CA CloudMinder™

Upgrade Guide

1.5

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: How to Upgrade CA CloudMinder 7

Overview of Upgrade Steps 8
Make Sure You Have Backup Files from Previous Installations or Upgrades 9
Back Up User Tasks 10
Identify the Upgrade Order for Your Environment 10
- High Availability Installations with the Provisioning Server and CA IAM Connector Server on the Same System 11
- High Availability Installations with the Provisioning Server and CA IAM Connector Server on Different Systems 12
- Non High Availability Installations with the Provisioning Server and CA IAM Connector Server on the Same System 12
- Non High Availability Installations with Provisioning Server and CA IAM Connector Server on Different Systems 13

Upgrade CA Directory 13
Upgrade the CA Provisioning Server and CA IAM Connector Server 14
- Provisioning Server Troubleshooting 16

Upgrade the CA SiteMinder Policy Server and CSP console 16
- Troubleshooting: CA SiteMinder Installation Fails 18
- Troubleshooting: Audit Logs Get Reset to Use the Filesystem instead of the Database 19

Upgrade the CA Secure Proxy Server 19
Upgrade the CA Identity Management Server 21
- Upgrade Tenant Backup Files 22
- Session Cookies May Allow Authentication After Log Off 22
- Set the Connection Type as Your JDBC Connection 23

Back Up Your /tmp/properties.sh Files to a Secure Location For the Next Upgrade 24
High-Availability: Layer 7 Gateway Server 25
- Deploy the First Gateway 25
- Deploy the Second Gateway 28
- Configure Gateway Database Replication 31
- Create an Internal Database 32
- Configure the Gateway One Database 33
- Configure the Gateway Two Database 34
- Harden the Gateway Servers 36
- Install Mobile Access Gateways (MAG) and Siteminder Assertion Packages 37
- Install the Layer 7 License File 38
- Import the Certificate for the Gateway 39
- Create Cluster Property: siteminder12.agent.configuration 40
- Create Cluster Property: token.salt 41

Restart Gateways 42
Update Load Balancer Ports 42

Chapter 1: How to Upgrade CA CloudMinder

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

Important! Note the following information before you begin the upgrade process:

- You upgrade each machine in your CA CloudMinder deployment in a specific order. See Identify the Upgrade Order for Your Environment (see page 10).
- The upgrade automatically updates the role definition files, which determine the roles and tasks that are available in a tenant environment. The role definition upgrade affects all tenants.
- You must back up all tasks in the User Console before starting the upgrade.

This section contains the following topics:

Overview of Upgrade Steps (see page 8)
Make Sure You Have Backup Files from Previous Installations or Upgrades (see page 9)
Back Up User Tasks (see page 10)
Identify the Upgrade Order for Your Environment (see page 10)
Upgrade CA Directory (see page 13)
Upgrade the CA Provisioning Server and CA IAM Connector Server (see page 14)
Upgrade the CA SiteMinder Policy Server and CSP console (see page 16)
Upgrade the CA Secure Proxy Server (see page 19)
Upgrade the CA Identity Management Server (see page 21)
Back Up Your /tmp/properties.sh Files to a Secure Location For the Next Upgrade (see page 24)
High-Availability: Layer 7 Gateway Server (see page 25)
Update Load Balancer Ports (see page 42)

Overview of Upgrade Steps

As a CA CloudMinder hosting administrator, you upgrade each server in your deployment. Follow this process:

1. Back Up Files (see page 9).
2. Back Up User Tasks (see page 10).
3. Identify the Upgrade Order for Your Environment (see page 10).
4. Upgrade CA Directory. (see page 13)
5. Upgrade the CA Provisioning Server and the CA IAM Connector Server. (see page 14)
6. Upgrade the CA SiteMinder Policy Server and CSP console (see page 16).
7. Upgrade the CA Secure Proxy Server. (see page 19)
8. Upgrade the Identity Management Server. (see page 21)

Make Sure You Have Backup Files from Previous Installations or Upgrades

Important! After completing the initial installation of CloudMinder, you must back up the file /tmp/properties.sh file on each server component to a secure location. You need this file for future upgrades because this file contains password information. If you do not have this file backed up from a previous installation or upgrade, you cannot proceed with new upgrades.

Make sure to back up the **properties.sh** file from the **/tmp** directory immediately after your initial installation.

The upgrade overwrites these files. After you update the servers in the environment, you use the backup versions of the files to complete the upgrade.

Important! Do not create back-up versions in the /tmp directory, as this directory is volatile. Copy the properties.sh files from your prior installation to each server. In the example below, replace **/tmp** with the location of your secure backup.

The following procedure places back up files in a serverkit directory.

Follow these steps:

1. On each CA Directory server system, enter the following commands:

   ```
   mkdir /serverkit
   ```

   ```
   cp /tmp/properties.sh /serverkit
   ```

2. On each Provisioning Server and CA IAM Connector Server system, enter the following commands:

   ```
   mkdir /serverkit
   ```

   ```
   cp /tmp/properties.sh /serverkit
   ```

3. On each CA SiteMinder Policy Server, enter the following commands to back up the properties file:

   ```
   /tmp/properties.sh
   ```

   ```
   mkdir /serverkit
   ```

4. On each SPS system, enter the following commands:

   ```
   /tmp/properties.sh
   ```

   ```
   mkdir /serverkit
   ```

   ```
   cp /tmp/properites.sh /serverkit
   ```

5. On each Identity Management server, enter the following commands:

   ```
   mkdir /serverkit
   ```

   ```
   cp /tmp/properites.sh /serverkit
   ```

Important! If there is more than one server of each type, back up each properties file on each system. For example, if you have two Directory servers, you must back up each, separate properties file under a unique name and move them to the serverkit folder.

