CA Identity Manager™

Upgrade Guide (JBoss)

12.6.4

CA Technologies Product References

This document references the following CA Technologies products:

- CA CloudMinder™ Identity Management
- CA Directory
- CA Identity Manager ™
- CA Identity Governance (formerly CA GovernanceMinder)
- CA SiteMinder®
- CA User Activity Reporting
- CA AuthMinder ™

Contact CA Technologies

Contact CA Support

For your convenience, CA Technologies provides one site where you can access the information that you need for your Home Office, Small Business, and Enterprise CA Technologies products. At http://ca.com/support, you can access the following resources:

- Online and telephone contact information for technical assistance and customer services
- Information about user communities and forums
- Product and documentation downloads
- CA Support policies and guidelines
- Other helpful resources appropriate for your product

Providing Feedback About Product Documentation

If you have comments or questions about CA Technologies product documentation, you can send a message to techpubs@ca.com.

To provide feedback about CA Technologies product documentation, complete our short customer survey which is available on the CA Support website at http://ca.com/docs.

Contents

Chapter 1: Upgrade Overview

This section contains the following topics:

Supported Upgrade Paths

You can upgrade to CA Identity Manager 12.6.4 from the following versions:

- CA Identity Manager r12
- CA Identity Manager r12.5 or 12.5 SPx
- CA Identity Manager r12.6 or 12.6 SPx

If you have a pre-r12 version of CA Identity Manager, first upgrade to r12, r12.5, or r12.5 SP1 to SP6. These versions include the imsconfig tool, which is required to upgrade a pre-r12 version. Then you can upgrade to CA Identity Manager 12.6.4.

How to Upgrade CA Identity Manager

Perform the following steps to upgrade to CA Identity Manager 12.6.4:

✓	Step
	1. Be sure your systems meet all upgrade prerequisites.
	2. Upgrade provisioning components.
	3. Upgrade the CA Identity Manager Server on the node or cluster.
	4. Upgrade the Report Server.
	5. Perform post-upgrade configuration.

Chapter 2: Upgrade Prerequisites

This section contains the following topics:

How to Meet Prerequisites for the Upgrade

Perform the following steps to meet all prerequisites before upgrading CA Identity Manager:

✓	Step
	1. Check hardware requirements.
	2. Check software requirements.
	3. Back up custom code.
	4. Upgrade CA Directory.
	5. Install JCE if using SiteMinder.
	6. Meet application server requirements.
	7. Configure SSL if needed.
	8. Meet Solaris and Linux requirements.
	9. Complete the upgrade worksheets.

Important! Be sure to disable all antivirus software before installation.
If antivirus software is enabled while installation takes place, problems can occur.
Remember to re-enable your antivirus protection after you complete the installation.

Check Hardware Requirements

CA Identity Manager Server

These requirements take into account the requirements of the application server that is installed on the system where you install the CA Identity Manager Server.

Component	Minimum	Recommended
CPU	Intel (or compatible) 2.0 GHz (Windows or Red Hat Linux), SPARC 1.5 GHz (Solaris) or POWER4 1.1 GHz (AIX)	Dual core Intel (or compatible) 3.0 GHz (Windows or Red Hat Linux), Dual core SPARC 2.5 GHz (Solaris) POWER5 1.5 GHz (AIX)
Memory	4 GB	8 GB
Available Disk Space	4 GB	8 GB
Temp Space	2 GB	4 GB
Swap/Paging Space	2 GB	4 GB
Processor	64-bit processor and operating system for intermediate and large deployments, dual core	64-bit processor and operating system, quad core

Provisioning Server or a Standalone Connector Server

Component	Minimum	Recommended
CPU	Intel (or compatible) 2.0 GHz (Windows or Red Hat Linux) SPARC 1.5 GHz (Solaris)	Dual core Intel (or compatible) 3.0 GHz (Windows or Red Hat Linux) SPARC 2.0 GHz (Solaris)
Memory	4 GB	8 GB
Available Disk Space	4 GB	8 GB
Processor	64-bit processor and operating system for intermediate and large deployments, dual core	64-bit processor and operating system, quad core

Provisioning Directory

Component	Minimum	Recommended
CPU	Intel (or compatible) 1.5 GHz (Windows or Red Hat Linux) SPARC 1.0 GHz (Solaris)	Dual core Intel (or compatible) 2.5 GHz (Windows or Red Hat Linux) SPARC 1.5 GHz (Solaris)
Memory	4 GB	8 GB
Available Disk Space	2 to 10 GB, depending on the number of endpoint accounts ■ Compact—Up to 10,000 accounts, 0.25 GB per data file (total 1 GB) ■ Basic—Up to 400,000 accounts, 0.5 GB per data file (total 2 GB) ■ Intermediate—Up to 600,000 accounts, 1 GB per data file, total 4 GB ■ Large—Over 600,000 accounts, 2 GB per data file, total 8 GB	2 to 10 GB, depending on the number of endpoint accounts ■ Compact—Up to 10,000 accounts, 0.25 GB per data file (total 1 GB) ■ Basic—Up to 400,000 accounts, 0.5 GB per data file (total 2 GB) ■ Intermediate—Up to 600,000 accounts, 1 GB per data file, total 4 GB ■ Large—Over 600,000 accounts, 2 GB per data file, total 8 GB
Processor	64-bit processor, 64-bit operating system, and CA Directory (64-bit version) for intermediate and large deployments	64-bit processor and operating system

All Components on One System

Hosting the entire CA Identity Manager product on a single physical system is not recommended for production environments. However, to do so, the hardware requirements are as follows:

Component	Minimum
CPU	Intel (or compatible) 3.1 GHz (Windows or Red Hat Linux) SPARC 2.5 GHz (Solaris)
Memory	8 GB
Available Disk Space	6 to 14 GB depending on the number of accounts

Component	Minimum	
Processor		64-bit processor and operating system, quad core
Swap/Paging Space	6 GB	

Check Software Requirements

Before upgrading CA Identity Manager, be sure all software components are at minimum supported versions.

Note: For a complete list of supported platforms and versions, see the CA Identity Manager support matrix on the CA Support Site.

Check the following software components for required versions:

- Operating System
- Java Development Kit (JDK) or Java Runtime Environment (JRE)
- Relational Database (MS SQL or Oracle)
- Application Server

Back Up Custom Code

Before you upgrade, be sure to back up your custom code, including the following:

- C++ custom connectors
- Provisioning manager plug-ins for Java custom connectors
- Each cluster member's customizations, such as non-default ports for workflow
- Custom files inside the EAR, for example, files under the IdentityMinder.ear/custom/ directory. Do *not* back up any files under the following folders:
  - resourcesBundles
  - identitymanager
  - provisioning
- Common program exits
- Custom email templates at the following location:
  `...\IdentityMinder.ear\custom\emailTemplates`
- Pluggable Authentication Module (PAM) DLLs

- CA Identity Manager Server custom code, such as Event Listener class files, Business Logic Task Handler (BLTH) class files, and Logical Attribute Handler (LAH) class files, and property files at the following location:
  `...\IdentityMinder.ear\config`
- Customized skin folder at the following location:
  `...\IdentityMinder.ear\user_console.war\app\imcss\`
- Customized help, back up the help property file at the following location:
  `..\IdentityMinder.ear\config\com\netegrity\config\`

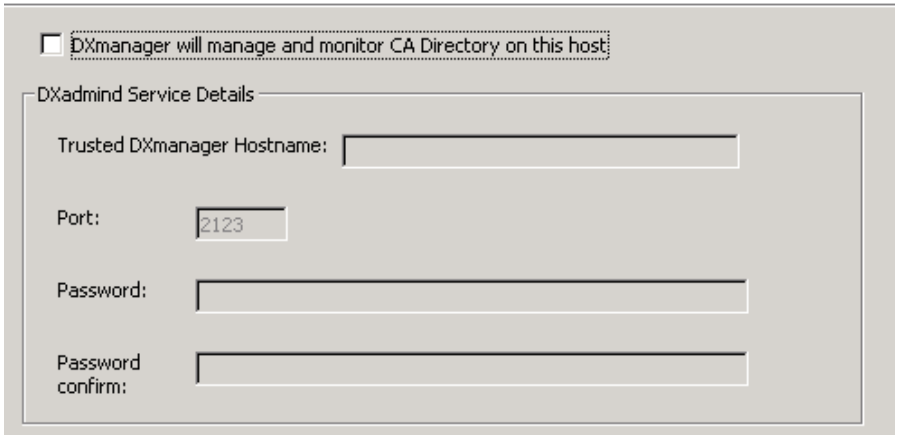
  Also, back up the help page HTML files mentioned in this property file.

Upgrade CA Directory on r12.5 or higher Systems

If you are upgrading a CA Identity Manager r12.5 SP5 or higher system, you must upgrade CA Directory before upgrading the Provisioning Directory. For an r12 system, the CA Directory upgrade occurs as part of the Provisioning Directory upgrade.

To upgrade CA Directory, navigate to the CA Directory installation folder on the CA Identity Manager media and run the dxsetup.exe file. The correct version of CA Directory is included on the CA Identity Manager installation media. The version of CA Directory included on the CA Identity Manager installation media contains fixes specific to the Provisioning Directory; this version is not licensed for general use as a User Store or Enterprise Directory.

Note: This installer asks for information to install DXadmind for DXmanager. You can safely uncheck this option. The Provisioning Directory does not use DXmanager.



Important! If you see an error during the CA Directory upgrade that asks you to close cmd.exe or to stop CA Identity Manager, click Ignore and continue with the upgrade.

Install JCE Libraries for SiteMinder

As of r12.5 SP7, the CA Identity Manager server requires the Java Cryptography Extension (JCE) libraries if you are also using CA SiteMinder.

Before you upgrade the CA Identity Manager server, download and install the Java Cryptography Extension Unlimited Strength Jurisdiction Policy Files. Select the one that works with your application server and JDK. The download ZIP file includes a ReadMe text file with installation instructions.

Install JBoss

CA Identity Manager 12.6.4 works with JBoss 5.0 and 5.1 Enterprise Application Platform (EAP), 5.1 Open Source and JBoss 6.1 (EAP). Therefore, install a new version of JBoss if your version is before 5.0. You can install new version on the same system as the previous version, but in a different file location from the previous version. Also, install the JDK identified in the support matrix as supporting your version of JBoss.

Note: For a complete list of supported platforms and versions, see the CA Identity Manager support matrix on CA Support.

When using JBoss as the application server, note the following points:

- The CA Identity Manager Server is a J2EE application that is deployed on a supported application server.

  For JBoss 5, the iam_im.ear is deployed in the *jboss_home*/server/default/deploy folder. For a clustered installation, iam_im.ear is under jboss_home/server/all/deploy.

- Policy XPress is enhanced to support Web Services SOAP (with basic authentication method) and REST (with basic authentication, proxy authentication, and OAuth authentication methods) such that it can be integrated with external applications that provide a web service interface. To use the Policy XPress web services (SOAP and REST) with JBoss 5.1 community edition, copy the following jars into your JBoss 5.1 community edition "\lib\endorsed" directory from the "client" directory, and then restart the application server:

  - jbossws-native-jaxrpc.jar
  - jbossws-native-jaxws.jar
  - jbossws-native-jaxws-ext.jar
  - jbossws-native-saaj.jar

Note: You do not need to consider copying these files for the EAP versions.

For JBoss 6.1, the iam_im.ear is deployed in the *jboss_home/*standalone/deployments folder.

Important! If any datastore file in the deploy directory is modified, JBoss loses the connection to that datastore and should be restarted.

- Install the required version of the JDK before installing the CA Identity Manager Server. You can download the JDK from the following Oracle URL:

  http://www.oracle.com/technetwork/java/index.html

Configure SSL

If you upgraded your application server and you are using a user directory with SSL, be sure that SSL is configured on your application server before the upgrade.

Solaris Requirements

Provisioning Server Requirements

Verify /etc/system and verify the following minimum IPC kernel parameter values:

- set msgsys:msginfo_msgmni=32
- set semsys:seminfo_semmni=256
- set semsys:seminfo_semmns=512
- set semsys:seminfo_semmnu=256
- set semsys:seminfo_semume=128
- set semsys:seminfo_smmsl=128

- set shmsys:shminfo_shmmni=128
- set shmsys:shminfo_shmmin=4

Solaris 9 or 10 Requirements

Before installing provisioning software on Solaris 9 or 10, download and install the required patches.

1. Download the Sun Studio 10 patches for the Provisioning SDK from the following location:

   `http://developers.sun.com/prodtech/cc/downloads/patches/ss10_patches.html`

2. Download and install patch 117830.

   Note: Sun Studio 11 does not require patching.

3. Download Solaris 9 patches for all Provisioning components from the following location:

   `http://search.sun.com/search/onesearch/index.jsp`

4. Download and install 9_recommended.zip.

Linux Requirements

These requirements exist on a Linux system. If you have registered your Red Hat installation, we recommend that you use yum to install the packages. Otherwise, you can use rpm to install the packages.

Alternatively, use Add/Remove Software to resolve the dependencies, and unchecking the Only Native Packages filter option. Using this approach, you select and install the required i686 architecture dependencies.

Note: The i686 suffix specifies that the library is 32-bit, for the x86 processor.

CA Identity Manager Server

Red Hat 5.x	Red Hat 6.x
glibc-2.5-65.i686.rpm	glibc-2.12-1.47.el6.i686.rpm
libXext-1.0.1-2.1.i386.rpm	libXext-1.1-3.el6.i686.rpm
libXtst-1.0.1-3.1.i386.rpm	libXtst-1.0.99.2-3.el6.i686.rpm
ncurses-devel-5.5-24.20060715.i386.rpm	ncurses-devel-5.7-3.20090208.el6.i686.rpm
ksh-20100202-1.el5_6.6.x86_64.rpm	ksh-20100621-12.el6.x86_64.rpm

Provisioning Server

Red Hat 5.x	Red Hat 6.x
compat-libstdc++-296-2.96-138.i386.rpm	compat-libstdc++-296-2.96-144.el6.i686.rpm
libstdc++-4.1.2-51.el5.i386.rpm	libstdc++-4.4.6-3.el6.i686.rpm
libidn-0.6.5-1.1.i386.rpm	libidn-1.18-2.el6.i686.rpm
libgcc-4.1.2-52.el5.i386.rpm	libgcc-4.4.6-3.el6.i686.rpm

CA IAM Connector Server

For Red Hat 5.x, no packages are required for the CA IAM CS. For Red Hat 6.x, install these packages in this order:

1. glibc-2.12-1.25.el6.i686.rpm
2. libX11-1.3-2.el6.i686.rpm
3. libxcb-1.5-1.el6.i686.rpm
4. libXtst-1.0.99.2-3.el6.i686.rpm
5. libXau-1.0.5-1.el6.i686.rpm
6. libXi-1.3-3.el6.i686.rpm
7. libXext-1.1-3.el6.i686.rpm
8. nss-softokn-freebl-3.12.9-3.el6.i686.rpm
9. libXmu-1.0.5-1.el6.i686.rpm
10. libXft-2.1.13-4.1.el6.i686.rpm
11. libXpm-3.5.8-2.el6.i686.rpm

Linux and FIPS

On a Linux system with FIPS enabled, ensure that sufficient entropy is available. CA Identity Manager requires random data from /dev/random to perform essential cryptographic functions. If data in /dev/random is exhausted, CA Identity Manager processes must wait for random data to be available. This waiting results in poor performance. Use rngd and rng-tools to ensure that /dev/random has sufficient data and reading processes are not blocked.

