export _database_name
_ps_ha_hosts=<SMPS LB VIP>; export _ps_ha_hosts
```

3. Add the following property if you are using this procedure to upgrade the CSP console and using JBOSS EAP:

```
JBOSS_EAP_PATCH=; export JBOSS_EAP_PATCH
```

4. Verify that the following properties are set to reference the Primary database information in the following file:

/opt/CA/siteminder/install_config_info/ca-ps-installer.properties

- DEFAULT_RDB_DBSERVER=*Primary-Database-Hostname*
- DEFAULT_RDB_DBNAME=*Primary-Database-Name*

Additional CSP console Prerequisites

1. Copy the following kits to the /root directory.

   `JBPAPP-8693.zip`

2. Verify that the following properties are in the /tmp/properties.sh file.

   `_ps_ha_hosts=<SMPS LB VIP>; export _ps_ha_hosts`

3. Add the following property to the /tmp/properties.sh file.

   `JBOSS_EAP_PATCH="/root/JBPAPP-8693.zip"; export JBOSS_EAP_PATCH`

4. Edit the following file to point to HostName and ServiceName of the primary database.

   `/opt/CA/siteminder/db/system_odbc.ini`

Additional Policy Server Prerequisites

1. Verify that the following properties are set to reference the Primary database information in the following file:

   /opt/CA/AdvancedAuth/Uninstall_Advanced Authentication Server/installvariables.properties

   `TWS_IMDB_HOST=`*`Primary-Database-Hostname`*
   `TWS_IMDB_DBNAME=`*`Primary-Database-Name`*
   `ARCOT_PRIMARY_HOST_NAME=`*`Primary-Database-Hostname`*
   `ARCOT_PRIMARYDB_URL=jdbc\:oracle\:thin\:@//`*`Primary-Database-Hostname`*`\:1521/`*`Primary-Database-Name`*
   `ARCOT_PRIMARY_SERVICE_NAME=`*`Primary-Database-Name`*

2. Verify that the following properties are set to reference the Primary database info in the following file:

   /opt/CA/AdvancedAuth/Uninstall_Arcot WebFort/installvariables.properties

   `TWS_IMDB_HOST=`*`Primary-Database-Hostname`*
   `TWS_IMDB_DBNAME=`*`Primary-Database-Name`*
   `ARCOT_PRIMARY_SERVICE_NAME=`*`Primary-Database-Name`*

3. Edit the following files to point to the primary database:

   - /opt/CA/AdvancedAuth/conf/arcotcommon.ini
   - /opt/CA/AdvancedAuth/Tomcat/conf/context.xml
   - /opt/CA/AdvancedAuth/Tomcat/webapps/tenant-services/META-INF/context.xml
   - /opt/CA/AdvancedAuth/odbc32v70wf/odbc.ini
   - /opt/CA/siteminder/db/system_odbc.ini

4. Set DR mode to live.

```
cd /opt/CA/saas/repo/application
./DR_mode.sh mode=live
```

Perform the Upgrade

Once you have met the prerequisite steps, perform the upgrade.

Follow these steps:

1. Perform all steps in the prerequisite procedure (see page 13).
2. If you are upgrading a DR site, perform all steps in the Disaster Recovery Site Prerequisites (see page 15).
3. **Before the next step, be sure that you unset the DISPLAY variable.**

   Important! Unless you unset the DISPLAY variable, the environment will be corrupted.
4. Run the upgrade by entering the following commands:

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

5. Restart all Policy Server services on all systems with the Policy Server.

   Repeat this step at the Disaster Recovery site if you have one.

Verify the Policy Server Upgrade

Follow these steps:

1. Verify dxserver status by entering these commands:

```
su – dsa
dxserver status
```

   You should see a *XXXXX-tenant-router* started message for each tenant.
2. Verify that the Policy server is working properly by entering this 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.ja
r 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
```

Verify the CSP console Upgrade

Follow these steps:

1. Verify dxserver status by entering these commands:
   ```
   su – dsa
   dxserver status
   ```
   You should see a *XXXXX-tenant-router* started message for each tenant.
2. Log in to the CSP console
3. Verify that the tenant and container tasks are visible.

Tomcat Configuration

After you upgrade the Policy Server, Tomcat may start temporarily then fail. If it fails, use this procedure.