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.

Note: When you import a previously exported environment, Identity Management displays a log in a status window in the Management Console. To see validation and deployment information for each managed object and its attributes in this log, select the Enable Verbose Log Output field on the Environment Properties page before you export the environment. Selecting the Enable Verbose Log Output field can cause significant performance issues during the import.

Follow these steps:

1. Click Environments in the Management Console.
2. Select the environment that you want to export.
3. Click the Export button.
4. Save the ZIP file to a location that is accessible to the production system.
5. Click Finish.

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

Identify the Upgrade Order for Your Environment

You upgrade each server in a CA CloudMinder environment in a specific order. Review the section that most closely matches your environment before you upgrade any servers.

High Availability Installations with the Provisioning Server and CA IAM Connector Server on the Same System

If your CA CloudMinder installation includes high availability, *and* the Provisioning Server and CA IAM Connector Server are installed on the same system, upgrade servers in the following order:

1. Primary CA Directory server.
2. Secondary CA Directory server.
3. Primary Provisioning Server.
4. Secondary Provisioning Server.
5. Primary CA SiteMinder Policy Server.
6. Secondary CA SiteMinder Policy Server.
7. The Cloud Service Provider Console (if the Console is not already installed on the same server as the CA SiteMinder Policy Server.)
8. Primary CA Secure Proxy Server.
9. Secondary CA Secure Proxy Server.
10. Primary Identity Management server.
11. Secondary Identity Management server.

High Availability Installations with the Provisioning Server and CA IAM Connector Server on Different Systems

If your CA CloudMinder installation includes high availability, *and* the Provisioning Server and CA IAM Connector Server are installed on different systems, upgrade servers in the following order:

1. Primary CA Directory server.
2. Secondary CA Directory server.
3. Primary CA Provisioning Server.
4. Secondary CA Provisioning Server.
5. Primary CA IAM Connector Server.
6. Secondary CA IAM Connector Server.
7. Primary CA SiteMinder Policy Server.
8. Secondary CA SiteMinder Policy Server.
9. The Cloud Service Provider Console (if the Console is not already installed on the same server as the SiteMinder Policy Server.)
10. Primary CA Secure Proxy Server.
11. Secondary CA Secure Proxy Server.
12. Primary Identity Management server.
13. Secondary Identity Management server.

Non High Availability Installations with the Provisioning Server and CA IAM Connector Server on the Same System

If your CA CloudMinder installation does not include high availability, *and* the Provisioning Server and CA IAM Connector Server are installed on the same system, upgrade servers in the following order:

1. CA Directory server.
2. CA Provisioning Server.
3. CA SiteMinder Policy Server.
4. The CSP Console (if the Console is not already installed on the same server as the SiteMinder Policy Server.)
5. Secure Proxy Server.
6. Identity Management server.

Non High Availability Installations with Provisioning Server and CA IAM Connector Server on Different Systems

If your CA CloudMinder installation does not include high availability, *and* the Provisioning Server and CA IAM Connector Server are installed on different systems, upgrade servers in the following order:

1. CA Directory server.
2. CA Provisioning Server.
3. CA IAM Connector Server.
4. CA SiteMinder Policy Server.
5. The Cloud Server Provider Console (if the Console is not already installed on the same server as the CA SiteMinder Policy Server.)
6. CA Secure Proxy Server.
7. Identity Management server.

Upgrade CA Directory

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 machine to be upgraded.
2. Verify that a backup (see page 9) of the /tmp/properties.sh file from the previous version exists.
3. Unzip the new kit for the machine being upgraded into the root file system folder. For example, enter the following commands:

   ```
   cd /
   ```

   ```
   unzip –o CAM-DIR_kit-version.zip
   ```

4. Update the /tmp/properties.sh file in the kit with information from the backup version of properties.sh:
   a. Diff the back file of the previous install and /tmp/properties.sh by entering the following command:

      Note: The following command assumes backup files are located in the /serverkit folder.

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

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

5. Run the upgrade by entering the following commands:

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

   Note: If this directory has a file named upgradeBackupList.sh, it will have an environment variable named BACKUP_LIST. This variable is an array of file names that will be backed up before the upgrade, and then restored after the upgrade. You may add or remove file names from this list as necessary.

Verify the upgrade:

Verify All DSA's are running by entering the following commands:

```
su – dsa
dxserver status
exit
```

Upgrade the CA Provisioning Server and CA IAM Connector Server

After you upgrade the CA Directory server, upgrade the CA Provisioning Server and CA IAM Connector Server. If the Provisioning Server and CA IAM Connector Server are running on the same system, running the upgrade will upgrade both components. If the Provisioning Server and CA IAM Connector Server are installed on separate systems, upgrade the Provisioning Server system before you upgrade CA IAM Connector Server.

Follow these steps:

1. SSH into the machine to be upgraded.
2. Verify that a backup (see page 9) of the /tmp/properties.sh file from the previous version exists.
3. Enter the following commands:

   ```
   su - root
   mv /dev/random /dev/random.orig
   ln -s /dev/urandom /dev/random
   ```

4. Unzip the new kit for the machine 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.

6. Run the upgrade by entering the following commands:

   Note: If this directory has a file named upgradeBackupList.sh, it will have an environment variable named BACKUP_LIST. This variable is an array of file names that will be backed up before the upgrade, and then restored after the upgrade. You may add or remove file names from this list as necessary.