Complete the Upgrade Worksheets

Provisioning Directory Information

Record the following provisioning information you need during the Provisioning Directory upgrade:

Field Name	Description	Your Response
Directory Name	The file system directory where you want the Provisioning Directory installed.	
Shared Secret	The password for the Provisioning Directory.	
Provisioning Directory Hostnames	The hostnames of any alternate Provisioning Directory systems in a high-availability configuration.	
Provisioning Server Hostnames	The hostnames of the primary Provisioning Server and any alternate Provisioning Servers already installed or to be installed.	
Provisioning Directory Deployment Size	The deployment size that best suits your environment. See the following note.	

Note: If you choose a deployment size that is too small for your environment, the existing data does not fit when loaded into the data files, and an upgrade error occurs. Consider the following guidelines, allowing for future growth:

- Compact—up to 10,000 accounts
- Basic—up to 400,000 accounts
- Intermediate—up to 600,000 accounts
- Large—more than 600,000 accounts

For each choice, the disk space required is covered under Hardware Requirements in this chapter.

Provisioning Server Information

Record the following provisioning information you need during the Provisioning Server upgrade:

Field Name	Description	Your Response
Directory Host	The hostname of the system with the primary Provisioning Directory installed.	
Directory Port	The port number of the system with the Provisioning Directory installed. **Default:** 20394	
Directory DN	The DN for binding to the Provisioning Directory. **Default:** eTDSAContainerName=DSAs,eTNamespaceName=CommonObjects,dc=etadb	
Shared Secret	The password for binding to the Provisioning Directory.	
Provisioning Directory Hostnames	The hostnames of any systems with alternate Provisioning Directories installed.	
Username	The Provisioning domain administrator's username.	
Password	The Provisioning domain administrator's password.	
Description	Provide a description for the Provisioning administrator.	

CA IAM Connector Server Information

The CA IAM Connector Server (CA IAM CS) is the new name for the Java Connector Server. Record the following provisioning information you need during the CA IAM CS upgrade:

Field Name	Description	Your Response
Password	The password for the Provisioning Server administrative user.	
Component Password	The password for CA IAM CS that the Provisioning Server uses for authentication.	

JBoss Information

Record the following JBoss information that you need during the CA Identity Manager installation:

Field Name	Description	Your Response
JBoss Folder	The location of the application server home directory.	
Access URL and port	The URL and port number for one of the following cases: ■ For a single node installation, the system that hosts the CA Identity Manager Server (system that hosts the application server). ■ For a cluster installation, the web server that provides load balancing.	
Java Virtual Machine	The path to the java executable for the JDK.	

Database Connection Information

An Oracle or Microsoft SQL Server database must already be configured and working. Record the following database information you need during the CA Identity Manager installation:

Field Name	Description	Your Response
Database Type	The database type (vendor/version) of the database created for task persistence, workflow, audit, reporting, object storage, and task persistence archive.	
Host Name	The hostname of the system where the database is located. **Note:** Be sure that you provide a hostname and *not* an IP address.	
Port Number	The port number of the database.	
Database Name	The database identifier.	
Username	The username for database access. **Note:** This user must have administrative rights to the database unless you plan to import the schema manually.	
Password	The password for the user account with administrative rights.	

Login Information

Record the following passwords which you need during the Provisioning Components installation.

Field Name	Description	Your Response
Username	A username that you create to log in to the provisioning components. Avoid the username siteminder if you have that product installed. This name conflicts with CA SiteMinder.	

Field Name	Description	Your Response
Provisioning Server password	A password for this Server.	
C++ Connector Server password	A password is needed for this server. Each C++ Connector Server can have a unique password.	
Provisioning Directory password	A password which Provisioning Server uses to connect to Provisioning Directory. For an alternate Provisioning Server, enter the Provisioning Directory password which is created for the primary Provisioning Server.	

SiteMinder Information

If you plan to use a SiteMinder Policy Server to protect CA Identity Manager, record the following information:

Field Name	Description	Your Response
Policy Server Host Name	The hostname of the SiteMinder Policy Server.	
SiteMinder Administrator Name	The administrator username for the SiteMinder Policy Server.	
SiteMinder Administrator Password	The administrator user password for the SiteMinder Policy Server.	
SiteMinder Folder (Solaris Only)	The location of SiteMinder on the system with a SiteMinder Policy Server installed.	
SiteMinder Agent Name	The name of the SiteMinder Agent that CA Identity Manager uses to connect to SiteMinder.	
SiteMinder Shared Secret	The shared secret of the given Agent Name.	

UNIX and Console Mode Installation

The examples in this guide provide the Solaris executable name for the installation program. However, you may be installing on AIX or Linux.

- For AIX, use: ca-im-*release*-aix.bin
- For LINUX, use: ca-*release*-linux.bin

release represents the current release of CA Identity Manager

If you are performing an installation in console mode, such as on a UNIX workstation, you add another option to the command line.

- For the main installation, add -i console. For example:
  `./ca-im-release-sol.bin -i console`
- For installation of provisioning components, add -console to the setup command.

Non-Provisioning Installation

This guide refers to the Windows and Solaris program names for the installers that provide options to install provisioning software. If you prefer to see no provisioning options, you can use these installers:

- For Windows, use IMWithoutProvisioning\ca-im-web-*release*-win.bat
- For Solaris, use IMWithoutProvisioning/ca-im-web-*release*-sol.sh

release represents the current release of CA Identity Manager.

Chapter 3: Provisioning Components Upgrade

This section contains the following topics:

Architecture Changes

CA Identity Manager now uses CA IAM CS as a proxy for C++ Connector Server (CCS). CA Identity Manager no longer communicates with CCS directly.

CA Identity Manager includes a router DSA and a notification DSA:

- The Provisioning Server goes through a router DSA to communicate with the Provisioning Directory. In previous releases of this product, connections to the Provisioning Directory came directly from the Provisioning Server and were authenticated with an LDAP bind username and password.

  For CA Directory DSAs on one system to communicate with DSAs on another system, they must have knowledge of each other. During Provisioning Directory installation, you identify each of the Provisioning Servers that may connect to it.

  In a production environment, we recommend that you run the Provisioning Servers and the Provisioning Directories on separate systems to take advantage of failover and load balancing capabilities, and for performance reasons. Each Provisioning Server communicates with a local CA Directory router, which communicates with the Provisioning Directories.

- A notification DSA named impd-notify is added during the upgrade. If you are upgrading from r12.0, the etaops-notify DSA is replaced with impd-notify during the upgrade. Also, the etrustadmin DSA is replaced with impd-main/co/inc and the etadmintemp DSA is removed.

Upgrade the Provisioning Directory

For the provisioning components to work with CA Identity Manager, upgrade the Provisioning Directory schema and CA Directory.

Note: If you want to install your Provisioning Directory on a new system, migrate the Provisioning Directory instead of performing an upgrade.

When upgrading CA Directory, the installer may ask you perform one of these actions:

- Close cmd.exe
- Stop CA Identity Manager

If you encounter either message, click Ignore and continue with the upgrade.

To upgrade the Provisioning Directory

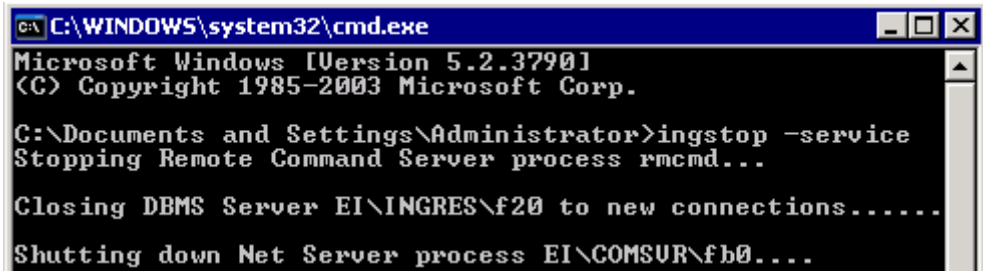
1. If you have primary and alternate Provisioning Directories, back up your primary Provisioning Directory.
2. Shut down all Provisioning Directories in your environment.
3. If you are upgrading from a release prior to CA Identity Manager r12.5, complete the following steps.

   Note: If you are upgrading from CA Identity Manager r12.5 or a higher release, skip to step 4.

   Starting at CA Identity Manager r12.5, CA Directory no longer uses Ingres as a data store. Instead, a new memory-mapped file technology named DXgrid is used. Therefore, you perform these Ingres steps:

   a. Stop Ingres with the following command:

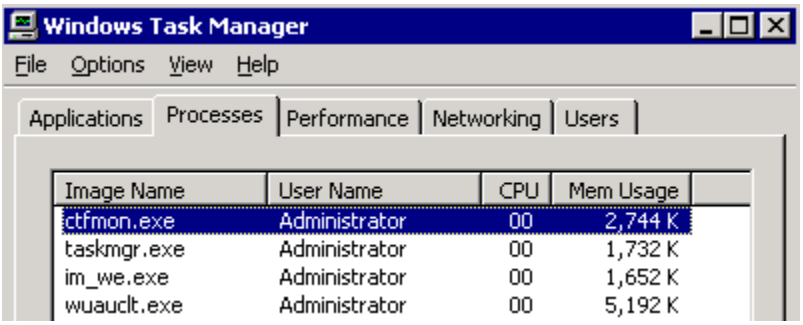
      ```
      ingstop –service
      ```



b. If you get an error, use this command:
```
ingstop -kill
```

c. Verify that all of the following Ingres processes are stopped (use the Window Task Manager or the UNIX ps command):

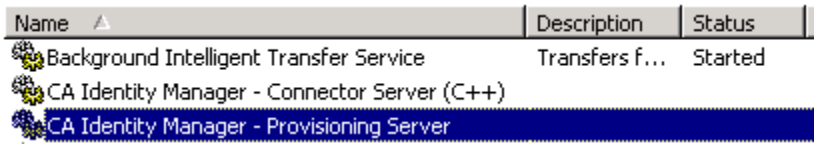
- dmfacp.exe
- dmfrcp.exe
- iidbms.exe
- iigcc.exe
- iigcn.exe
- iijdbc.exe
- iistar.exe



d. Restart Ingres with the following command:
```
ingstart –service
```

e. Issue the following dxserver command:
```
dxserver start all
```

4. Stop the Connector Server and Provisioning Server services.

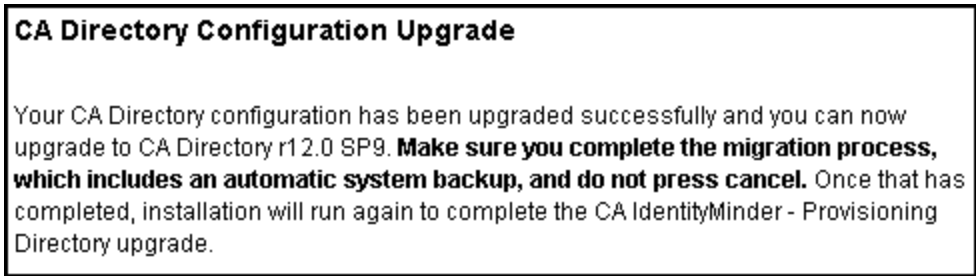


5. Choose the upgrade method for the provisioning directory:

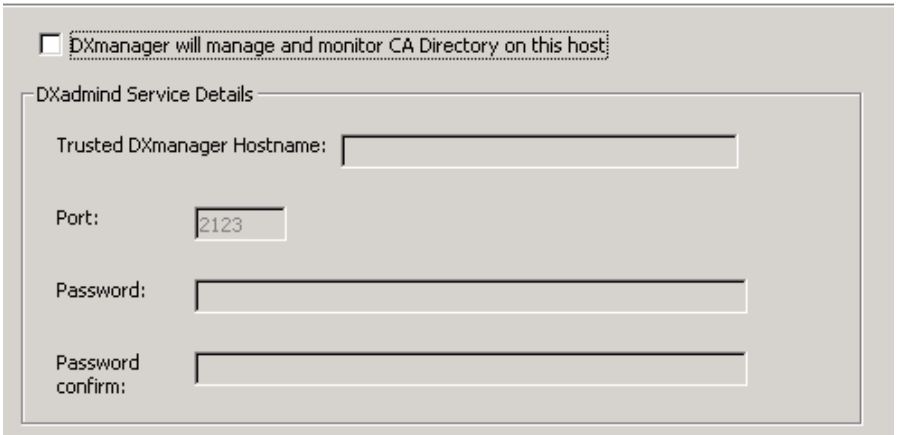
- If you are upgrading from an r12.5 or r12.5 SP release, you can upgrade using the installer, which starts the upgrade wizard.
- If you are upgrading from an r12 release, use upgrade.bat (or upgrade.sh) in the CADirectory/dxserver directory, not the Provisioning Directory setup.exe file. The upgrade.bat script examines your system, performs any prerequisite cleanup, upgrades CA Directory and then upgrades the Provisioning Directory.

6. Answer the question about deployment size if the Select Deployment Size screen appears in your upgrade. Consider the following guidelines, while allowing room for future growth:
   - Compact—up to 10,000 accounts
   - Basic—up to 400,000 accounts
   - Intermediate—up to 600,000 accounts
   - Large—more than 600,000 accounts

   Note: If you are installing a Provisioning Directory in an established CA Identity Manager installation, be sure to make the deployment size large enough. Otherwise, an error occurs because the data does not fit when loaded into the data files.
7. If you are installing the Provisioning Directory in an FIPS 140-2 enabled environment, select the FIPS 140-2 Compliance mode check box during installation and provide the FIPS Key File.
8. If you are upgrading a pre-r12.5 installation, a CA Directory Upgrade Configuration message appears:



9. Click Finish to perform the CA Directory upgrade. Note the following:
   - The CA Directory starts by backing up your current installation when you click Migrate.
   - Select a Typical installation type when prompted during the CA Directory upgrade.
   - Due to architectural changes effective in CA Directory r12 SP1 and higher, reporting databases and unnecessary DSAs are removed before the CA Directory upgrade.
   - During CA Directory installation, you are asked for information about installing DXadmind for DXManager, however, you can safely uncheck this option. The Provisioning Directory does not use DXManager.



Once the CA Directory upgrade completes, the Provisioning Directory upgrade resumes.

10. Go through the wizard and enter the information you collected for the upgrade.

    During upgrade, you can select a check box to configure Provisioning Directory high availability. If you choose this option, you supply the hostnames of all alternate Provisioning Directories and specify the primary Provisioning Directory.

11. When the upgrade completes, uninstall and reinstall any alternate Provisioning Directories. For more information, see the *Installation Guide*.

After the upgrade completes, you can find CA Directory documentation in the following locations:

- Windows: Go to Start, Programs, CA, Directory, Documentation.
- UNIX: Navigate to /opt/CA/Directory/doc.

Migrate the Provisioning Directory

When upgrading to CA Identity Manager 12.6.4, you can migrate the Provisioning Directory to a new system. This migration can accommodate requirements for memory or a 64-bit operating system.

Follow these steps:

1. Install CA Directory on the new system using the CA Directory component installer.
2. Copy any custom schema files from the existing Provisioning Directory system to the new system. Custom schema files exist in the following situations:
   - The COSX (etrust_cosx.dxc) has been modified.
   - The LDA connector (etrust_lda.dxc) is installed.
   - A custom C++ connector schema has been created.

