CA CloudMinder™

Upgrade Guide

1.53

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 7

Overview of Upgrade Steps 7
Locate Backup Files 8
Review the Support Matrix 8
Product ISO Images 9
Steps to Address OAuth Security Vulnerability 9

Chapter 2: Upgrade Procedures 13

Review the Upgrade Order 13
CA Directory Upgrade 13
Provisioning Server and CA IAM Connector Server Upgrade 15
MSGMNI kernel Installation Error 16
Policy Server and CSP Console Upgrade 17
Policy Server and CSP Console Prerequisites 17
Additional Disaster Recovery Prerequisites 18
Perform the Upgrade 20
Verify the Policy Server Upgrade 21
Verify the CSP console Upgrade 22
Tomcat Configuration 22
Modify DefaultHostSettings 23
Set the Registry for the Policy Server 23
Update the SiteMinder Realm for the Tenant 23
Secure Proxy Server Upgrade 24
Update the SSL Version 25
Proxy UI for the Secure Proxy Server 26
Sign Out from the ProxyUI 26
Verify the Secure Proxy Server Upgrade 27
Identity Management Server Upgrade 27
Upgrade Tenant Backup Files 29
Set the Connection Type as Your JDBC Connection 30
Disaster Recovery Site Post-Upgrade 31
Back Up Files for the Next Upgrade 32
Update Tenants 33

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 (see page 7)
Locate Backup Files (see page 8)
Review the Support Matrix (see page 8)
Product ISO Images (see page 9)
Steps to Address OAuth Security Vulnerability (see page 9)

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. Upgrade CA Directory. (see page 13)
3. Upgrade the Provisioning Server and CA IAM Connector Server (see page 15).
4. Upgrade the SiteMinder Policy Server and CSP console (see page 17).
5. Upgrade the Secure Proxy Server. (see page 24)
6. Upgrade the Identity Management Server. (see page 27)

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 Directory Server
- Provisioning Server
- CA SiteMinder Policy Server
- CSP console
- 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 Policy servers, back up the properties file for each server.

Review the Support Matrix

Be sure that you have all the software that is identified in the Product Support Matrix 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 1.53	ISO File Name	MD5SUM	File Size
CA Business Intelligence r3.3 for Linux - DVD	DVD06213531E.iso	2276e0786505e7ad3504b3a6ca77c864	5,415,825,408
CA Business Intelligence for Linux r3.3 SP2 - DVD This version is required for Oracle 12c.	DVD02122155E.ISO	6888bce2f7fc7756a9187ce5cb70cb5d	1,556,060,160
CA CloudMinder 1.53 Cloud Components (DVD 1 of 2)	DVD02182624E.ISO	e9d54f7ea2ddff4143f1ab6f0e12472a	2,997,401,600
CA CloudMinder 1.53 Cloud Components (DVD 2 of 2)	DVD02182714E.ISO	d3863ed724c085e8b1284977a5027559	2,921,121,792
CA CloudMinder 1.53 On-premise Components	DVD02182827E.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

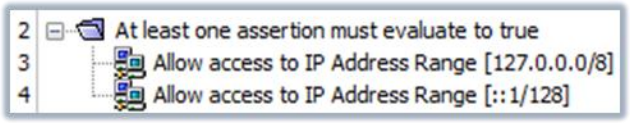
The Gateway in CA CloudMinder 1.5x uses some of the storage and validation endpoints that are affected by the vulnerability of lacking TLS certificate validation. Because the endpoints in question only need to be accessible by the Gateway itself, you can mitigate the vulnerability by only allowing local 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 (see page 13)
CA Directory Upgrade (see page 13)
Provisioning Server and CA IAM Connector Server Upgrade (see page 15)
Policy Server and CSP Console Upgrade (see page 17)
Secure Proxy Server Upgrade (see page 24)
Identity Management Server Upgrade (see page 27)
Disaster Recovery Site Post-Upgrade (see page 31)
Back Up Files for the Next Upgrade (see page 32)
Update Tenants (see page 33)

Review the Upgrade Order

Once you have located your backup files, 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 Directory
2. Provisioning Server and CA IAM Connector Server
3. CA SiteMinder Policy Server
4. CSP console
5. Secure Proxy Server
6. Identity Management 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.