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

   Note: Verify the soft link exists:

   ```
   mv /dev/random /dev/random.orig
   ln -s /dev/urandom /dev/random
   ```

Verify the upgrade:

1. Verify that all DSAs are running:

   ```
   su – dsa
   dxserver status
   ```

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

2. Verify that the Provisioning Server is running:

   a. Login 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.

   Note: The following is for JCS only.

3. Verify that CA IAM Connector Server 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.

Upgrade the CA SiteMinder Policy Server and CSP console

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 as well as your CSP console. You use the same kit to upgrade both the CSP console and the SiteMinder Policy Server.

Follow these steps:

1. SSH into the machine to be upgraded.
2. Verify that a backup (see page 9) of the **/tmp/properties.sh** file exists for SiteMinder Policy Server and for the CSP console.
3. Enter the following commands on the system where the CA SiteMinder Policy Server or CSP console is installed.

   ```
   su - root
   mv /dev/random /dev/random.orig
   ln -s /dev/urandom /dev/random
   ```

4. If it is running, stop the RiskMinder case manager using the following sub-steps:
   ```
   ps -ef|grep arrfcasemgmtserver
   ```

If the preceding command shows any running processes, stop it using the following command:

```
cd /opt/CA/AdvancedAuth/bin
./casemanagementserver stop
```

5. Set the following properties in the backup version of **properties.sh**:

   _hco_name=DefaultHostSettings; export _hco_name # Host Configuration Object

6. Unzip the new kit for the machine being upgraded into the root file system folder. For example, enter the following commands:

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

7. 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 -y /serverkit/properties.sh /tmp/properties.sh
      ```

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

   _hco_name=DefaultHostSettings; export _hco_name # Host Configuration Object

8. Run the upgrade by entering the following commands:

Note: If the following directory has a file named upgradeBackupList.sh, it will have an environment variable named BACKUP_LIST. This variable is an array of file names that will be backed up before the upgrade, and then restored after the upgrade. You may add or remove file names from this list as necessary.

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

Verify the Upgrade

1. Verify dxserver status

   a. su – dsa

   b. dxserver status

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

   Note: Only perform the next step for the CSP Console.

2. Verify that the CSP Console is working properly by making sure the tenant and container tasks exist by issuing the following command:

   ```
   ps –ef | grep ui
   ```

   If working properly, you should see a message similar to the following:

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

3. Restart the CA SiteMinder Policy Server or CSP console.

Reset the Audit Logs

Perform the following steps for SiteMinder Policy Server. These steps are not necessary for the CSP console.

1. From the server console, navigate to /opt/CA/siteminder/bin.
2. Start the smsconsole, and select the Data tab.
3. Select Audit logs from the label Database.
4. Select ODBC from the menu against the label Storage.
5. Select the checkbox Use Policy Store Database and click Apply.

Troubleshooting: CA SiteMinder Installation Fails

Symptom:

The CA SiteMinder installation fails.

Solution:

Do the following:

Verify that you created the symbolic link between the random and urandom directories as follows:

```
su - root
mv /dev/random /dev/random.orig
ln -s /dev/urandom /dev/random
```

Troubleshooting: Audit Logs Get Reset to Use the Filesystem instead of the Database

Symptom:

The Audit logs configuration gets reset to use the filesystem instead of the database.

Solution:

Do the following:

1. in the SiteMinder Policy Server console, navigate to /opt/CA/siteminder/bin.
2. Start the smconsole, and then select the Data tab.
3. Select Audit logs option from the drop-down menu against “Database:” label.
4. Select the ODBC option from the drop-down menu against “Storage:” label.
5. Select the Use Policy Store Database checkbox.
6. Click Apply.

Upgrade the CA Secure Proxy Server

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 machine to be upgraded.
3. Set the following property in the **properties.sh**:

   Set # Host Configuration Object to match the **_hco_name_** value set in the SiteMinder Policy Server.

   _hco_name=DefaultHostSettings; export _hco_name
4. Unzip the new kit, for the machine 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:

Note: If this directory has a file named upgradeBackupList.sh, it will have an environment variable named BACKUP_LIST. This variable is an array of file names that will be backed up before the upgrade, and then restored after the upgrade. You may add or remove file names from this list as necessary.

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

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

7. Repeat steps 1-6 for each Secure Proxy Serve node.
8. Restart the CA Secure Proxy Server using the following commands:

```
service s98sps stop
service s98sps start
```

Upgrade Verification

1. Putty to the CA Secure Proxy Server ensure services are running.
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 start
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 start
   ```

Upgrade the CA Identity Management Server

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

Note the following before you upgrade the Identity Management server:

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

Follow these steps:

1. Set the following properties in the backup version of properties.sh:

   _ web_agent_name=camadmin; export web_agent_name

2. SSH into the machine to be upgraded.
3. Verify that a backup (see page 9) of the /tmp/properties.sh file exists.
4. Unzip the new kit for the machine being upgraded into the root file system folder. For example, enter the following commands:

   ```
   cd /
   unzip –o CAM-IM_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 added the properties to and the tmp/properties file by entering the following command:

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

   b. Make appropriate changes to the backup version of properties.sh file as required.

6. Run the upgrade:

   Note: If the following directory has a file named upgradeBackupList.sh, it will have an environment variable named BACKUP_LIST. This variable is an array of file names that will be backed up before the upgrade, and then restored after the upgrade. You may add or remove file names from this list as necessary.