   Copy the schema files from the local %DXHOME%/config/schema directory to the same directory on the new system.
3. Install the 12.6.4 Provisioning Directory on the new system using the *same* domain name as the existing system.
4. Stop the etrustadmin DSA on the old system and dump the data.

   If you are upgrading a r12.5 SP system, use the following command:

   ```
   dxdumpdb -f filename -v DSA_Name
   ```

   For example:

   ```
   dxdumpdb -f hostname-impd-notify.ldif  -v hostname-impd-notify
   dxdumpdb -f hostname-impd-co.ldif  -v hostname-impd-co
   dxdumpdb –f hostname-impd-inc.ldif  -v hostname-impd-inc
   dxdumpdb -f hostname-impd-main  -v hostname-impd-main
   ```

   If you upgrading a r12.6 system, use the following command:

   ```
   dxdumpdb -O -f filename -p dc=etadb -S DSA_name database_name
   ```
5. Stop the -main, -co, and -inc DSAs on the new host by running the following commands from a command prompt:

   ```
   dxserver stop new_system_name-impd-main
   dxserver stop new_system_name-impd-inc
   dxserver stop new_system_name-impd-co
   ```
6. Load the data file produced in Step 4 into all the DSAs by running the following commands from a command prompt:

   ```
   dxloaddb -s new_system_name-impd-main filename
   dxloaddb -s new_system_name-impd-co filename
   dxloaddb -s new_system_name-impd-inc filename
   ```

7. Restart the DSAs on the new host by running the following commands from a command prompt:

   ```
   dxserver start new_system_name-impd-main
   dxserver start new_system_name-impd-inc
   dxserver start new_system_name-impd-co
   ```

   The 12.6.4 Provisioning Directory is now running on the new system with all the data from the old system. The old Provisioning Directory can now be removed.

8. Uninstall and reinstall any alternate Provisioning Directories.

   Note: For more information, see the *Installation Guide*.

Note: Be sure to use the *new* Provisioning Directory hostname when upgrading the Provisioning Servers. The default in the upgrade installer is set to the old hostname.

Upgrade the Provisioning Server

Important! The Provisioning Server uses an instance of CA Directory to communicate with the Provisioning Directory. Be sure to install or upgrade CA Directory on the Provisioning Server system, using the CA Directory component installer, *before* upgrading the Provisioning Server.

The component CA Directory installer is located on the CA Identity Manager media, under CADirectory_x64.

The Provisioning Server upgrade includes the C++ Connector Server, and also performs all connector upgrades by default.

Note the following when upgrading the Provisioning Server:

- Before upgrading the Provisioning Server, be sure that inbound requests are completed. Use View Submitted Tasks to verify these requests are complete.
- Before installing the Provisioning Server, uninstall and reinstall any alternate Provisioning Directories if they exist. For more information, see the *Installation Guide*.
- If you have more than one Provisioning Server, upgrade the primary first, then upgrade all alternate Provisioning Servers.

To upgrade the Provisioning Server

1. Run the CA Identity Manager installer from the CA Identity Manager media.

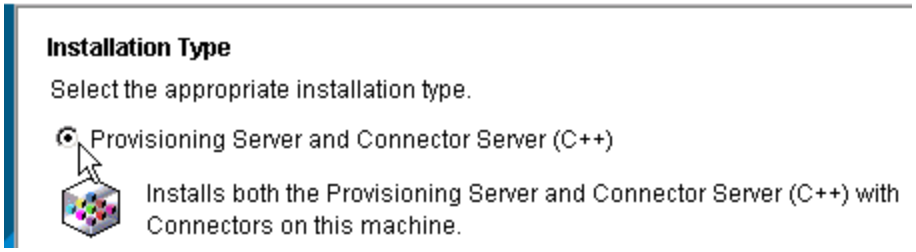
   The Upgrade Wizard starts.

2. In the Upgrade Wizard, next to Provisioning Server, click Launch Upgrade.

   The Provisioning Server upgrade starts. Note the following:

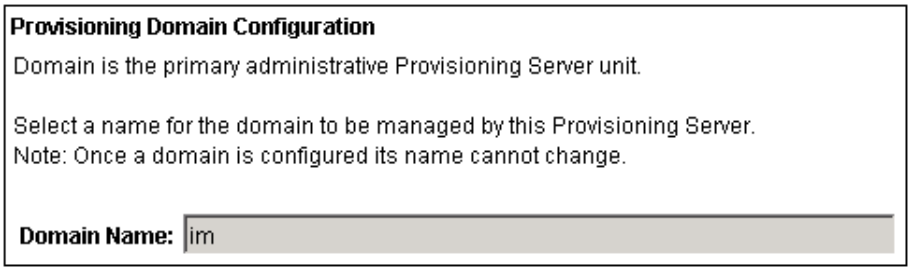
3. If you see a Deprecated Connector Warning, consult the *Connectors Guide* for migration steps to complete after the upgrade.

4. Select the Custom setup type when prompted.
5. Select the appropriate Installation Type, depending on which components are installed on the system (Provisioning Server, C++Connector Server, or both).

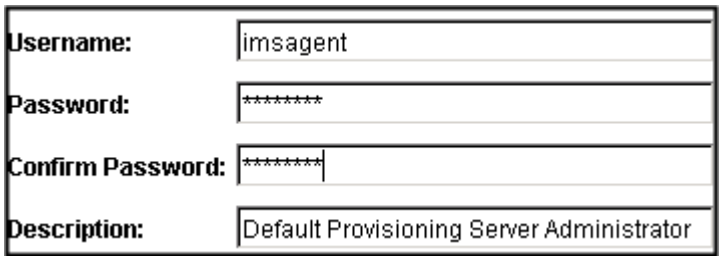


6. You can select a check box during upgrade to indicate Provisioning Directory high availability. If you select this option, supply the hostnames of any alternate Provisioning Directories and specify the primary Provisioning Directory.
7. Complete the Provisioning Domain screens.

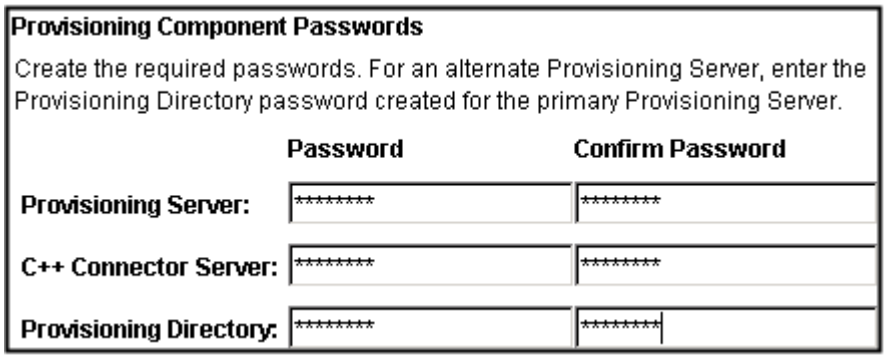
   Note: You may notice a slight delay when you click Next on the first Provisioning Domain screen.



8. Enter a password for the domain.



9. Supply provisioning components passwords.



10. Go through the wizard and enter the information you collected for the upgrade.

    Your Provisioning Server is upgraded.

Upgrade C++ Connector Server (CCS)

From CA Identity Manager r12.6, provisioning server communicates with CA IAM CS, not with CCS. CCS now communicates with CA IAM CS, which then forwards the message.

If your current installation includes a standalone CCS, you need to upgrade it carefully.

Follow these steps:

1. Upgrade CCS.
2. Install CA IAM CS on the same computer as the upgraded CCS.

   This instance of CA IAM CS will forward communication from CCS to the provisioning server.

Upgrade CA IAM Connector Server

The Java Connector Server is now called CA IAM Connector server, or CA IAM CS. This Connector Server uses ServiceMix instead of Apache DS. If you are upgrading from CA Identity Manager r12.5 or a lower release, the upgrade program deletes or moves some files and folders.

Follow these steps:

1. Verify that your customized settings are in the properties files described in Customize the Configuration for CA IAM CS in the *Connectors Guide*. When you upgrade, any changes you made to the configuration files are lost.
2. If you are upgrading a CA Identity Manager r12 installation that had FIPS enabled, FIPS is enabled after the upgrade. To prevent FIPS being enabled after the upgrade, edit the following file *before* upgrading:

   `jcs_home/conf/server_jcs.xml`

   Ensure that the file contains the following property:

   `<property name="fipsEnabled"><value>false</value></property>`

   Alternatively, you can disable FIPS using an override file after the upgrade.
3. Navigate to the following subfolder and double-click the *setup* file:

   `Provisioning\ConnectorServer`
4. When upgrading to CA IAM CS, note the following:
   - Most fields are automatically populated during the CA IAM CS upgrade. You should only need to supply passwords during the upgrade.
   - When providing the component password during the upgrade, you can supply any password that is at least 6 characters long. The installer resets the CA IAM CS component password to te text that you entered in this field.
   - During the upgrade, Upgrade Wizard asks you to register CA IAM CS so that updated metadata for existing and new connectors can be registered with the Provisioning Server.

   Use the following information to register CA IAM CS:

   Domain

   Defines the Provisioning Server domain.

   Server Host

   Defines the Provisioning Server.

   Server Port

   Defines the port on which the Provisioning Server runs.

   Username

   Specifies the Provisioning Server administrator.

Password

Defines the Provisioning Manager administrator password.

5. After the installation is complete, deploy every connector that you plan to use. For instructions, See Add a Connector in the *Connectors Guide*.

   Note: The following connectors each require additional files. If you plan to use any of these connectors, follow the instructions in the Connectors Guide to deploy these additional files as well as the connector itself:

   - IBM Lotus Domino
   - Oracle PeopleSoft
   - RSA SecurID
   - SAP R3

Upgrade the Provisioning Manager

The Provisioning Manager will appear as an option in the Upgrade Wizard. To upgrade the Provisioning Manager, click Launch Upgrade across from this component.

The Provisioning Manager upgrade does not need any new information. Once launched, the upgrade runs and the Provisioning Manager is updated on your system.

Configure a Remote Provisioning Manager

If you installed the Provisioning Manager on a different system from the Provisioning Server, you configure communication to the server.

Note: To install the Provisioning Manager, install the CA Identity Manager Administrative Tools on a Windows system.

Follow these steps:

1. Log in to the Windows system where you installed Provisioning Manager.
2. Go to Start, Programs, CA Identity Manager, Provisioning Manager Setup.
3. Enter the hostname of the Provisioning Server.
4. Click Configure.
5. For an alternate Provisioning Server, select the domain name from the pull-down list.
6. Click Ok.

   You can now start the Provisioning Manager and see the domain name that you configured.

Upgrade Other Provisioning Components

If you use any of the following provisioning components in your CA Identity Manager deployment, they must be upgraded as described.

Connector Xpress

Run the Connector Xpress installer from the CA Identity Manager media to upgrade Connector Xpress.

Remote Agents

Run the specific agent installer from the Provisioning Component media (under \RemoteAgent) to upgrade these components. If you want IPv6 support, you will need to upgrade your agents.

Password Sync Agents

Run the Password Sync Agent installer from the Provisioning Component media (under \Agent) to upgrade this component.

Note: To upgrade the AS400 agent, you uninstall the old version of this agent and install the new agent.

Credential Provider

Run the Credential Provider installer from the Provisioning Component media (under \Agent) to upgrade this component.

Bulk Loader Client/PeopleSoft Feed

Run the Bulk Loader Client installer from the Provisioning Component media (under \Clients) to upgrade this component.

CA IAM CS SDK

Run the CA IAM CS SDK installer from the CA Identity Manager media (under \Provisioning) to upgrade this component.

CCI Standalone

Run the CCI Standalone installer from the Provisioning Component media (under \Infrastructure) to upgrade this component.

Chapter 4: Upgrade on a Single JBoss Node

This section contains the following topics:

Upgrade or Migration on a JBoss Node

At this release, a 64-bit version of JBoss is required. Based on the version of your application server, you upgrade or migrate CA Identity Manager. See the following definitions of these terms:

Upgrade

You leave the existing version of CA Identity Manager installed and install the new CA Identity Manager to replace it.

Migration

You uninstall the previous version of CA Identity Manager installed and install the new CA Identity Manager.

See the following table to choose the correct procedure:

Current Application Server	Upgrade or Migration Procedure
JBoss 4.2 or earlier	Migrate a Node to a New JBoss (see page 42)
JBoss 5.x (32-bit version)	Migrate a Node to a New JBoss (see page 42) to move to JBoss 5 (64-bit) or JBoss 6.1 EAP
JBoss 5.x (64-bit version)	Upgrade on a JBoss 5 Node (see page 42) to remain on JBoss 5, or Migrate a Node to a New JBoss (see page 42) to move to JBoss 6.1 EAP

Upgrade on a JBoss Node

If you are remaining on the same version of JBoss, you can upgrade the CA Identity Manager server.

Follow these steps:

1. Run the CA Identity Manager installer on the system where CA Identity Manager was installed.
2. The Upgrade Wizard starts.
3. Click Launch Upgrade from the Upgrade Wizard.
4. Select the Full Upgrade option.
5. Respond to the prompts that appear.

The following components are upgraded with the installer:

- EAR folder names
- All binaries (jars/JSPs)
- All property files (resource bundles, and so forth)
- All additional JMS queues
- Global Transaction Support on data sources
- Directories and Environments

All unused files will be deleted.

The following custom configuration files will be preserved:

- Policy Server connection
- Data store definitions

Migrate a Node to a new JBoss

Perform the following steps to migrate CA Identity Manager on a node to a new version of JBoss:

✓	Step
	1. Uninstall the CA Identity Manager Server.
	2. Install the new CA Identity Manager Server on the JBoss node.

✓	Step
	3. Perform upgrades from r12 (if you are upgrading from CA Identity Manager r12)

Uninstall the CA Identity Manager Server

Uninstalling this server has no affect on CA Identity Manager environments and directories, which are stored in CA Identity Manager databases. You can still use existing environments and directories after you install the CA Identity Manager server.

To uninstall the CA Identity Manager Server on Windows

1. If you are using SiteMinder in your environment, stop the SiteMinder services.
2. Go to Start, Control Panel, Add/Remove Programs.
3. Select CA IAM Suite (Identity Manager)
4. Click Change/Remove.
5. Select CA Identity Manager.
6. Click Change/Remove.

   All non-provisioning components are uninstalled.

To uninstall CA Identity Manager components on UNIX

1. Navigate to the following location:

   `IM_HOME/../IAM_Suite/IdentityManager/install_config_info/iam-suite-uninstall`
2. Run the following script:

   `sh uninstall.sh`
3. Navigate to the following location:

   IM_HOME/install_config_info/im-uninstall
4. Run the following script:

   `sh uninstall.sh`

For any provisioning components, use the individual component installer to uninstall the component.

Install the CA Identity Manager Server on a JBoss Node

Once you have uninstalled CA Identity Manager server, you can install the CA Identity Manager server.

Note: If you see options to upgrade the workflow database and migrate task persistence data during the installation, enable those options. They appear in some situations when your previous installation was CA Identity Manager r12.

Follow these steps:

1. Install the new version of JBoss.

   Note: (for JBoss 5 only) If you are upgrading CA Identity Manager on a system which already has JBoss 5, perform these steps:

   a. Back up the *jboss_home*\server\all directory on all nodes.

   b. Remove the *jboss_home*\server\all directory.

   c. Install the all directory from the JBoss install source under *jboss_home*\server.