Follow these steps:

1. Navigate to the following directory:

   ```
   /opt/CA/AdvancedAuth/Tomcat/webapps/tenant-services/WEB-INF/cla
   sses/resources
   ```

2. Edith the following file:

   `config.properties`

3. Change IM_WEBSERVICE_HOST as follows:

   - If you just upgraded the first Policy Server, set it to the host of the first Identity Management server.
   - if you just upgraded the second Policy Server, set it to the host of the second Identity Management server.
   - If you are using load balancing at the application tier, set it to the Identity Management server VIP.

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
   ```

Modify DefaultHostSettings

The Host Configuration Object may have a Policy Server with the following name: <IPAddress>

Follow these steps:

1. Start the CSP console.
2. Select Infrastructure, Hosts, Host Configuration Object, Modify Host Configuration Object.
3. If you see <IPAddress> as a host in the Policy Server table, delete that row.

Set the Registry for the Policy Server

Follow these steps:

1. To enable audit logging for CA CloudMinder, edit the sm.registry file. The default location of this file is:
   `Siteminder_home\registry`
2. Set the value of **LogCloudMinder** in the registry to **1**.
3. Set the value of **Enable Enhance Tracing** to **3**.

   You can use the XPSConfig utility to set these registry entries.

Secure Proxy Server Upgrade

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

Follow these steps:

1. SSH into the system to be upgraded.
2. Become the root user:

   ```
   su -root
   ```

3. Install the 32-bit version of the libkeyutils.so.1 library.
4. Verify that a backup (see page 8) of the /tmp/properties.sh file from the previous version exists. The properties.sh file is replaced when you unzip the kit. Therefore, make a backup now if no backup copy exists.
5. 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.
6. Unzip the new kit, for the system being upgraded into the root file system folder:

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

7. Copy the following Kits to the /root directory:
   - jdk-7u40-linux-x64.tar.gz
   - jdk-7u40-linux-i586.tar.gz
   - UnlimitedJCEPolicyJDK7.zip
8. 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.

c. Modify the following properties in /tmp/properties.sh to match the following lines:

```
JAVA64_KIT=/root/jdk-7u40-linux-x64.tar.gz; export
JAVA64_KIT
JAVA32_KIT=/root/jdk-7u40-linux-i586.tar.gz; export
JAVA32_KIT
_jce_zip_file=/root/UnlimitedJCEPolicyJDK7.zip; export
_jce_zip_file
```

9. If you are upgrading a system at a disaster recovery site, set DR mode to live as follows:

```
/opt/CA/saas/repo/application/DR_mode.sh mode=live
```

10. Run the upgrade by executing the following commands:

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

Update the SSL Version

Follow these steps:

1. Navigate to this location:

```
/opt/CA/secure-proxy/httpd/conf/extra
```

2. Check if the /httpd-ssl.conf file has the SSLProtocol defined.
3. If the SSLProtocol does not support SSLv3, navigate to this location:

```
/opt/CA/secure-proxy/proxy-engine/conf/server.conf
```

4. Open the server.conf file.
5. Check the versions tag under the sslparams tag.

   If the versions tag is set to SSLv3, replace it as follows:

```
versions="TLSv1"'
```

6. Restart the Secure Proxy Server.

Update Oauth

If you have created copies of oauth.jsp, openid.jsp, or forms.jsp, the installer will not upgrade those copies. Some administrators use copies of oauth.jsp as Resource Filters for the realm to redirect to the launch url of the application. CA CloudMinder has changed the implementation of oauth.jsp, openid.jsp, and forms.jsp. Therefore, you cannot access the User Console when logging in with an authmethod if the corresponding CA SiteMinder realm uses a copy of these JSPs as a resource filter.

This problem can be solved in one of two ways:

- **Change the realms**: Change the resource filter of the affected realms to `/chs/redirect/<tenantname>/<uniqueNameToIdentifyTheRealm>`

  For example, if the tenant name is Forwardinc, and the realm is used to authenticate users with Facebook, the new resource filter for the realm could be: `/chs/redirect/forwardinc/facebook`

- **Keep the realms intact**: Delete the existing copies of the files, and then create new copies. See the following procedure.

Keeping the realms intact

If you support a tenant that is using Oauth, perform these steps on each Secure Proxy Server:

1. Change to the redirectjsp directory:

   ```
   cd
   /opt/CA/secure-proxy/Tomcat/webapps/affwebservices/redirectjsp
   ```

2. Back up the existing App/Tenant specific oauth.jsp files. For example:

   ```
   mv oauth-google.jsp oauth-google.jsp.orig
   mv oauth-facebook.jsp oauth-facebook.jsp.orig
   ```

3. Replace the App/Tenant oauth files with the new oauth.jsp file that came with upgrade.

   ```
   cp oauth.jsp oauth-google.jsp
   cp oauth.jsp oauth-facebook.jsp
   ```

4. Update the oauth.jsp file.

   If your external and internal hostnames are different for your Secure Proxy Server system, edit the server.conf file on the Secure Proxy Server system. Change this file to list both the internal and external hostnames for redirects.

   a. Edit opt/CA/secure-proxy/proxy-engine/conf/server.conf

   b. Change the line which reads:

      ```
      redirectrewritablehostnames=<internal hostname>
      ```

      Replace this line with the following line:

      ```
      redirectrewritablehostnames=<internal hostname, external
      hostname>
      ```

5. Restart the Secure Proxy Server as follows:

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

Proxy UI for the Secure Proxy Server

This procedure enables the CSP administrator to access the proxy UI.

Follow these steps:

1. Log in to the CSP console.
2. Navigate to policies, Domain, Domains and edit domain DOMAIN-SPSADMINUI-cam-agent
3. Add the following user directory on the General tab:

   `cacsp Directory`
4. Click Submit.
5. Navigate to policies, Domain, Domains and edit domain DOMAIN-SPSADMINUI-cam-agent
6. Navigate to Policies and edit "POLICY-SPSADMINUI-cam-agent. Make these changes on the Users tab.
   a. Add users and Add All.
   b. Click Ok and Submit.

The Proxy UI can be accessed from following URLs:

- https://*Primary SPS Hostname*:8443/proxyui/
- https://*Secondary SPS Hostname*:8443/proxyui/

Sign Out from the ProxyUI

Use the procedure to enable signout from the Proxy UI.

Follow these steps:

1. Log in to the CSP console.
2. Navigate to Infrastructure, Agent, Agent configuration Object.
3. Edit CAM-AgentObj as follows:
   a. Edit parameter LogoffUri
   b. In the Edit parameter, click Add and enter this value: `/proxyui/logout.jsf`
   c. Click OK and then Submit.
   d. Clear the cache.

Verify the Secure Proxy Server Upgrade

Follow these steps:

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
   ```

Disaster Recovery Site Post-Upgrade

The following steps are required only at a Disaster Recovery site.

Secure Proxy Server

Set the DR mode back to standby.

```
cd /opt/CA/saas/repo/application/
./DR_mode.sh mode=standby
```

CSP console

1. Set the DR mode back to standby:

   ```
   cd /opt/CA/saas/repo/application
   ./DR_mode.sh mode=standby
   ```
2. Edit the following file to point to HostName and ServiceName of the standby database.

   ```
   /opt/CA/siteminder/db/system_odbc.ini
   ```

Policy Server

1. Set the DR mode back to standby.

   ```
   cd /opt/CA/saas/repo/application/
   ./DR_mode.sh mode=standby
   ```

2. Edit the following files to point to HostName and ServiceName of the standby database.
   - /opt/CA/AdvancedAuth/conf/arcotcommon.ini
   - /opt/CA/AdvancedAuth/Tomcat/conf/context.xml
   - /opt/CA/AdvancedAuth/Tomcat/webapps/tenant-services/META-INF/context.xml
   - /opt/CA/AdvancedAuth/odbc32v70wf/odbc.ini
   - /opt/CA/siteminder/db/system_odbc.ini

Load Balancer

Enable Secure Proxy Server node to be able to receive traffic when failover to the DR site occurs

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. The upgrade creates a backup copy of the properties.sh files without passwords in /opt/CA/config.

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 SiteMinder Policy Server
- CSP console
- Secure Proxy 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.

Install the Right 1.52 Hotfix

After you upgrade CA CloudMinder, install the latest hotfix package that applies to CA CloudMinder 1.52.

The hotfix includes support for disaster recovery. Even if you do not require this feature, each system in your installation requires the hotfix. However, actual configuration of disaster recovery is optional. The CA CloudMinder 1.52 bookshelf includes a *Disaster Recovery Guide* with complete configuration instructions.