   ```
   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.

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.

Session Cookies May Allow Authentication After Log Off

For each tenant, set the <tenant>_ims_realm to persistent. Change the realm to use a persistent session.

Follow these steps:

1. Login to the Cloud Service Provider Console.
2. Navigate to Policies, Domain, Domains.
3. Edit the <tenant>Domain and navigate to Realms tab.
4. Edit <tenant>_ims_realm realm and look for the Session section
5. Change the Session to Persistent.
6. Click OK, and then Submit.
7. Repeat the steps above for all tenants.
8. Refresh the cache by navigating to Administration, Policy Server, Cache Management->Flush All

Set the Connection Type as Your JDBC Connection

After the upgrade, the IdentityMinder 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 Your /tmp/properties.sh Files to a Secure Location For the Next Upgrade

Important! After completing the installation of the product, you must back up the file /tmp/properties.sh file on each server component to a secure location. You need these files for future upgrades because this file contains password information. If you do not have this file backed up from a previous installation or upgrade, you cannot proceed with new upgrades.

Make sure to back up the **properties.sh** file from the **/tmp** directory immediately after the upgrade, just as you must do after your initial installation.

The upgrade overwrites these files. After you update the servers in the environment, you use the backup versions of the files to complete the upgrade.

Important! Do not create back-up versions in the **/tmp** directory, as this directory is volatile. Copy the **properties.sh** files from your prior installation to each server. In the example below, replace **/tmp** with the location of your secure backup.

The following procedure places back up files in a serverkit directory.

Follow these steps:

1. On each CA Directory server system, enter the following commands:

   ```
   mkdir /serverkit
   ```

   ```
   cp /tmp/properties.sh /serverkit
   ```

2. On each Provisioning Server and CA IAM Connector Server system, enter the following commands:

   ```
   mkdir /serverkit
   ```

   ```
   cp /tmp/properties.sh /serverkit
   ```

3. On each CA SiteMinder Policy Server, enter the following commands to back up the properties file:

   ```
   /tmp/properties.sh
   ```

   ```
   mkdir /serverkit
   ```

4. On each SPS system, enter the following commands:

   ```
   /tmp/properties.sh
   ```

   ```
   mkdir /serverkit
   ```

   ```
   cp /tmp/properites.sh /serverkit
   ```

5. On each Identity Management server, enter the following commands:

   ```
   mkdir /serverkit
   ```

   ```
   cp /tmp/properites.sh /serverkit
   ```

Important! If there is more than one server of each type, back up each properties files on each system. For example, if I have two Directory servers, you must back up each, separate properties file and move them to the serverkit folder.

High-Availability: Layer 7 Gateway Server

The Layer 7 Gateway servers are new components in CA CloudMinder 1.5.

Use this procedure to install the Layer 7 Gateway servers.

Note: These instructions assume you are installing two Gateway servers in a high-availability deployment.

For additional information, see the the complete Layer 7 Installation and Maintenance Manual.

Deploy the First Gateway

These steps describe how to deploy the first gateway server.

Important! Delete any previous installations or data before deploying the gateway. Residual test installations or MySQL data can cause installation problems.

Follow these steps:

1. Log in to the system as the root user.
2. Perform base system configuration:
   a. Configure the network card for IPv4 with the following values:
      - Machine name
      - IP Address
      - Default gateway
      - DNS nameserver

b. Disable IPv6:

```
NETWORKING_IPV6=no in /etc/sysconfig/network
```

c. Configure the timezone:

```
/etc/sysconfig/clock
```

d. Install the NTP server, if you have not already done so:

```
yum install ntp
```

e. Enable NTP autostart:

```
/sbin/chkconfig ntpd on
```

f. Start the NTP Service:

```
service ntpd start
```

3. Reboot the machine:

```
sync;sync;reboot
```

4. Log in to the system as the root user.

5. Install the MySQL packages with the following commands:

```
cd ~/download
rpm -ivh MySQL-client-5.5.30-1.rhel5.x86_64.rpm
rpm -ivh MySQL-server-5.5.30-1.rhel5.x86_64.rpm
cp -p my.cnf /etc
service mysql start
```

Note: If the first RPM attempt fails, the base RedHat system may already have another version of MySQL installed. Use rpm -e to remove any conflicts.

6. /usr/bin/mysql_secure_installation and set the following values:

- Enter current password for root (enter for none): Press <enter> for none
- Set root password?: Y
- New password: 7layer
- Re-enter new password: 7layer
- Remove anonymous users?: Y
- Disallow root login remotely?: Y
- Remove test database and access to it? : Y
- Reload privilege tables now?:Y

7. Install the JDK under /opt/SecureSpan/JDK with the following commands:

   Note: System scripts reference the JDK files in this location. Install the JDK in this specific subdirectory only.

   ```
   cd ~/download
   mkdir tmp
   cd tmp
   tar xvzf ../jdk-7u21-linux-x64.tar.gz
   mkdir /opt/SecureSpan/
   mv jdk1.7.0_21 /opt/SecureSpan/JDK
   unzip ../UnlimitedJCEPolicyJDK7.zip
   cp -p UnlimitedJCEPolicy/*jar
   /opt/SecureSpan/JDK/jre/lib/security/
   ```

   Set the following values for the preceding command:

   ```
      cp: overwrite
   `/opt/SecureSpan/JDK/jre/lib/security/local_policy.jar'?: Y
   ```

   ```
      cp: overwrite
   `/opt/SecureSpan/JDK/jre/lib/security/US_export_policy.jar'?: Y
   ```

8. Install the ssgnodb rpm and the required dependencies with the following commands:

   ```
   cd ~/download
   rpm -ivh ssg-7.1.1-3_noDB.noarch.rpm
   mkdir tmp
   cd tmp
   tar xvzf ../mysql-connector-java-5.1.20.tar.gz
   cp -p
   mysql-connector-java-5.1.20/mysql-connector-java-5.1.20-bin.jar
   /opt/SecureSpan/Gateway/runtime/lib/mysql-connector-java-5.1.20
   .jar
   chown layer7:layer7
   /opt/SecureSpan/Gateway/runtime/lib/mysql-connector-java-5.1.20
   .jar
   chmod 444
   /opt/SecureSpan/Gateway/runtime/lib/mysql-connector-java-5.1.20
   .jar
   ```

9. Add ssg service with the following commands:

   ```
   cd ~/download
   chmod +x ssg
   cp -p ssg /etc/init.d/ssg
   /sbin/chkconfig --add ssg
   ```

Deploy the Second Gateway

These steps describe how to deploy the second gateway server.

Important! Delete any previous installations or data before deploying the gateway. Residual test installations or MySQL data can cause installation problems.

Follow these steps:

1. Log in to the system as the root user.
2. Perform base system configuration:
   a. Configure the network card for IPv4 with the following values:
      - Machine name
      - IP Address
      - Default gateway
      - DNS nameserver
   b. Disable IPv6:

      ```
      NETWORKING_IPV6=no in /etc/sysconfig/network
      ```

   c. Configure the timezone:

      ```
      /etc/sysconfig/clock
      ```

   d. Install the NTP server, if you have not already done so:

      ```
      yum install ntp
      ```

   e. Enable NTP autostart:

      ```
      /sbin/chkconfig ntpd on
      ```

   f. Start the NTP Service:

      ```
      service ntpd start
      ```

3. Reboot the machine:

   ```
   sync;sync;reboot
   ```

4. Log in to the system as the root user.

5. Download the following files to ~/download:

   From CA Support:

   - add_slave_user.sh
   - create_slave.sh
   - harden.sh
   - my.cnf
   - ssg
   - ssg-7.1.1-3_noDB.noarch.rpm

   From Oracle:

   - jdk-7u21-linux-x64.tar.gz
   - UnlimitedJCEPolicyJDK7.zip

   From MySQL:

   - mysql-connector-java-5.1.20.tar.gz
   - mySQL-client-5.5.30-1.rhel5.x86_64.rpm
   - mySQL-server-5.5.30-1.rhel5.x86_64.rpm

6. Install the MySQL packages with the following commands:

   ```
   cd ~/download
   rpm -ivh MySQL-client-5.5.30-1.rhel5.x86_64.rpm
   rpm -ivh MySQL-server-5.5.30-1.rhel5.x86_64.rpm
   cp -p my.cnf /etc
   service mysql start
   ```

   Note: If the first RPM attempt fails, the base RedHat system may already have another version of MySQL installed. Use rpm -e to remove any conflicts.

7. /usr/bin/mysql_secure_installation and set the following values:

   - Enter current password for root (enter for none): Press <enter> for none
   - Set root password?: Y
   - New password: 7layer
   - Re-enter new password: 7layer
   - Remove anonymous users?: Y
   - Disallow root login remotely?: Y
   - Remove test database and access to it? : Y
   - Reload privilege tables now?:Y

8. Install the JDK under /opt/SecureSpan/JDK with the following commands:

   Note: System scripts reference the JDK files in this location. Install the JDK in this specific subdirectory only.

   ```
   cd ~/download
   mkdir tmp
   cd tmp
   tar xvzf ../jdk-7u21-linux-x64.tar.gz
   mkdir /opt/SecureSpan/
   mv jdk1.7.0_21 /opt/SecureSpan/JDK
   unzip ../UnlimitedJCEPolicyJDK7.zip
   cp -p UnlimitedJCEPolicy/*jar
   /opt/SecureSpan/JDK/jre/lib/security/
   ```

   Set the following values for the preceding command:

   ```
      cp: overwrite
   `/opt/SecureSpan/JDK/jre/lib/security/local_policy.jar'?: Y
   ```

   ```
      cp: overwrite
   `/opt/SecureSpan/JDK/jre/lib/security/US_export_policy.jar'?: Y
   ```

9. Install the ssgnodb rpm and the required dependencies with the following commands:

   ```
   cd ~/download
   rpm -ivh ssg-7.1.1-3_noDB.noarch.rpm
   mkdir tmp
   cd tmp
   tar xvzf ../mysql-connector-java-5.1.20.tar.gz
   cp -p
   mysql-connector-java-5.1.20/mysql-connector-java-5.1.20-bin.jar
   /opt/SecureSpan/Gateway/runtime/lib/mysql-connector-java-5.1.20
   .jar
   chown layer7:layer7
   /opt/SecureSpan/Gateway/runtime/lib/mysql-connector-java-5.1.20
   .jar
   chmod 444
   /opt/SecureSpan/Gateway/runtime/lib/mysql-connector-java-5.1.20
   .jar
   ```

10. Add ssg service with the following commands:

    ```
    cd ~/download
    chmod +x ssg
    cp -p ssg /etc/init.d/ssg
    /sbin/chkconfig --add ssg
    ```

Configure Gateway Database Replication

Configure database replication on your Layer 7 Gateway servers by creating a Master-Master configuration.

Follow these steps:

1. SSH into both Gateways.
2. Stop the gateway process on both servers by entering the following command:
   `service ssg stop`

   Note: You may see the following message:

   Shutting down Gateway Services: [FAILED]

   This simply means that the gateway service had not been started. Continue with database replication.
3. Enter the following command on both gateways:
   `cd ~/download; chmod +x add_slave_user.sh; chmod +x create_slave.sh`
4. On Gateway one, run the following command:
   `./add_slave_user.sh`