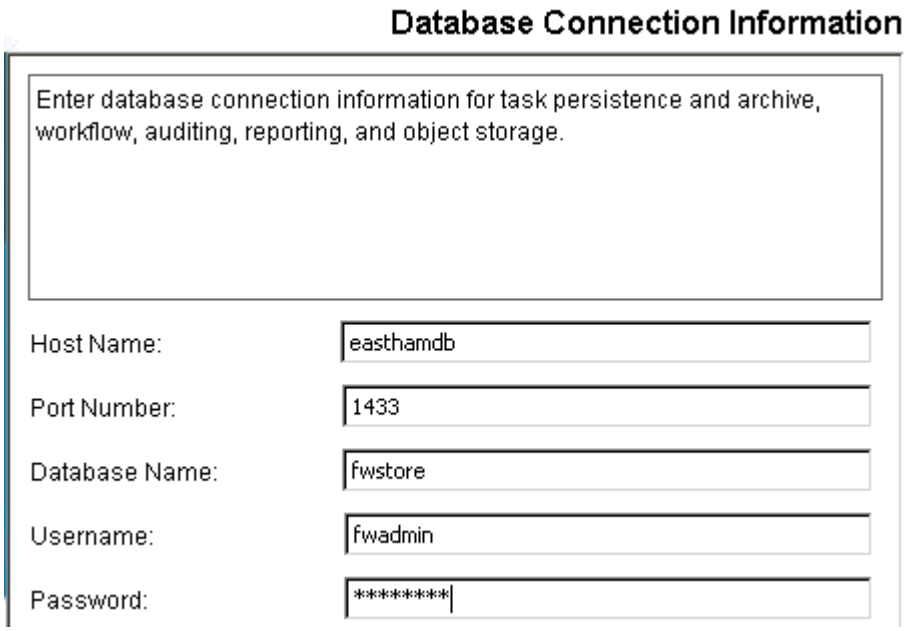
2. Perform a new install of the CA Identity Manager Server.

   - Windows: From your installation media, run the following program:
     `ca-im-release-win32.exe`
   - UNIX: From your installation media, run the installation program. For example, for Solaris:
     `ca-im-release-sol.bin`

   release represents the current release of CA Identity Manager.

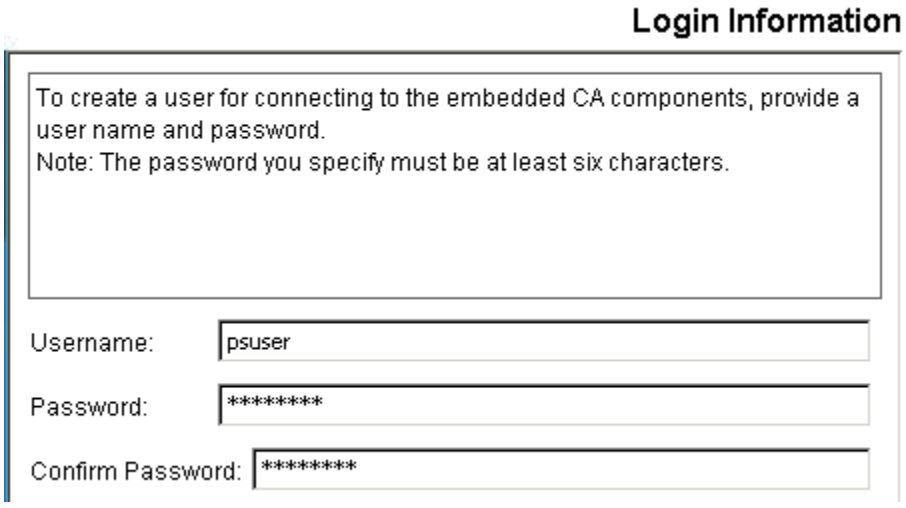
3. Select the option to install the CA Identity Manager Server.

4. Supply the details for the JBoss that you collected in your worksheet (see page 20).
5. For database credentials, provide the same values that existed at the previous installation.



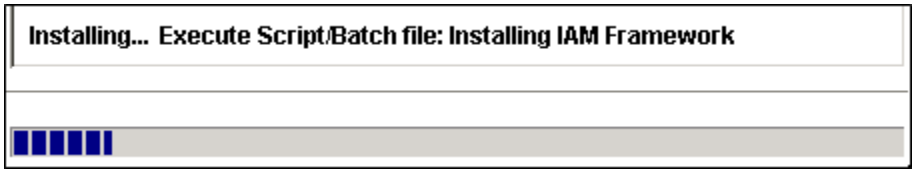
Important! If you are upgrading from CA Identity Manager r12 and you have different database stores for task persistence, workflow, audit, and reports, you will need to update the data sources manually after installation to point to the separate stores.

6. Create a user on the Login Information section using a password you can recall.



7. Review the summary of your upgrade choices and click Install.

   The installer installs the components you selected and gradually update the progress bar.



8. When the installation completes, inspect the Install Complete message. If you see errors on the screen, note the path for the logs, which explain the errors.
9. Install the latest version of the JK Connector and be sure that the workers.properties file has the following parameters set:

```
worker.worker.ping_mode=A
worker.worker.fail_on_status=400,404,500,503
worker.worker.recovery_options=28
```

Perform Upgrades from r12

If you are upgrading CA Identity Manager from r12, perform the following procedures to upgrade the workflow database and migrate task persistence data.

Upgrade the Workflow Database

This procedure applies only if you are upgrading from CA Identity Manager r12.

To work with WorkPoint 3.4.2, you update the workflow database, so you can continue to use the workflow processes that you developed in WorkPoint 3.3.

Follow these steps:

1. Locate the WorkPoint scripts in the Workpoint\database under the Administrative Tools folder. The scripts are in the following default locations:
   - **Windows:** C:\Program Files\CA\Identity Manager\IAM Suite\Identity Manager\tools\Workpoint\database
   - **UNIX:** /opt/CA/IdentityManager/IAM_Suite/Identity_Manager/tools/Workpoint/database
2. Run the following scripts:

   wp331_to_wp34_cnv_step1.sql

   This script creates the tables for Workpoint 3.4, adds columns the old tables, and inserts rows into the WP_*_TYPE tables.

   wp331_to_wp34_cnv_step2.sql

   This script creates the stored procedures that are required to convert the data.

wp331_to_wp34_cnv_step3.sql

This script converts the text data to columns and populates the new WP_BULK_DATA table from the old WP_BULK_STORAGE table.

wp34_20060927_add.sql

This script creates the tables for Workpoint 3.4.20060927 and inserts rows into the WP_INI and WP_*_TYPE tables.

wp34_20070625_add.sql

This script creates the tables for Workpoint 3.4.2.20070625 and inserts rows into the WP_INI and WP_*_TYPE tables.

wp342_20071218_add.sql

This script creates the tables for Workpoint 3.4.2.20071218 and inserts rows into the WP_INI and WP_*_TYPE tables.

wp342b_to_wp342c.sql

This script adds tables and rows to support the completion code.

wp342c_to_wp342d.sql

This script updates field lengths and scripts.

wp342d_to_wp342e.sql

This script adds index definitions.

3. Save all changes to the database.

Migrate Task Persistence Data

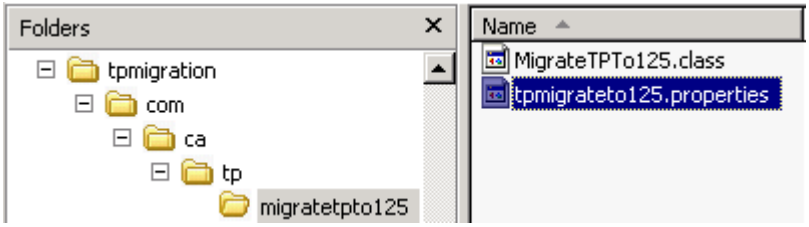
This procedure applies only if you are upgrading from CA Identity Manager r12.

You can manually migrate tasks, depending on task state or date range, by running the task persistence data migration tool.

Follow these steps:

1. Find the tpmigration125.properties file in the following location:

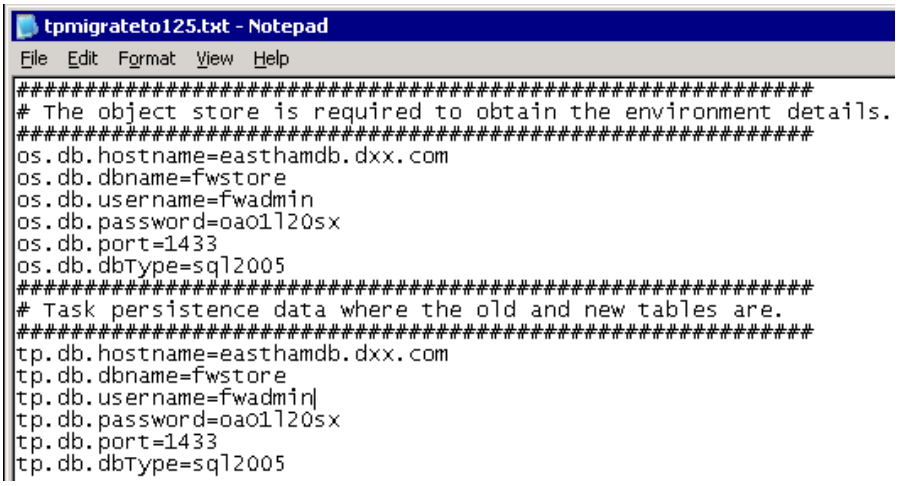
   admin_tools/tpmigration/com/ca/tp/migratetpto125



2. Update this file with the object store and task persistence information for your database.

   Note: For any supported version of SQL Server, enter sql2005.

Equation 1: The user views sections to change in the tipmigrateto125.properties file.



3. Be sure that the environment variable JAVA_HOME is set.
4. From a command line, navigate to *admin_tools*/tpmigration and run the task persistence migration tool as follows:
   - For Windows:
     `runmigration.bat`
   - For UNIX:
     `runmigration.sh`
5. Enter the following information:
   a. For the environment protected Alias, enter all.

      Note: If you do not specify all, only one environment can be entered.

   b. For task state, enter All (with a Capital A).
      Note: If you do not specify All, only one task state can be entered.

   c. For the version to migrate from, enter 2 for 12.0.

   d. Date range for the tasks to be migrated (y/n).

      Note: If you choose 'y', enter a Start Date (mm/dd/yy) and End Date (mm/dd/yy).

   The migration starts. After the migration completes, the status indicates how many tasks were migrated.
6. Be sure to verify that no errors appeared.
7. Repeat steps 4 and 5, but use the -pending option instead of All for task state.

Verify the Upgraded Node

When you have completed all the steps, check that the upgrade was successful.

To verify the upgraded node

1. Start the databases used by the CA Identity Manager server.
2. Start any extra Policy Servers and CA Identity Manager nodes that you stopped.
3. Access the Management Console and confirm the following points:
   - You can access the following URL from a browser:

     http://*im_server*:*port*/iam/immanage

     For example:

     http://MyServer.MyCompany.com:*port-number*/iam/immanage
   - The Management Console opens.

- No errors are displayed in the application server log.
- You do not receive an error message when you click the Directories link.

4. Verify that you can access an upgraded environment using this URL format:

   http://*im_server*:*port*/iam/im/*environment*

Chapter 5: Upgrade on a JBoss Cluster

This section contains the following topics:

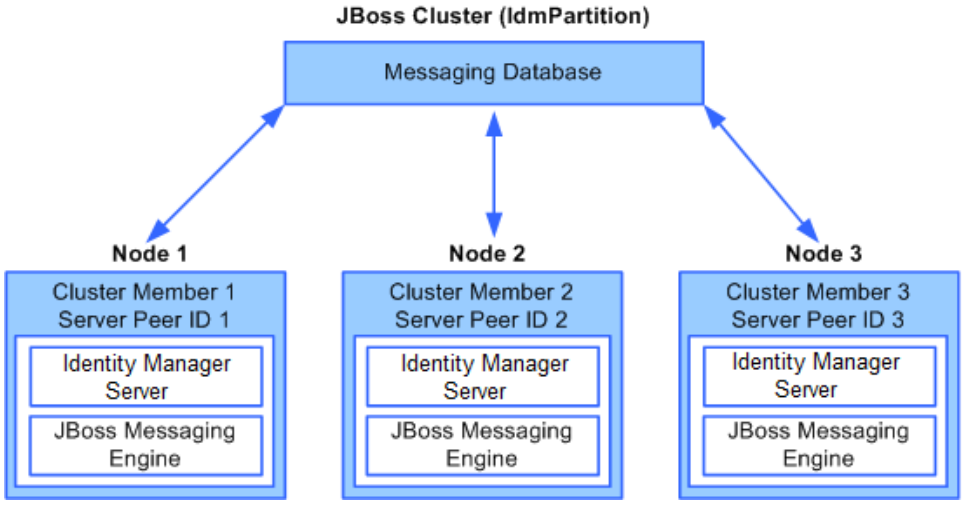
Sample Installations on a JBoss Cluster

The following topics illustrate the JBoss cluster architecture supported by CA Identity Manager 12.6.4:

CA Identity Manager on a JBoss 5 Cluster

In configuring JBoss clustering, you create a master node and it is usually the node that starts first in the cluster. As other nodes start, they receive deployment files from the master node. If the master node fails, another node becomes the new master node.

The following JBoss 5 figure shows the relationship between the nodes and cluster members. Each node contains one cluster member. Each member of the cluster has a unique Server Peer ID. The master node would be cluster member 1, assuming it was created first.



In this figure, the messaging database is a central store for cluster members to share messages and each node contains three components:

CA Identity Manager Server

Provides the core functionality of the product.

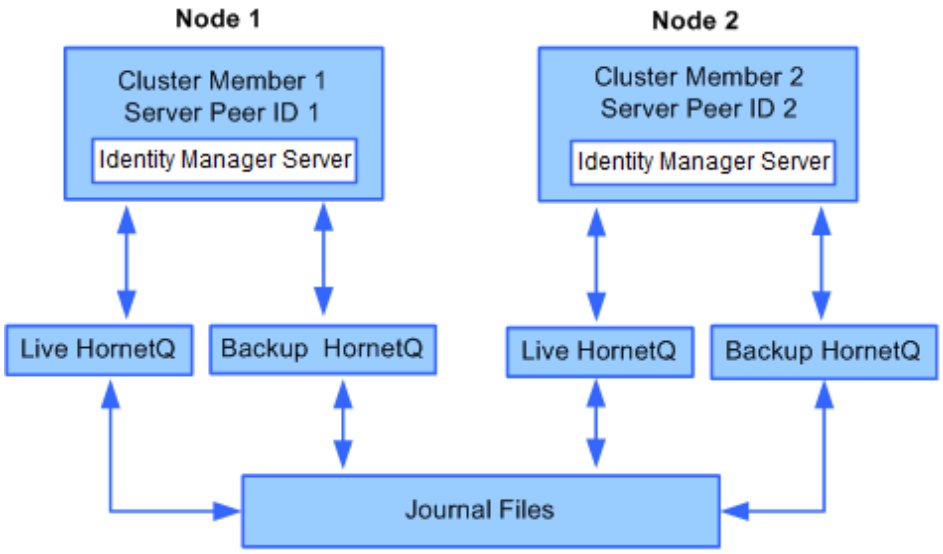
JBoss Messaging Engine

Provides messaging functionality for members of the cluster using JMS.

CA Identity Manager on a JBoss 6.1 Cluster

On JBoss Enterprise Application Platform (EAP) 6.1, CA Identity Manager supports clusters that use either the unicast or multicast form of communication between nodes. In either type of cluster, you create a master node and it is usually the node that starts first in the cluster. As other nodes start, they receive deployment files from the master node. If the master node fails, another node becomes the new master node.