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-7u40-linux-x64.tar.gz" instead of "jdk-6u45-linux-x64.bin" as in this example:

JAVA64_KIT=/*JDK-Installation-Directory*/jdk-7u40-linux-x64.tar.gz; export JAVA64_KIT

1. 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-7u40-linux-x64.tar.gz" instead of "jdk-6u45-linux-x64.bin" as shown in this example:

      JAVA64_KIT=/JDK-installation-directory/jdk-7u40-linux-x64.tar.gz; 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.

MSGMNI kernel Installation Error

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

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. If you are using JBOSS 5.1.2 EAP, download JBPAPP-8693.zip from the JBoss site. Enter the location of the ZIP file followed by an export command. For example:
      `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 17).
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 17).
2. If you are upgrading a DR site, perform all steps in the Disaster Recovery Site Prerequisites (see page 18).
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/classes/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.

Update the SiteMinder Realm for the Tenant

Follow these steps:

1. Log in to the CSP console
2. Click Policies, Domain, Domains.
3. Select *tenant*Domain.
4. Go to the Realms tab.
5. Modify realm *tenant*_chsforms_realm_es.
6. Locate the Persistent Session option under Session.
7. Select to enable Persistent Session.
8. Click Ok and then Submit.

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
```

d. Make sure the existing cert and key values are in the properties file so that the cert and key files are used; otherwise, new values are generated.

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.

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
   ```

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. Export the directory and environment to XML for each tenant environment.

   Important! You need the XML files in case you have modified any default roles, task, or screens. These items are overwritten during the upgrade.
5. 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
   ```
6. 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 _jce_zip_file property to the full file path to the JCE policy zip file. You download the UnlimitedJCEPolicyJDK7.zip file from the Oracle web site.
   d. Modify the property "JAVA64_KIT" to use "jdk-7u40-linux-x64.tar.gz" instead of "jdk-6u45-linux-x64.bin" as shown here:

      JAVA64_KIT=/JDK-installation-directory/jdk-7u40-linux-x64.tar.gz; export JAVA64_KIT
   e. If you are using JBOSS 5.1.2 EAP, download JBPAPP-8693.zip from the JBoss site. Enter the location of the ZIP file followed by an export command. For example:

      JBOSS_EAP_PATCH="/root/JBPAPP-8693.zip"; export JBOSS_EAP_PATCH
   f. 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
      ```
   g. 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
      ```
7. Run the upgrade:

   ```
   cd /opt/CA/saas/repo/application/
   ./appliance_local.sh   config
   ```
8. Reimport the directory and environment XML files that you backed up.

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.

Disaster Recovery Site Post-Upgrade

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

Identity Manager Server

1. Set the DR mode back to standby as follows:

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

2. Edit the following files to point to the HostName and ServiceName of the standby database.

   - jbosshome/server/all/deploy/iam_im_imtaskpersistencedb-ds.xml
   - jbosshome/server/all/deploy/iam_im_reportsnapshot-ds.xml
   - jbosshome/server/all/deploy/iam_im_objectstore-ds.xml
   - jbosshome/server/all/deploy/iam_im_imarchivedb-ds.xml
   - jbosshome/server/all/deploy/iam_im_imauditdb-ds.xml
   - jbosshome/server/all/deploy/iam_im_imworkflowdb-ds.xml
   - jbosshome/server/all/deploy/iam_im_webfort-ds.xml

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 Directory
- Provisioning Server and CA IAM Connector Server
- CA SiteMinder Policy Server
- CSP console
- Secure Proxy Server
- Identity Management

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.

Update Tenants

For this release, set the User Type value should be set to Business/Consumer/System type for use by directory synchronization.

Follow these steps:

1. Log into the management console as cspadmin.
2. Export the tenant directory.xml.
3. Edit the exported XML.

   Search for the following section:

   ```
   <ImsManagedObjectAttr physicalname="camUserType"
   description="User Type" displayname="User Type"
   valuetype="String" wellknown="%USER_TYPE%" maxlength="0"
   hidden="true" system="true">
   ```
4. Insert required="true" preceding the wellknown parameter=%USER_TYPE% parameter as follows::

   ```
   <ImsManagedObjectAttr physicalname="camUserType"
   description="User Type" displayname="User Type"
   valuetype="String" required="true" wellknown="%USER_TYPE%"
   maxlength="0" hidden="true" system="true">
   ```
5. Import the edit XML file.
6. Set the User Type attribute in the On-Premise JCS Directory Synchronization, AD Template Configured, Attributes section.
7. Perform Directory Synchronization.
8. Restart the environment.

The value of User Type is defined as follows:

- 0 -- Business User
- 1 -- Consumer
- 2 -- System
- Other values -- Business user