5. For the root user password, enter 7layer.

   Important! Enter known or default values for configurations that are not specified in this section.
6. For the slave hostname, enter the fully qualified machine name of Gateway two.
7. Set the node to primary (1).
8. On Gateway two, run the following command:
   `./add_slave_user.sh`
9. For the root user password, enter 7layer.

   Important! Enter known or default values for configurations that are not specified in this section.
10. For the slave hostname, enter the fully qualified machine name of Gateway one.
11. Set the node to secondary (2).
12. On Gateway one, run the following command:
    `./create_slave.sh`

    Note: This script uses port 3306. If required, change the port to 3307.
13. Enter the hostname of Gateway two.
14. Enter the hostname of Gateway one for MASTER.

    Important! Do not clone the database.

15. On Gateway two, run the following command:
    `./create_slave.sh`

    Note: This script uses port 3306. If required, change the port to 3307.
16. Enter the hostname of Gateway one.
17. Enter the hostname of the second gateway for MASTER.

    Important! Do not clone the database.
18. Verify replication with the following command:
    `mysql -p -e "show slave status\G"`

    Note: -p is required to prompt for root password.

    Enter 7layer for the password.

    - For Gateway one, MASTER is Gateway two.
    - For Gateway two, MASTER is Gateway one.

Create an Internal Database

Create an internal database on Gateway one.

In a clustered configuration, you create an internal database on only Gateway one. This database is replicated automatically to Gateway two. The Gateway one database is the primary, while the Gateway two database is used for failover.

Follow these steps:

1. On Gateway one, enter:
   `/opt/SecureSpan/Gateway/runtime/bin/setup.sh --jdk /opt/SecureSpan/JDK`
2. Select 2 Configure the Layer 7 Gateway.
3. Press Enter to accept the default Java VM Path.
4. Press Enter to accept the Java VM Memory Allocation [512].
5. Set the following configuration values:
   - Database Connection: Yes
   - Database Host: enter "localhost" or the Gateway hostname

     For example, enter L7host.forewardinc.com.

- Database Port: 3306
- Database Name: ssg
- Database Username: gateway, or choose any username.
- Database Password: 7layer, or choose any password.

  Note: If you modify the database username and password, record these values for later use.

- Administrative DB User: root
- Administrative DB Password: 7layer

  Important! Do not modify the administrative database user and password values. They reference existing default values.

- Configure Failover Connection: No
- SSM Username: admin
- SSM Password: <YOUR PASSWORD>
- Administrative HTTPS Listener? [No]: No
- Cluster Hostname: Enter the hostname of the application tier load balancer.
- Cluster Password: <YOUR PASSWORD>

  Note: Record this password for use when configuring Gateway two.

- Enabled: Yes
- Press Enter to return to the menu

6. Type X to return to the UNIX shell.

Configure the Gateway One Database

This section covers connecting Gateway one to the internal database.

Follow these steps:

1. SSH into Gateway one.
2. Enter /opt/SecureSpan/Gateway/runtime/bin/setup.sh --jdk /opt/SecureSpan/JDK.
3. Select 2 - Configure the Layer 7 Gateway.
4. Select 2 - Database Connection.
5. Enter the username and password you set when you created the database.
6. Database Host [localhost]: This is the primary MySQL database. Enter the fully qualified domain name (FQDN) for gateway one.
7. Database Port [3306]: Leave as the default.
8. Database Name [ssg]: Leave as the default.

9. Database Username [gateway]: Leave as the default or choose any user name.
10. Enter a database password that you choose.

    Note: If you modify the database username and password, record these values for later use.
11. Select 3 - Configure Database Failover Connection.
12. Database Failover Host: This is the failover MySQL database. Enter the FQDN for gateway two.
13. Database Port [3306]: Leave as the default.
14. Select S - Save and Exit.
15. Press [Enter] to continue.
16. Enter the following commands:
    - /sbin/chkconfig ssg on
    - /sbin/chkconfig --list ssg

    The system responds with:

    ssg 0:off 1:off 2:on 3:on 4:on 5:on 6:off

Configure the Gateway Two Database

This section covers connecting Gateway two to the internal database.

Follow these steps:

1. SSH into Gateway two.
2. Enter /opt/SecureSpan/Gateway/runtime/bin/setup.sh --jdk /opt/SecureSpan/JDK
3. Select 2 - Configure the Layer 7 Gateway.
4. Java VM Path [/opt/SecureSpan/JDK/jre]: Press Enter to accept the default.
5. Java VM Memory Allocation [512]: Press Enter to accept the default.
6. Database Connection: Yes
7. Enter the username and password you set during database creation.
8. Database Host [localhost]: This is the primary MySQL database. Enter the fully qualified domain name (FQDN) for gateway one.

   Note: Although this is the second gateway, always use gateway one as the database connection.

   For example, enter L7host.forwardinc.com
9. Database Port [3306]: Leave as the default.
10. Database Name [ssg]: Leave as the default.

11. Database Username [gateway]: Leave as the default or choose any user name.
12. Enter a database password that you choose.

    Note: If you modify the database username and password, record these values for later use.
13. Administrative DB User: root
14. Administrative DB Password: 7layer

    Important! Do not modify the administrative database user and password values. They reference existing default values.
15. Configure Failover Connection: Yes
16. Database Failover Host: This is the failover MySQL database. Enter the FQDN for gateway two.

    Note: Although this is the second gateway, always use gateway two as the failover connection.
17. Database Failover Port [3306]: Leave as the default.
18. SSM Username: admin

    SSM Password: Enter the same password as you entered when creating the internal database on gateway one.
19. Administrative HTTPS Listener? [No]: No
20. Cluster Hostname: Enter the name of the application tier load balancer.
21. Cluster Password: Enter the same password as you entered when creating the internal database on gateway one.
22. Press Enter.
23. Press Enter.
24. Type X to return to the UNIX shell.
25. Enter the following commands:
    - /sbin/chkconfig ssg on
    - /sbin/chkconfig --list ssg

The system responds with:

```
ssg          0:off  1:off  2:on   3:on   4:on   5:on   6:off
```

Harden the Gateway Servers

This section describes how to harden the Gateways. Perform the steps and commands on both machines.

Follow these steps:

1. SSH into the Gateway server as root user and enter the following commands:

   ```
   useradd -m ssgconfig
   passwd ssgconfig
   ```

   Provide the password of your choice for the user ssgconfig.

   ```
   cd ~/download
   chmod +x harden.sh
   cp -p harden.sh ~/harden.sh
   cd ~
   ```

   ```
   ./harden.sh -h vmware
   ```

2. If ./harden.sh -h vmware fails, review error messages and manually resolve any conflicts. For example, you many need to run the following commands:

   ```
   yum erase subscription-manager
   yum erase yum-updatesd
   yum erase yum-security
   yum erase rhn-client-tools
   echo "SINGLE=/sbin/sulogin" >> /etc/sysconfig/init
   ```

3. Review ~/harden.sh.log for hardening results, manually resolve conflicts, and re-run the hardening process as needed.

   Note: Once the harden.sh script has been run successfully, you can no longer log in as root. If you wish to gain root access to the system, log in as user ssconfig and run the su command to change your login ID to root. Typically, you must run the harden.sh script multiple times even if the script shows no error messages upon execution.

Install Mobile Access Gateways (MAG) and Siteminder Assertion Packages

Note: The steps for this procedure are different on the two Gateways of your high-availability deployment. Follow the instructions carefully.

Follow these steps:

On Gateway one:

1. Connect with SSH.
2. Run the following commands:
   - service ssg stop
   - rpm -Uvh --nodeps ssg-mag-2.0-1-cloudminder.noarch.rpm
   - rpm -Uvh ssg-sm12-7.0-1-cloudminder.x86_64.rpm
3. Register the agent by running the following commands:
   - cd /opt/SecureSpan/siteminder/bin/
   - ./smreghost.sh -i <SITEMINDER-IP> -u <SITEMINDER-USER> -p <SITEMINDER-PASS> -hn <CLUSTER-HOSTNAME> -hc <SITEMINDER-CONFIG-SETTING> -cf <SITEMINDER-FIPS-MODE>

     Note: The SiteMinder values refer to the existing SiteMinder deployment for this environment.

     This command builds the SmHost.conf file.

     An example of this command is as follows:

     ./smreghost.sh -i SMPSVIP -u siteminder -p <pwd> -hn layer7 -hc DefaultHostSettings -cf COMPAT
4. Restart the service by running the following command:

   ```
   service ssg start
   ```

On Gateway two:

1. Connect with SSH.
2. Run the following commands:
   - service ssg stop
   - rpm -Uvh --nodeps ssg-mag-2.0-1-cloudminder.noarch.rpm
   - rpm -Uvh ssg-sm12-7.0-1-cloudminder.x86_64.rpm

3. Restart the service by running the following command:

   ```
   service ssg start
   ```

After installing the MAG and SiteMinder assertion packages, perform the remaining configuration steps on Gateway one only. No further configuration is necessary on Gateway two.

Install the Layer 7 License File

Note: In a high-availability environment where you have installed two gateways, perform these steps on Gateway one only.

Upon initial log in to the Gateway, the Layer 7 Policy Manager prompts you to install your license file.

Follow these steps:

1. Navigate to the Layer 7 Policy Manager web interface at the following URL:

   https://<GATEWAY_ONE_HOSTNAME>:8443/ssg/webadmin

2. Log in using the credentials you created during installation for the Gateway admin user.

   These are the credentials you entered for SSM username and SSM password.

   Note: The Gateway includes a login security feature to prevent unauthorized access. After several failed login attempts, the system locks. After 20 minutes, the lockout timer expires and you may attempt login again.

   The Cluster License window appears.

3. Click Install License.

4. Navigate to the location where you unpacked the Layer 7 tarball and select the following license file:

   ```
   CA_Cloudminder_MSP_SSGv7_5yr.xml
   ```

5. Click I Agree to start the license installation.

   The Cluster License window reappears.

   Note: Installation is proceeding at this time. The system may seem unresponsive for several minutes while the installation completes. Do not attempt to interact with the system until installation is confirmed.

6. Verify that the license is valid and close the window.

Import the Certificate for the Gateway

Note: In a high-availability environment where you have installed two gateways, perform these steps on Gateway one only.

Import the digital certificate for the Layer 7 Gateway.

Follow these steps:

1. Select Manage, then Manage Certificates.
2. Click Add.

   The Add Certificate Wizard opens.
3. Select Retrieve via SSL Connection and enter the HTTPS URL of the certificate as follows:

   `https://localhost:8443`
4. Click Next.
5. Click to Accept hostname mismatch, if applicable.
6. Leave the Certificate Name unchanged. Click Next.
7. Select the following usage options:

   Outbound SSL Connections

   Signing Certificated for Outbound SSL Connections

   Signing Client Certificates
8. Confirm that the certificate is a Trust Anchor.
9. Leave Revocation Checking as the default.
10. Click Finish.
11. Click Close.

Create Cluster Property: siteminder12.agent.configuration

Note: In a high-availability environment where you have installed two gateways, perform these steps on Gateway one only.

Configure the siteminder12.agent.configuration property settings for your Layer 7 Gateway node. This cluster property helps manage the interaction of the Gateway with the CA SiteMinder® component.

If your node is part of a cluster, all other nodes in the cluster inherit the new settings as well.

Follow these steps:

1. Select Manage, then Manage Cluster-Wide Properties.
2. Click Add.
3. In the Key field, enter:

   `siteminder12.agent.configuration`
4. Navigate to the Layer 7 Gateway tarball and locate the following file in a text editor:

   `siteminder12.agent.configuration.txt`
5. Save a copy of this file. Rename the copy to reflect the name of the tenant for which you are configuring OAuth. For example:

   `siteminder12.agent.configuration.forwardinc.txt`
6. Open the file in a text editor.
7. Navigate to the following file:

   `SmHost.conf`

   Note: The SmHost.conf file is found in the same location as the smreghost script. The smreghost script runs during installation and creates the SmHost.conf file. You can find it on Gateway one in /opt/SecureSpan/siteminder/bin.
8. Open the file in a text editor.
9. In the SiteMinder agent configuration file, perform the following operations:
   a. Replace <SITEMINDER-AGENT> with the configured Agent ID from SiteMinder.

      This is the agent associated with all realms.
   b. Replace <SITEMINDER-IP> with the VIP or host name for the CA SiteMinder® Policy Server listed in SmHost.conf.
   c. Replace <SITEMINDER-SECRET> with the secret listed in SmHost.conf.

      Copy and paste the secret, excluding the quotation marks (").
   d. Replace <SITEMINDER-FIPSMODE> with the FIPS mode listed in SmHost.conf.
   e. Replace <CLUSTER-HOSTNAME> with the host name listed in SmHost.conf.

f. If required, modify other parameters. If not, leave the parameters as the default values.

Note: The *agent.ipcheck* parameter must remain set to True.

g. Save the SiteMinder agent configuration file, then copy the contents of the file to your clipboard.

10. In the Policy Manager, in the Value field for the siteminder12.agent.configuration property, paste the updated contents of the siteminder12.agent.configuration.txt file.
11. Click Ok.

Create Cluster Property: token.salt

Note: In a high-availability environment where you have installed two gateways, perform these steps on Gateway one only.

Configure the token.salt property settings for your Layer 7 Gateway node. If your node is part of a cluster, all other nodes in the cluster inherit the new settings as well.

Salt enhances the security of the token store. It is a random string that the system uses to encrypt the token store.

Follow these steps:

1. Select Manage, then Manage Cluster-Wide Properties.
2. Examine the list of properties. If token.salt already exists, skip the remainder of this process.

   If the property does not already exist, click Add.
3. In the Key field, enter:

   `token.salt`
4. In the Value field, enter a random string that will act as salt for the token store. Generate a random string by running the following on the command line:

   openssl rand -base64 32
5. Copy the output and paste it into the Value field.
6. Click Ok.

Restart Gateways

To complete the Layer 7 Gateway installation, restart the service on both Gateways by running the following command:

```
service ssg start
```

You have now completed the Layer 7 Gateway installation.

The Layer 7 Gateway is used to enable CloudMinder to act as an OAuth Authorization Server for an OAuth client. For example, if a tenant wants their users to access an OAuth client application through single sign-on, you can configure CloudMinder to validate the request for user authorization. Perform the necessary configuration for each tenant and each OAuth client application by following the steps in SSO with CloudMinder as an OAuth Authorization Server.

Update Load Balancer Ports

Upgrading to CA CloudMinder 1.5 adds two new components to your environment: the Layer 7 Gateway servers and Radius Proxy servers. Update the load balancers in your high-availability environment to open the appropriate ports.

Component	Port In	Port Out	Traffic Flow	Description
Web Tier Load Balancer	8443	8443		External calls to the Layer 7 Gateway (L7) distributed across all Gateway instances.
Web Tier Load Balancer	1812	1812	(ext)->LB1->SPS	External calls to the Radius Proxy server (Radius) distributed across all SPS instances.

Application Tier Load Balancer	1812	1814	SPS->LB2->Auth.Radius	Radius requests coming from the Radius Proxy running inside SPS. Port 1814 is used to respond back to the Radius Proxy.
Application Tier Load Balancer	20498	20498	L7->LB2->DXrouter	User Directory requests coming from the Layer 7 Gateway distributed across the application tier DXrouter instances.

SPS = Secure Proxy Server

L7 = Layer 7 Gateway Server

Radius = Radius Proxy Server

For further information about port configuration on the load balancers in your high-availability environment, see the topic entitled Port Communication Tables.