For example, consider the situation where you have a cluster of two nodes. The following figure shows the relationship between the nodes and cluster members. Each node contains one cluster member. Each member of the cluster has a unique Server Peer ID. The master node would be cluster member 1, assuming it was created first.



In this figure, the following components exist:

CA Identity Manager Server

Provides the core functionality of the product.

Live and Backup HornetQ Instances

Provides messaging functionality for members of the cluster. On each node, you configure two HornetQ instances, a live instance and a backup.

Journal Files

Persists HornetQ messages using journal files without using a database. You configure each HornetQ instance to store journal files. In this example, all nodes share a set of journal files, which are on a Storage Area Network (SAN) Server. This scenario is referred to as a Shared Store.

In you choose Replication instead of a Shared Store during installation, journal files are stored on each node.

Decide to Use Unicast or Multicast

If you install CA Identity Manager on JBoss 6.1 EAP, you can use either unicast or multicast as the messaging protocol. This protocol is the means of communication between nodes in the cluster. We recommend testing both options to determine the best choice for your organization.

Consider unicast in these situations:

- The servers in your JBoss cluster are on different subnets. This situation commonly exists when you install a JBoss cluster on virtual machines.
- If network congestion is a concern, unicast helps to reduce how many packets are sent between cluster nodes.

Consider multicast in these situations:

- Default deployment of JBoss on a single network
- JBoss 5 is required for the cluster.

Upgrade or Migration on a JBoss Cluster

Based on the version of your application server, you upgrade or migrate CA Identity Manager. See the following definitions of these terms:

Upgrade

You leave the existing version of CA Identity Manager installed and install the new CA Identity Manager to replace it.

Migration

You uninstall the previous version of CA Identity Manager installed and install the new CA Identity Manager.

See the following table to choose the correct procedure:

Current Application Server	Procedure to Perform
JBoss 4.2 or earlier JBoss 5.x (32-bit version)	Perform either of these procedures: ■ Migrate a Cluster to JBoss 5 (64-bit) (see page 56) ■ Migrate a Cluster to JBoss 6.1 EAP (see page 61)
JBoss 5.x (64-bit version)	Perform either of these procedures: ■ Upgrade on a JBoss Cluster (see page 55) to remain on JBoss 5 ■ Migrate a Cluster to JBoss 6.1 EAP (see page 61)

Current Application Server	Procedure to Perform
JBoss 6.1 EAP	Upgrade on a JBoss Cluster (see page 55) to remain on JBoss 6.1 and continue to use multicast

Note: If you are upgrading CA Identity Manager on JBoss 6.1 EAP and intend to switch from multicast to unicast or from a shared store to replication, you modify the standalone.sh/bat and standalone-full-ha.xml files. See the JBoss documentation for help.

Upgrade on a JBoss Cluster

This procedure applies if you plan to continue using the currently installed version of JBoss (5.x 64-bit or 6.1 EAP with multicast). Upgrade the CA Identity Manager server by using this procedure.

Follow these steps:

1. Run the CA Identity Manager installer on the system where CA Identity Manager is installed.

   The Upgrade Wizard starts.
2. Click Launch Upgrade from the Upgrade Wizard.
3. Select the Full Upgrade option.
4. Respond to the prompts that appear.
5. Repeat these steps on the other systems where CA Identity Manager is installed.

The following components are upgraded with the installer:

- EAR folder names
- All binaries (jars/JSPs)
- All property files (resource bundles, and so forth)
- All additional JMS queues
- Global Transaction Support on data sources
- Directories and Environments

All unused files will be deleted.

The following custom configuration files will be preserved:

- Policy Server connection
- Data store definition

Migrate a Cluster to JBoss 5 (64-bit)

The following procedures describe how to migrate a JBoss 4.2 or 5 (32-bit) cluster to JBoss 5 (64-bit).

✓	Step
	1. Uninstall the CA Identity Manager server.
	2. Test the default multicast address.
	3. Create the master node.
	4. Add cluster nodes.
	5. Configure the JK connector.
	6. Perform upgrades from r12 (if you are upgrading from CA Identity Manager r12)

Uninstall the CA Identity Manager Server

Uninstalling this server has no affect on CA Identity Manager environments and directories, which are stored in CA Identity Manager databases. You can still use existing environments and directories after you install the CA Identity Manager server.

To uninstall the CA Identity Manager Server on Windows

1. If you are using SiteMinder in your environment, stop the SiteMinder services.
2. Go to Start, Control Panel, Add/Remove Programs.
3. Select CA IAM Suite (Identity Manager)
4. Click Change/Remove.
5. Select CA Identity Manager.
6. Click Change/Remove.

   All non-provisioning components are uninstalled.

To uninstall CA Identity Manager components on UNIX

1. Navigate to the following location:

   `IM_HOME/../IAM_Suite/IdentityManager/install_config_info/iam-suite-uninstall`

2. Run the following script:

   `sh uninstall.sh`

3. Navigate to the following location:

   IM_HOME/install_config_info/im-uninstall

4. Run the following script:

   `sh uninstall.sh`

For any provisioning components, use the individual component installer to uninstall the component.

Test the Default Multicast Address

Use this procedure to test if you can use the default multicast address. The run script uses a multicast address, either the default address or an alternative address supplied by your network administrator.

The first part of the test may succeed, but subsequent parts of this test may fail. Therefore, perform full testing in different directions to determine the reliability of multicast for your installation.

Follow these steps:

1. Install JBoss and the JDK on the computer.
2. Run sender on first node as follows:
   a. Navigate to the lib folder.
      - On a JBoss 5 node, navigate to jboss-home-1/server/all/lib.
      - On a JBoss 6.1 node, navigate to jboss-eap-6.1\modules\system\layers\base\org\jgroups\main.

   b. Run the following command:

      java -cp jgroups-3.2.7.Final-redhat-1.jar org.jgroups.tests.McastSenderTest -mcast_addr 224.10.10.10 -port 5555

3. Run receivers on other nodes in the cluster as follows:
   a. Navigate to the lib folder.
      - On a JBoss 5 node, navigate to jboss-home-1/server/all/lib.
      - On a JBoss 6.1 node, navigate to jboss-eap-6.1\modules\system\layers\base\org\jgroups\main.

b. Run the following command:

java -cp jgroups-3.2.7.Final-redhat-1.jar org.jgroups.tests.McastReceiverTest -mcast_addr 224.10.10.10 -port 5555

4. Send a message from the first node as follows:
   a. On the console of the first node, enter any text and press enter.
   b. Confirm that a reply appears, to acknowledge the text was sent.
   c. Confirm that the message appears on the console of all other nodes in the cluster.
   d. If either the send or receive test fails, ask your network administrator to provide a multicast address that works and repeat this test.

Create the Master Node for JBoss 5

You begin creating the JBoss 5 cluster by creating the master node, the first node in the cluster.

Follow these steps:

1. Install JBoss and the JDK on the computer.
2. Start the CA Identity Manager installation program.
   - Windows: From your installation media, run the following program:

     `ca-im-`*`release`*`-win32.exe`
   - UNIX: From your installation media, run the installation program. For example, for Solaris:

     `ca-im-`*`release`*`-sol.bin`

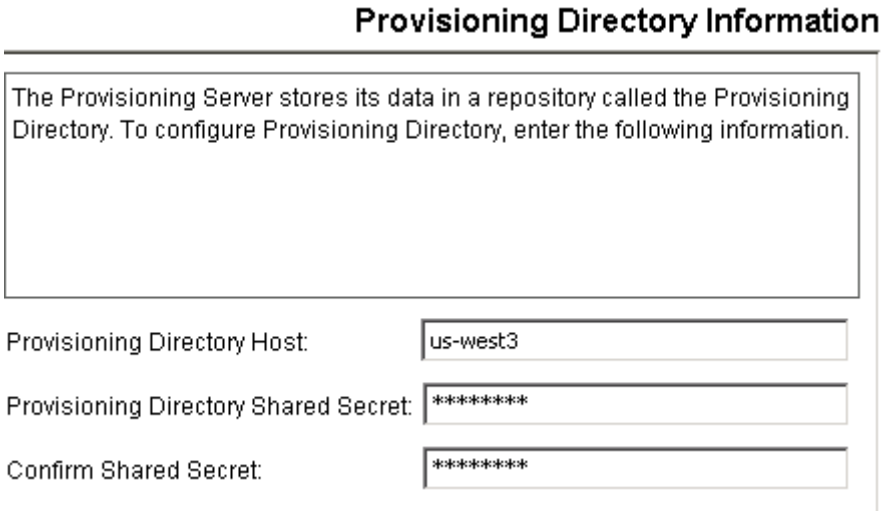
   release represents the current release of CA Identity Manager.

   Important! Make sure that you have the collected the information needed by the installer (see page 20), such as user names, host names, and ports.
3. Complete the section requesting database credentials by entering the same values from the previous release of CA Identity Manager.

   If you are starting from CA Identity Manager r12 and you have different database stores for task persistence, workflow, audit, and reports, update the data sources manually after installation to point to the separate stores.

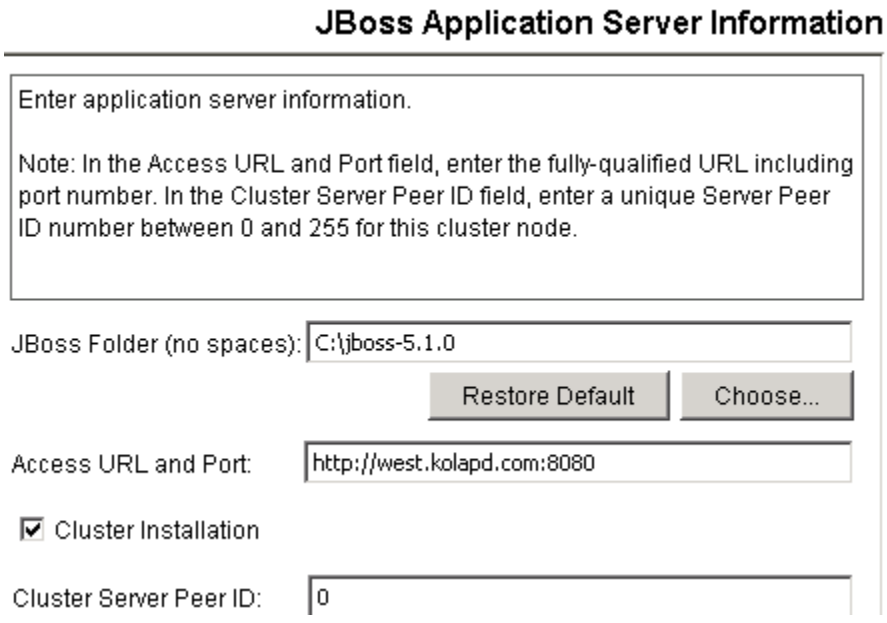
   Note: If you see options to upgrade the workflow database and migrate task persistence data during the installation, enable those options.
4. Complete the Select Components section by including the CA Identity Manager Server and any other components that you need on this system.
5. Complete the other sections based on your requirements for the installation.

6. When you enter any password or shared secret in the installation, be sure to provide a password that you can recall when needed.



7. Complete the JBoss Application Server Information page as follows:
   a. Enter the Access Server URL and port with the URL and port number of the web server used for load balancing.
   b. Select Cluster Installation.
   c. Enter a Peer ID, a unique number between 0 and 255. Make a record of the Peer ID, so that you use a different number for other nodes.

Figure 1: The user enters JBoss information.



8. If the multicast address test failed, perform one of the next two steps for Windows or Solaris.
9. On a Windows system, edit run.bat in the *jboss_home*\bin directory:
   a. Locate the line that begins as follows:
      `ARGS="${ARGS}`
   b. Add a multicast address preceded by the -u argument as follows:
      `ARGS="${ARGS} -g IdmPartition -Djboss.messaging.ServerPeerID=PeerID -u multicast-address"`
   c. If you are installing on a system that supports IPv6/IPv4, uncomment the IDM_OPTS entry:
      `set IDM_OPTS=%IDM_OPTS% -Djava.net.preferIPv4Stack=true`
10. For a Solaris system, edit run.sh in the *jboss_home*\bin directory:
   a. Locate the line that begins as follows:
      `ARGS="${ARGS}`
   b. Add a multicast address preceded by the -u argument as follows:
      `ARGS="${ARGS} -g IdmPartition -Djboss.messaging.ServerPeerID=PeerID -u multicast-address"`
   c. If you are installing on a system that supports IPv6, modify one of the following properties in the IDM_OPTS entry:
      - For IPv6 only systems, uncomment the following entry:
        `IDM_OPTS="$IDM_OPTS -Djava.net.preferIPv6Addresses=true"`
      - For IPv6/IPv4 systems, uncomment the following entry:
        `IDM_OPTS="$IDM_OPTS -Djava.net.preferIPv4Stack=true"`

If any issues occur during installation, inspect the installation logs.

Add Cluster Nodes for JBoss 5

We recommend that you install each cluster node on a separate system. However, if you install all nodes on one system, each node needs a separate jboss_home. This precaution is necessary to avoid contention over the workpoint.log in the *jboss_home*/bin directory.

Follow these steps:

1. Install JBoss and the JDK on the computer.
2. Install the CA Identity Manager server on that system.
   - Windows: From your installation media, run the following program:
     `ca-im-release-win32.exe`
   - UNIX: From your installation media, run the following program:
     `ca-im-release-sol.bin`

   release represents the current release of CA Identity Manager.
3. Be sure to supply the same values for FIPS, SiteMinder, database, and shared secret details and all other values entered for the master node.
4. Select Cluster Installation.
5. Enter a Peer ID that is different from the other nodes you have created.
6. If the multicast address test failed, edit the MULTI_CAST_ADDRESS value in the run.bat or run.sh file. Enter a unique multicast address.
7. If you are installing on a system that supports IPv6, modify one of the following properties in the IDM_OPTS entry in the standalone.bat or standalone.sh file:
   - For IPv6 only systems on Solaris, uncomment the following entry:
     `IDM_OPTS="$IDM_OPTS -Djava.net.preferIPv6Addresses=true"`
   - For IPv6/IPv4 systems, uncomment the following entry:
     `IDM_OPTS="$IDM_OPTS -Djava.net.preferIPv4Stack=true"`

If any issues occur during installation, inspect the installation logs.

Migrate a Cluster to JBoss 6.1 EAP

The following procedures describe how to migrate a JBoss 5 or lower cluster to 6.1 EAP using either unicast or multicast communication..

✓	Step
	1. Uninstall the CA Identity Manager server.
	2. Test the default multicast address (if you plan to stay on multicast)
	3. Create the master node.
	4. Add cluster nodes.
	5. Configure journal files (if you plan to use unicast)
	6. Configure the JK connector.

✓	Step
	7. Perform upgrades from r12 (if you are upgrading from CA Identity Manager r12)

Uninstall the CA Identity Manager Server

Uninstalling this server has no affect on CA Identity Manager environments and directories, which are stored in CA Identity Manager databases. You can still use existing environments and directories after you install the CA Identity Manager server.

To uninstall the CA Identity Manager Server on Windows

1. If you are using SiteMinder in your environment, stop the SiteMinder services.
2. Go to Start, Control Panel, Add/Remove Programs.
3. Select CA IAM Suite (Identity Manager)
4. Click Change/Remove.
5. Select CA Identity Manager.
6. Click Change/Remove.

   All non-provisioning components are uninstalled.

To uninstall CA Identity Manager components on UNIX

1. Navigate to the following location:

   `IM_HOME/../IAM_Suite/IdentityManager/install_config_info/iam-suite-uninstall`
2. Run the following script:

   `sh uninstall.sh`
3. Navigate to the following location:

   IM_HOME/install_config_info/im-uninstall
4. Run the following script:

   `sh uninstall.sh`

For any provisioning components, use the individual component installer to uninstall the component.

Test the Default Multicast Address

Use this procedure to test if you can use the default multicast address. The run script uses a multicast address, either the default address or an alternative address supplied by your network administrator.

The first part of the test may succeed, but subsequent parts of this test may fail. Therefore, perform full testing in different directions to determine the reliability of multicast for your installation.

Follow these steps:

1. Install JBoss and the JDK on the computer.
2. Run sender on first node as follows:
   a. Navigate to the lib folder.
      - On a JBoss 5 node, navigate to jboss-home-1/server/all/lib.
      - On a JBoss 6.1 node, navigate to jboss-eap-6.1\modules\system\layers\base\org\jgroups\main.
   b. Run the following command:

      java -cp jgroups-3.2.7.Final-redhat-1.jar org.jgroups.tests.McastSenderTest -mcast_addr 224.10.10.10 -port 5555
3. Run receivers on other nodes in the cluster as follows:
   a. Navigate to the lib folder.
      - On a JBoss 5 node, navigate to jboss-home-1/server/all/lib.
      - On a JBoss 6.1 node, navigate to jboss-eap-6.1\modules\system\layers\base\org\jgroups\main.
   b. Run the following command:

      java -cp jgroups-3.2.7.Final-redhat-1.jar org.jgroups.tests.McastReceiverTest -mcast_addr 224.10.10.10 -port 5555
4. Send a message from the first node as follows:
   a. On the console of the first node, enter any text and press enter.
   b. Confirm that a reply appears, to acknowledge the text was sent.
   c. Confirm that the message appears on the console of all other nodes in the cluster.
   d. If either the send or receive test fails, ask your network administrator to provide a multicast address that works and repeat this test.

Create the Master Node for JBoss 6.1

You begin creating the JBoss 6.1 cluster by creating the master node, the first node in the cluster.

Follow these steps:

1. Install JBoss and the JDK on the computer.
2. Start the CA Identity Manager installation program.

- Windows: From your installation media, run the following program:
  `ca-im-release-win32.exe`
- UNIX: From your installation media, run the installation program. For example, for Solaris:
  `ca-im-release-sol.bin`

release represents the current release of CA Identity Manager.

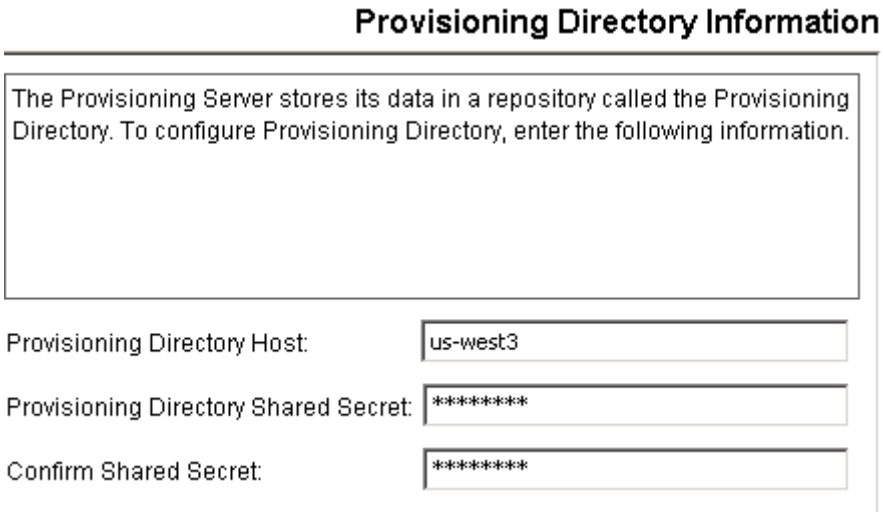
Important! Make sure that you have the collected the information needed by the installer (see page 20), such as user names, host names, and ports.

3. Complete the section requesting database credentials by entering the same values from the previous release of CA Identity Manager.

   If you are starting from CA Identity Manager r12 and you have different database stores for task persistence, workflow, audit, and reports, update the data sources manually after installation to point to the separate stores.

   Note: If you see options to upgrade the workflow database and migrate task persistence data during the installation, enable those options.

4. Complete the Select Components section by including the CA Identity Manager Server and any other components that you need on this system.
5. Complete the other sections based on your requirements for the installation.
6. When you enter any password or shared secret in the installation, be sure to provide a password that you can recall when needed.



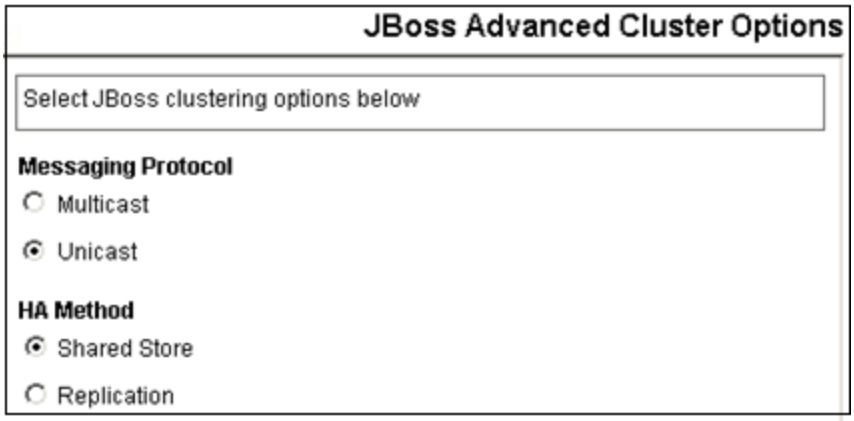
7. Complete the JBoss Application Server Information page as follows:
   a. Enter the Access Server URL and port with the URL and port number of the web server used for load balancing.
   b. Select Cluster Installation.
   c. Enter a Peer ID, a unique number between 0 and 255. Make a record of the Peer ID, so that you use a different number for other nodes.

8. Select the Advanced Cluster Options.
   - Choose Multicast or Unicast as the messaging protocol.
   - Choose Shared Store or Replication for high availability.

     A shared store requires a Storage Area Network (SAN) server to store journal files.

     Replication stores journal files on each node.

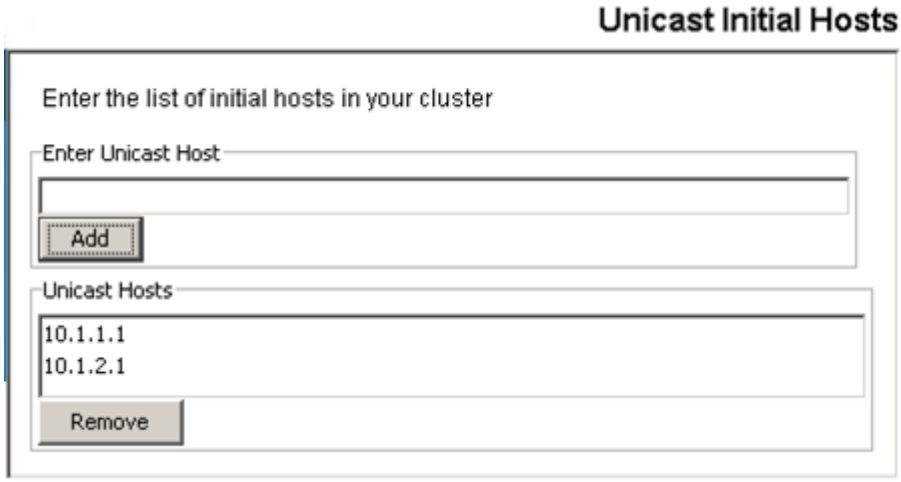
Figure 2: Choose Advanced Options



9. If you chose multicast, skip to the next step.

   Supply a list of unicast initial hosts of the systems where JBoss is installed.

Figure 3: Add initial hosts in JBoss cluster



10. If you chose Unicast, skip to the next step.

    If the multicast address test failed, edit the MULTI_CAST_ADDRESS value in the standalone.bat or standalone.sh file. Enter a unique multicast address.

11. If you are installing on a system that supports IPv6, modify one of the following properties in the IDM_OPTS entry in the standalone.bat or standalone.sh file:

    - For IPv6 only systems on Solaris, uncomment the following entry:
      `IDM_OPTS="$IDM_OPTS -Djava.net.preferIPv6Addresses=true"`
    - For IPv6/IPv4 systems, uncomment the following entry:
      `IDM_OPTS="$IDM_OPTS -Djava.net.preferIPv4Stack=true"`

12. If any issues occur during installation, inspect the installation logs.

Add Cluster Nodes for JBoss 6.1

We recommend that you install each cluster node on a separate system. However, if you install all nodes on one system, each node needs a separate jboss_home. This precaution is necessary to avoid contention over the workpoint.log in the *jboss_home*/bin directory.

Follow these steps:

1. Install JBoss and the JDK on the computer.
2. Install the CA Identity Manager server on that system.

    - Windows: From your installation media, run the following program:
      `ca-im-`*`release`*`-win32.exe`
    - UNIX: From your installation media, run the following program:
      `ca-im-`*`release`*`-sol.bin`

    release represents the current release of CA Identity Manager.

3. Be sure to supply the same values for FIPS, SiteMinder, database, and shared secret details and all other values entered for the master node.
4. Select Cluster Installation.
5. Enter a Peer ID that is different from the other nodes you have created.
6. Select the Advanced Cluster Options, matching the choices you made in the master node procedure.
7. If you chose multicast, skip to the next step.

    Confirm the same set of unicast initial hosts you supplied for the master node.

8. If you chose unicast, skip to the next step.

    If the multicast address test failed, edit the MULTI_CAST_ADDRESS value in the standalone.bat or standalone.sh file. Enter a unique multicast address.

9. If you are installing on a system that supports IPv6, modify one of the following properties in the IDM_OPTS entry in the standalone.bat or standalone.sh file:
   - For IPv6 only systems on Solaris, uncomment the following entry:
     `IDM_OPTS="$IDM_OPTS -Djava.net.preferIPv6Addresses=true"`
   - For IPv6/IPv4 systems, uncomment the following entry:
     `IDM_OPTS="$IDM_OPTS -Djava.net.preferIPv4Stack=true"`

If any issues occur during installation, inspect the installation logs.

Configure Journal Files

To implement high availability on JBoss 6.1 EAP, CA Identity Manager uses the HornetQ messaging provider. HornetQ persists messages using journal files without using a database. CA Identity Manager stores journal files based on the following installation choice:

- Replication method -- CA Identity Manager stores journal files on each node.
- Shared Store -- CA Identity Manager stores journal files on a Storage Area Network (SAN) Server.

Journal Files for Replication

If you chose Replication during the installation, the installation program configured the first node with two HornetQ instances, a live instance and a backup. On each additional node, you configure live and backup HornetQ instances.

Follow these steps:

1. On the second node in the cluster, navigate to the following location:

   `jboss_home/standalone/configuration`
2. Edit the standalone-full-ha.xml file.
3. Replace each occurrence of *node1* with *node2.*
4. Replace each occurrence of *node2* with *node1*.
5. For a cluster of three or more nodes, edit standalone-full-ha.xml in a similar manner.

   For example, make these changes for a three-node cluster:
   - Node 1
     - A live HornetQ is a member of backup group *node1*
     - Backup HornetQ is a member of backup group *node2*
   - Node 2
     - A live HornetQ is a member of backup group *node2*
     - Backup HornetQ is a member of backup group *node3*

- Node 3
  - A live HornetQ is a member of backup group *node3*
  - Backup HornetQ is a member of backup group *node1*

Journal Files for a Shared Store

If you chose Shared Store during the installation, you configure two HornetQ instances, a live instance and a backup, on each node. You configure each instance to store journal files on a Storage Area Network (SAN) Server.

Follow these steps:

1. Create a SAN Server with paths to each node.

   For example, if you have a two-node cluster, you configure a SAN Server with paths of *//network-path/node1* and *//network-path/node2*.

2. On the first node, navigate to the following location:
   `jboss_home/standalone/configuration`
3. Edit the standalone-full-ha.xml file.
4. Locate the <hornetq-server> section of the file.
5. Uncomment the section and set the paths for the correct directories.

```
<!-- un mark this for node 1 and set your path until node1jr
<paging-directory path="//network/path/node1jr/paging"/>
   <bindings-directory path="//network/path/node1jr/bindings"/>
   <journal-directory path="//network/path/node1jr/journal"/>
   <large-messages-directory
path="//network/path/node1jr/large-messages"/>
-->
```

6. Locate the <hornetq-server name="backup"> section of the file.
7. Uncomment this section and set the paths for the correct directories.

```
<!-- un mark this for node 1 backup (which is node2jr) and set your
path until node2jr
 <paging-directory path="//network/path/node2jr/paging"/>
 <bindings-directory path="//network/path/node2jr/bindings"/>
 <journal-directory path="//network/path/node2jr/journal"/>
 <large-messages-directory
path="//network/path/node2jr/large-messages"/>
-->
```

8. Repeat this procedure for the second node in the cluster, replacing *node1* with *node2* and *node2* with *node1*.
9. For a cluster of three or more nodes, edit the standalone-full-ha.xml file in a similar manner.

   For example, in a three-node cluster, make these changes:

- Node 1
  - A live HornetQ points at *network-path*/*node1*
  - Backup HornetQ points at *network-path*/*node2*
- Node 2
  - A live HornetQ points at *network-path*/*node2*
  - Backup HornetQ points at /network/path/*node3*
- Node 3
  - A live HornetQ points at *network-path*/*node3*
  - Backup HornetQ points at *network-path*/*node1*

Configure the JK Connector

Follow these steps:

1. Install a JK connector based on these instructions:

   http://community.jboss.org/wiki/usingmodjk12withjboss

2. Note the following when you use this procedure:

   a. When you configure the modjk workers, use the workers.properties file in this location:

   Windows: C:\Program Files\CA\Identity Manager\IAM Suite\Identity Manager\tools\samples\ConnectorConfiguration\windows\IIS_JBoss

   UNIX: /opt/CA/IdentityManager/IAM_Suite/Identity_Manager/tools/samples/Cluster/JBoss/ConnectorConfiguration

   b. In this file, replace worker.worker*N*.* (the worker name) with your corresponding node's Peer ID.

   If you have more than two nodes, copy a worker.workerN.* set for each additional node and rename the worker name.

   c. Fill in the worker.worker*N*.host field with your corresponding nodes' hostnames.

   For example, consider a cluster where the CA Identity Manager server is installed on three JBoss hosts named myhostA, myhostB, and myhostC, using Peer IDs 1, 2, and 3. The workers.properties file appears as follows:

```
worker.worker1.port=8009
worker.worker1.host=myhostA
.
.
```

```
worker.worker1.recovery_options=28

worker.worker2.port=8009
worker.worker2.host=myhostB
.
.
worker.worker2.recovery_options=28

worker.worker3.port=8009
worker.worker3.host=myhostC
.
.
worker.worker3.recovery_options=28
.
.
worker.router.balance_workers=worker1,worker2,worker3
```

d. Copy the uriworkermap.properties file in the above location to *APACHE_HOME*/conf.

e. Omit the step about configuring Tomcat for session stickiness. This feature is already configured by the installer and in the workers.properties file.

Perform Upgrades from r12

If you are upgrading CA Identity Manager from r12, perform the following procedures to upgrade the workflow database and migrate task persistence data.

Upgrade the Workflow Database

This procedure applies only if you are upgrading from CA Identity Manager r12.

To work with WorkPoint 3.4.2, you update the workflow database, so you can continue to use the workflow processes that you developed in WorkPoint 3.3.

Follow these steps:

1. Locate the WorkPoint scripts in the Workpoint\database under the Administrative Tools folder. The scripts are in the following default locations:
   - **Windows:** C:\Program Files\CA\Identity Manager\IAM Suite\Identity Manager\tools\Workpoint\database
   - **UNIX:** /opt/CA/IdentityManager/IAM_Suite/Identity_Manager/tools/Workpoint/database
2. Run the following scripts:

   wp331_to_wp34_cnv_step1.sql

   This script creates the tables for Workpoint 3.4, adds columns the old tables, and inserts rows into the WP_*_TYPE tables.

   wp331_to_wp34_cnv_step2.sql

   This script creates the stored procedures that are required to convert the data.

   wp331_to_wp34_cnv_step3.sql

   This script converts the text data to columns and populates the new WP_BULK_DATA table from the old WP_BULK_STORAGE table.

   wp34_20060927_add.sql

   This script creates the tables for Workpoint 3.4.20060927 and inserts rows into the WP_INI and WP_*_TYPE tables.

   wp34_20070625_add.sql

   This script creates the tables for Workpoint 3.4.2.20070625 and inserts rows into the WP_INI and WP_*_TYPE tables.

   wp342_20071218_add.sql

   This script creates the tables for Workpoint 3.4.2.20071218 and inserts rows into the WP_INI and WP_*_TYPE tables.

   wp342b_to_wp342c.sql

   This script adds tables and rows to support the completion code.

   wp342c_to_wp342d.sql

   This script updates field lengths and scripts.

wp342d_to_wp342e.sql

This script adds index definitions.

3. Save all changes to the database.

Migrate Task Persistence Data

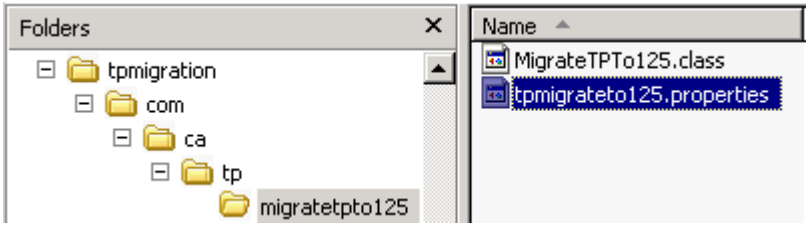
This procedure applies only if you are upgrading from CA Identity Manager r12.

You can manually migrate tasks, depending on task state or date range, by running the task persistence data migration tool.

Follow these steps:

1. Find the tpmigration125.properties file in the following location:

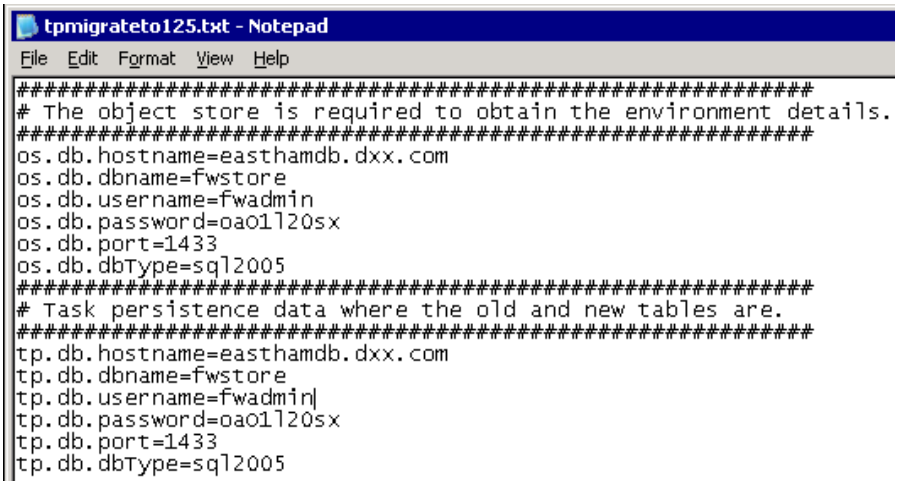
   admin_tools/tpmigration/com/ca/tp/migratetpto125



2. Update this file with the object store and task persistence information for your database.

   Note: For any supported version of SQL Server, enter sql2005.

Equation 2: The user views sections to change in the tipmigrateto125.properties file.



3. Be sure that the environment variable JAVA_HOME is set.
4. From a command line, navigate to *admin_tools*/tpmigration and run the task persistence migration tool as follows:
   - For Windows:
     `runmigration.bat`
   - For UNIX:
     `runmigration.sh`
5. Enter the following information:
   a. For the environment protected Alias, enter all.

      Note: If you do not specify all, only one environment can be entered.

   b. For task state, enter All (with a Capital A).
      Note: If you do not specify All, only one task state can be entered.

   c. For the version to migrate from, enter 2 for 12.0.

   d. Date range for the tasks to be migrated (y/n).

      Note: If you choose 'y', enter a Start Date (mm/dd/yy) and End Date (mm/dd/yy).

   The migration starts. After the migration completes, the status indicates how many tasks were migrated.
6. Be sure to verify that no errors appeared.
7. Repeat steps 4 and 5, but use the -pending option instead of All for task state.

Start the JBoss Cluster

Once all configuration is complete, start all servers in the following order.

Follow these steps:

1. Start one of the SiteMinder Policy Servers that supports CA Identity Manager.

   Note: If you have a Policy Server cluster, make sure that only one Policy Server is running while you create CA Identity Manager directories, create or modify CA Identity Manager environments, or change WorkPoint settings.

2. From a command line, navigate to:

   jboss_home/bin

3. Start the CA Identity Manager server by entering the following command:
   - For JBoss 5 on Windows:

     run.bat -c all
   - For JBoss 5 on UNIX:

     ./run.sh -c all
   - For JBoss 6.1 on Windows:

     standalone.bat
   - For JBoss 6.1 on UNIX:

     ./standalone.sh
4. Wait for a message that shows that the server has started. This message similar to the following message appears in a console window:

   ```
   DATE+TIME INFO  [com.sun.jersey.server.impl.application.WebApplicationImpl]
   (main) Initiating Jersey application, version 'Jersey: 1.1.5.1 DATE+TIME'
   ```
5. If you have already installed a SiteMinder Web Agent, start the Web Server where you installed the SiteMinder Web Agent and the application server proxy plug-in.

Verify the Clustered Installation

When you have completed all steps and started the cluster, check that the installation was successful.

Follow these steps:

1. Start the databases used by the CA Identity Manager server.
2. Start any extra Policy Servers and CA Identity Manager nodes that you stopped.
3. Access the Management Console and confirm the following points:
   - You can access the following URL from a browser:

     http://*Identity_Manager_server_node:port*/iam/immanage

     For example:

     http://MyServer.MyCompany.com:*port-number/*iam/immanage
   - The Management Console opens.
   - No errors are displayed in the application server log.
   - You do not receive an error message when you click the Directories link.
4. Verify that you can access an upgraded environment using this URL format:

   http://*web_server_proxy_host*/iam/im/*environment*

Chapter 6: Report Server Upgrade

If you currently use reporting in CA Identity Manager, you need to upgrade the Report Server and the CA Identity Manager default reports.

This section contains the following topics:

Upgrade the Report Server

Upgrade the Report Server to the supported version, CA Business Intelligence 3.3 SP1 (BusinessObjects Enterprise XI Release 3.1 SP6). Previous versions of this software are not supported.

Note: You need at least 9GB of disk space to install or upgrade the Report Server.

To upgrade the Report Server

1. Exit all applications that are running.
2. Log in to the CA Support site.
3. Go to the Download Center.
4. Under Products, click CA Identity Manager and the current release.
5. Download the CA Business Intelligence Common Reporting package and unzip it. If you have already installed CA Business Intelligence 3.3, you can omit this procedure. Instead, install service pack 6 (see page 76).

   Important! The installation zip contains multiple folders. The installer executable requires this folder structure. If you moved the CA Business Intelligence installer after extracting the zip, copy the entire folder structure to the same location and verify that you execute the installation media from the VM folder.

6. Verify that all the servers are running the same previous version of the Report Server.
7. On UNIX, export the previous installation, so that the new installer can detect an older version. Issue this command:

   `export CASHCOMP=`*`current-installation-location`*

   For example:

   `export CASHCOMP=/opt/CA/SharedComponents`
8. Navigate to Disk1\InstData\VM and double-click the installation executable.

   The installer detects the previous installation and gives you the option to migrate the old data.
9. Click Update as the Installation Type when prompted.
10. Accept default settings during the rest of the installation.
11. Click Install.

Note: The upgrade can take up to 45 minutes to complete.

To verify the upgrade of the Report Server

Inspect the biek.properties file in the Report Server install folder. A successful installation shows the following:

```
Version=BusinessObjects Enterprise XI Release 3.1 SP6
```

Install the Service Pack for the Report Server

If you previously installed the Report Server 3.3, you only need to install Service Pack 6. It is available for download on the CA Support site, under CA Identity Manager product downloads. The download page includes a ZIP file for Windows and TAR files for Solaris and UNIX.

Copy the JDBC JAR Files

Follow these steps:

1. Navigate to the jdbcdrivers folder where the CA Identity Manager Admin toolkit is installed. The default location is as follows:
   - Windows: C:\Program Files\CA\Identity Manager\IAM Suite\Identity Manager\tools\lib\jdbcdrivers
   - UNIX: /opt/CA/IdentityManager/IAM_Suite/Identity_Manager/tools/lib/jdbcdrivers
2. Copy ojdbc14.jar (for Oracle) or sqljdbc.jar (for SQL Server) to the following location:
   - Windows: CA\SC\CommonReporting3\common\4.0\java\lib
   - UNIX: /opt/CA/SharedComponents/CommonReporting3/bobje/java/lib

   Note: Copy sqljdbc.jar from Tools\lib\jdbcdrivers\1.2 to use the 1.2 driver that is compatible with the Report Server.
3. Open the CRConfig.xml file, found in the following location:
   - Windows: CA\SC\CommonReporting3\common\4.0\java
   - UNIX: /opt/CA/SharedComponents/CommonReporting3/bobje/java
4. Add the location of the JDBC JAR files to the Classpath. For example:
   - Windows: <Classpath>report_server_home\common\4.0\java\lib\sqljdbc.jar; report_server_home\ common\4.0\java\lib\ojdbc14.jar …</Classpath>
   - UNIX: <Classpath>${BOBJEDIR}/java/lib/sqljdbc.jar:${BOBJEDIR}/java/lib/ojdbc14.jar: …</Classpath>
5. Save the file.
6. Restart the Report Server as follows:
   - For Windows, do the following:
     a. Go to Start, Program Files, BusinessObjects XI *version*, BusinessObjects Enterprise, Central Configuration Manager.

        The Central Configuration Manager opens.

     b. Select all services and click Restart.
   - For UNIX, do the following:

     ```
     cd /opt/CA/SharedComponents/CommonReporting3/bobje
     ./stopservers
     ./startservers
     ```

Deploy Default Reports

CA Identity Manager comes with default reports you can use for reporting. BIConfig is a utility that uses a specific XML format to install these default reports for CA Identity Manager.

If you are upgrading from a previous version of the Report Server, first remove the CA Identity Manager Reports folder using the Central Management Console. The existing reports do not work. You can then deploy default reports for the new Report Server.

Important! This process updates all default reports. If you customized any default reports, be sure to back them up before performing the update.

Follow these steps:

1. Gather the following information about the Report Server:
   - Hostname
   - Administrator name
   - Administrator password
   - Snapshot database type
2. Copy all content from the Reports installer-root-directory/disk1/cabi/biconfig folder to the *im_admin_tools_dir*/ReportServerTools folder.
3. Set the JAVA_HOME variable to the 32-bit version of the JDK1.5 you installed.
4. Run one of the following commands:
   - For a Microsoft SQL Snapshot Database:

     ```
     biconfig -h "hostname" -u "administrator_name" -p "administrator_password"
     -f "ms-sql-biar.xml"
     ```

   - For an Oracle Snapshot Database:

     ```
     biconfig -h "hostname" -u "administrator_name" -p "administrator_password"
     -f "oracle-biar.xml"
     ```

   Note: In a UNIX operating environment, be sure that biconfig.sh has execute permissions.
5. View the biconfig.log file found in the location where you ran the command in Step 4.
6. Verify that the default reports installed successfully. Inspect the end of the log file for status; a successful install appears as follows:

   ```
   ReportingDeployUtility - Reporting utility program terminated and return code =
   0
   ```

BusinessObjects XI 3.x Post-Installation Step

If you run report tasks and receive a "Server Input% not found or server may be down" error message, perform this procedure.

Follow these steps:

1. Log in to the Central Management Console using the username and password you entered during the Report Server installation.
2. Under the main dashboard, select Servers.
3. Under the Server Name column, search for Input File Repository server and double-click the name.
4. In the Server Name text box, enter the following:

   Input.*report_server_hostname*.InputFileRepository
5. Click Save.
6. Under the Server Name column, search for Output File Repository server and double-click the name.
7. In the Server Name text box, enter the following:

   Output.*report_server_hostname*.OutputFileRepository
8. Click Save.
9. Restart *all* the servers by selecting the servers in the Server List.

Chapter 7: Post-Upgrade Configuration

This section contains the following topics:

Recompile Custom Code

When you upgrade the Provisioning Server, all connectors are upgraded by default. However, custom connectors and code will need to be recompiled using Microsoft Visual Studio 2008 SP1.

Note: For more information on upgrading specific connectors on endpoints or migrating deprecated connectors to their replacement connectors, see the *Connectors Guide*.

The following custom code must be recompiled:

- Pluggable Authentication Module (PAM)

  If you are currently using PAM, you must recompile PAM using Microsoft Visual Studio 2008 SP1.

  Note: For more information on PAM, see the *Provisioning Reference Guide*.

- Program Exits

  If you are currently using Program Exits, you must recompile them using Microsoft Visual Studio 2008 SP1.

  Note: For more information on Program Exits, see the *Provisioning Reference Guide*.

- Custom Java Connectors

  CA IAM CS is compatible with the CA Identity Manager r12 JCS SDK connector code.

  Note: For more information on upgrading or migrating custom Java connectors, see the *Connector Programming Guide*.

- Custom C++ Connectors

  If you are currently using the C++ Connector Server with custom connectors, you must recompile the custom connectors using Microsoft Visual Studio 2008 SP1.

  Note: For more information on custom C++ connectors, see the *Programming Guide for Provisioning*. This guide is part of the Provisioning SDK, a separate download available on the CA Support site.

To recompile custom connector code

1. Install Microsoft Visual Studio 2008 SP1.
2. Install the Provisioning SDK. The Provisioning SDK is included in a separate download available on the CA Support Site.

   The installer detects the previous SDK version and updates it. Any files or folders, such as custom code placed in the Provisioning SDK admin folder, are preserved.
3. If the original custom code makefiles did not use eta.dep, update the makefiles as follows:
   a. Replace the exception handling flag from /GX to /EHsc.
   b. Remove /YX from the compiler command line option.
   c. Add the following to the compile flag:
      ```
      /D "_CRT_SECURE_NO_WARNINGS" /D "_CRT_NON_CONFORMING_SWPRINTFS" /D "_USE_32BIT_TIME_T"
      ```
   d. Set the correct versions in the makefile, as follows:
      - APPVER = 6.0
      - _WIN32_IE = 0x0700
   e. Add the following to the compile flag:
      ```
      /D "_BIND_TO_CURRENT_VCLIBS_VERSION"
      ```
      This tells the compiler to use VS.2008 SP1 libraries and dlls.
   f. Merge the built EXE and DLL files with the manifest file.
   g. Update the connector source and remove references to obsolete MFC functions.
4. Build the new connector for this release of CA Identity Manager. Refer to Microsoft's web site if there are compilation errors.
5. Deploy the connector.

Update Relational Database User Stores

The sample directory.xml files for Relational Database user stores require an update so that group members appear.

Follow these steps:

1. In the Management Console, click Directories.
2. Click the name of the RDB directory to export.

   The Properties for the CA Identity Manager directory window appear.
3. At the bottom of the properties window, click Export.
4. When prompted, save the XML file.
5. Edit the XML file.
6. Remove the following section:

```
<Table name="tblUsers" primary="true" />
<Table name="tblUserAddress">
   <Reference childcol="userid" primarycol="id"/>
</Table>
<Table name="tblUserRoles">
   <Reference childcol="userid" primarycol="id"/>
</Table>
<Table name="tblUserDelegators">
   <Reference childcol="userid" primarycol="id"/>
</Table>
<Table name="tblUserPasswordhints">
   <Reference childcol="userid" primarycol="id"/>
</Table>
<Table name="tblUserIdentityPolicy">
   <Reference childcol="userid" primarycol="id"/>
</Table>
<Table name="tblOrganizations">
   <Reference childcol="id" primarycol="org"/>
</Table>
```

7. Insert the following section where you removed the preceding section.

```
<Table name="tblUsers" primary="true" />
<Table name="tblUserAddress">
   <Reference childcol="userid" primarycol="id"/>
</Table>
<Table name="tblUserRoles">
   <Reference childcol="userid" primarycol="id"/>
</Table>
<Table name="tblUserDelegators">
   <Reference childcol="userid" primarycol="id"/>
</Table>
<Table name="tblUserPasswordhints">
```

```
   <Reference childcol="userid" primarycol="id"/>
</Table>
<Table name="tblUserIdentityPolicy">
   <Reference childcol="userid" primarycol="id"/>
</Table>
<Table name="tblOrganizations">
   <Reference childcol="id" primarycol="org"/>
</Table>
<Table name="tblGroupMembers">
   <Reference childcol="userid" primarycol="id"/>
</Table>
<Table name="tblGroupAdmins">
   <Reference childcol="userid" primarycol="id"/>
</Table>
```

8. Adapt this code to your specific table and column names to match your user store schema.
9. Save the XML file.
10. In the Management Console, import the updated XML file.

Environment Changes

A number of changes with this release affect CA Identity Manager environments. To be sure all new or changed features function correctly, use the following procedures on each CA Identity Manager environment.

Convert an Environment to the new UI7 Format

You can convert an environment to conform to the CA User Interface version 7 standard:

Follow these steps:

1. Select an environment in the Management Console.
2. Click Advanced Settings, Miscellaneous.
3. Add a parameter called DefaultConsole.
4. Set the DefaultConsole to ui7.
5. Save and restart the environment.

Upgrade r12 or r12.5 Environments with Access Roles

If you upgraded from a pre-C9 version of CA Identity Manager r12 or a pre-SP4 version of CA Identity Manager r12.5, perform these steps for each environment with access roles:

To upgrade environments with access roles

1. Select an environment with access roles in the Management Console.
2. Export the Role Definitions from this environment.
3. Verify that the exported XML file contains all the Access Roles and Access Tasks.
4. In the User Console, login as a user with privileges to manage all access roles and tasks.
5. Delete all Access Roles and Access Tasks from the environment.
6. In the Management Console, select the environment.
7. Choose Advanced Settings, Miscellaneous.
   a. Add EnableSMRBAC to the Property Field.
   b. In the value field, enter: true.
   c. Click Add.
8. Import the Role Definitions that you exported in Step 2.

   This import creates all Access Roles and Access Tasks and associates them with SiteMinder objects. In the SiteMinder user interface, you can use these objects to assign Access Roles to policies and Access Tasks with Responses.
9. Repeat these steps for each environment with access roles.

Update Role Definitions

Each upgrade of CA Identity Manager requires an update of role definitions. This update is required so that the environment has the current version of roles and tasks and the product works as documented. Use the following procedure to import the role definition files one at a time for your situation.

Follow these steps:

1. In the Management Console, click Environments.
2. Select the environment.
3. Go to Role and Task Settings.

4. Click Import.
5. Select any file and click Finish to import that file.

   For example, select Access Requests and click Finish to include tasks where you can manage services.
6. Scroll up to see role definition files under the heading, Category: Upgrade to 12.6SP.
7. Select the role definition files that apply to the release where you are starting.

   Note: You choose one file to upgrade role definitions and click Finish; then, you choose the next file to import.

   For each file you choose, select the right version. The columns show if the file applies if you have a provisioning server and if the user store has an organization. For example, for an r12.0 CA Identity Manager environment that uses a provisioning server, and the CA Identity Manager user store has a flat hierarchy (no organization), select the following files:

   - Upgrade-12-to-12.5-RoleDefinitions-ProvisioningNoOrganization.xml
   - Upgrade-12.5-to-12.6-RoleDefinitions-ProvisioningNoOrganization.xml
   - Upgrade-12.6-to-12.6SP-RoleDefinitions-ProvisioningNoOrganization.xml

     The 12.6SP files upgrade the environment to the current SP release of 12.6.

After you import the role definition files, you can view and execute new tasks by assigning them to the appropriate admin role.

Add Support for Roles Modified in Provisioning Manager

If you modify roles in Provisioning Manager, the changes appear in the User Console after you import a new role definition file.

Follow these steps:

1. If you did *not* update the role definitions using the previous section, perform the following steps. Otherwise, skip to step 2.
   a. In the Management Console, click Environments.
   b. Select the environment.
   c. Go to Role and Task Settings.

d. Click Import.

e. Scroll to see role definition files under the heading, Category: Provisioning Roles.

f. Select Provisioning Roles Inbound Notification Support.

2. If you *did* update the role definitions, perform the following steps.

   a. Log in to the User Console.

   b. Use Modify Admin Role on the Provisioning Synchronization Manager role.

      Add the Provisioning Modify Provisioning Role task to this role.

   c. Use Modify Admin Role on the System Manager role.

      Add the Provisioning Modify Provisioning Role task to this role.

When you next modify a role in Provisioning Manager, the changes for that role appear in the User Console.

Update System Manager Role

Starting at CA Identity Manager r12.5 SP7, the System Manager role requires a change to work with Identity Policies. Update the System Manager role so that the member policy includes provisioning roles in its scope.

Update Roles that Manage Provisioning Roles

Starting at CA Identity Manager r12.5 SP7, a new requirement exists for admin roles that provide access to provisioning role management tasks. A provisioning role scope rule is required in each member policy rule. Without these scope rules, no roles are found in a search for provisioning role tasks. This requirement is a change in the enforcement behavior of provisioning role scope from previous releases.

If you are upgrading from r12.5 SP6 or earlier, use Modify Admin Role to add scope rules to the admin roles that manage these tasks.

Update Existing Account Screens

Some account screens have been updated to include new account functionality. If you have any of the following endpoints in your environment, import the updated role definitions file for the endpoint to update the account screen in CA Identity Manager:

- ActiveDirectory
- JNDI
- Access Control

- CA-ACF2
- CA-Top Secret
- DB2 Server
- KRB Namespace
- Lotus Domino Server
- Oracle Server
- PeopleSoft
- RSA SecurID 7
- Siebel
- UNIX-etc
- Windows NT
- All dynamic (DYN) connectors

  Note: All dynamic connector account screens need to be recreated after the upgrade. For more information about generating new account screens for these connectors, see the *Connector Xpress Guide*.

To update existing account screens

1. In the Management Console, click Environments.
2. Select the environment.
3. Go to Role and Task Settings.
4. Click Import.

   Multiple role definitions files are listed for import.
5. Select the role definitions file for the account screens you want to update.
6. Click Finish.

Add New Account Screens

Each upgrade of CA Identity Manager may include support for new types of endpoints. To manage accounts on those endpoints, you add the new account management screens to the environment.

Follow these steps:

1. In the Management Console, click Environments.
2. Select the environment.
3. Click Role and Task Settings.

4. Click Import.
5. Scroll up to see the heading Category: EndpointType.

   Multiple role definitions files are listed for import.
6. Select the role definitions file for the account screens you want to add.
7. Click Finish.

Add New Report Screens

At 12.6.3, CA Identity Manager added new screens to the Create Snapshot Definition task. The new screens are the tabs for Snapshot Policies, Role Settings, User Attributes, and Endpoint Account Attributes. To update that task, you import a role definition file into the environment.

Follow these steps:

1. In the Management Console, click Environments.
2. Select the environment.
3. Go to Role and Task Settings.
4. Click Import.
5. Select snapshot-screen-definitions.xml.
6. Click Finish to import that file and restart the environment.

After you import the role definition file, you can use updated task.

Enable Preventative Identity Policies

A preventative identity policy is a type of identity policy that prevents users from receiving privileges that may result in a conflict of interest or fraud. These policies support a company's Segregation of Duties (SOD) requirements. To enable preventative identity policies, import the Upgrade-to-12.6-EnvironmentSettings.xml file.

This file is located under *admin_tools*\Updates\Environment-Settings.

To enable preventative identity policies

1. In the Management Console, click Environments.
2. Select the environment and click Advanced Settings.
3. Click Import.

4. Browse for the Upgrade-to-12.6-EnvironmentSettings.xml file under *admin_tools*\Updates\Environment-Settings.
5. Click Finish.

Add Delegation

If you enable delegation in a CA Identity Manager Environment, do the following:

- Add the %DELEGATORS% well-known attribute to the directory.xml file.
- If you are using an RDB user store, run the following script to update your user store database with the delegation table:
  - SQL: mssql-userdelegators-add-on.sql
  - Oracle: oracle-userdelegators-add-on.sql

  These scripts can be found in the following locations:
  admin_tools\samples\NeteAutoRdb\Organization
  admin_tools\samples\NeteAutoRdb\NoOrganization

Migrate Tasks to New Recurrence Model

A new, global recurrence model is available for the Execute Explore And Correlate task and the Capture Snapshot Data task.

To switch to the global recurrence model

1. Migrate existing recurring tasks, as follows:
   a. Select the task, either Modify Explore And Correlate Definition or Modify Snapshot Definition.
   b. Search for any definitions with recurrence schedules.
   c. Select the conversion check box and click Submit.

      This converts all recurrence schedules that exist for all definitions of the selected type. Any changes to the recurrence schedule must be made before the conversion.
2. Add new recurrence tabs, as follows:
   a. In the User Console, go to Roles And Tasks, Admin Tasks, Modify Admin Task.
   b. Select the Execute Explore And Correlate task or the Capture Snapshot Data task.
   c. Select the Tabs tab.
   d. Select Task Recurrence from the drop-down list.

e. Click the up arrow next to the Task Recurrence tab to move it to the top of the list.

f. Change the tab controller to the Wizard Tab Controller.

g. Click Submit.

3. Remove existing recurrence tabs, as follows:

a. In the User Console, go to Roles And Tasks, Admin Tasks, Modify Admin Task.

b. Select the Create Explore And Correlate Definition task, the Modify Explore And Correlate Definition task, the Create Snapshot Definition task, or the Modify Snapshot Definition task.

c. Select the Tabs tab.

d. Click the delete (-) image to the right of the Recurrence tab to remove it.

e. Click Submit.

Update Auditing Settings

Starting at CA Identity Manager r12.5 SP7, a new architecture exist to support multiple EARs. In each environment, changes are needed for auditing to work.

To update audit settings for an environment

1. Access the Management Console
2. Click Environments, *Environment*, Advanced Setting, Auditing.
3. Export existing settings and save the file.
4. Locate this line in the exported settings file:

   <Audit enabled="true" auditlevel="BOTH" datasource="auditDbDataSource">

5. Change this line to the following:

   <Audit enabled="true" auditlevel="BOTH"
   datasource="iam/im/jdbc/auditDbDataSource">

6. Import the updated audit settings into the same environment.
7. Repeat this procedure for each environment.

Upgrade Workflow from CA Identity Manager r12

If approvals are required for the individual add/remove actions within the AccumulatedProvisioningRolesEvent, additional configuration is required for updating roles, tasks, and workflow process definitions.

Note: This additional configuration is required only if deployments need to approve individual actions within the AccumulatedProvisioningRolesEvent, and the CA Identity Manager environment was created in a release before CA Identity Manager r12 CR1.

To approve or reject individual actions within the AccummulatedProvisioningRolesEvent, an approver uses a specific approval screen that lets that user Approve or Reject option button for each action. If at least one action is approved, the event moves into the approved state and gets executed. If all actions are rejected, the event moves into the rejected state and then to the canceled state.

Note: To view the status of each action, use the View Submitted Tasks task to view the details of the AccumulatedProvisioningRolesEvent.

This procedure includes references to admin_tools, which represents the folder for the CA Identity Manager Administrative Tools.

The Administrative Tools are placed in the following default locations:

- **Windows:** C:\Program Files\CA\Identity Manager\IAM Suite\Identity Manager\tools
- **UNIX:** /opt/CA/IdentityManager/IAM_Suite/Identity_Manager/tools

To enable workflow for the AccumulatedProvisioningRolesEvent

1. In the Management Console, select an environment.
2. Click Role and Task Settings.
3. Import the appropriate Upgrade-12-to-12.6-RoleDefinitions.xml file (either the Organization or NoOrganization version).

   Note: For new environments created with CA Identity Manager r12.0 CR1 or later, the AccumulatedProvisioningRolesUpdate.xml import is not necessary as the approval task is available with new environments.
4. Restart the application server.
5. Verify that the Approve Accumulated Provisioning Roles task exists by using View Admin Task.
6. Run the Archive.bat program, which is located in the admin_tools\Workpoint\bin folder.

7. Import the AccumulatedProvisioningRolesApproveProcess.zip, which is located in the admin_tools\Workpoint\bin folder.
8. Open Designer.bat to verify that this process definition now exists.

   Workflow now supports the AccumulatedProvisioningRolesEvent.

Chapter 8: Task Persistence

Update URI Mapping Files

As of r12.5 SP7, the URIs have changed, so you should update the URI mapping files, so that they redirect web requests to the new targets. See the following table:

Component	New URL	Old URL
User Console	http://*hostname:port*/iam/im/*alias*	http://*hostname:port*/idm/*alias*
Management Console	http://*hostname:port*/iam/immanage	http://*hostname:port*/idmmanage

Reapply r12 Workpoint Customizations

If you upgraded from CA Identity Manager r12, the following WorkPoint files were renamed to *filename*.bak and a new version of the file was installed. Reapply any modifications you made to these files:

- From the Workpoint/bin directory: Archive.bat/.sh, Designer.bat/.sh, init.bat/.sh
- From the Workpoint/conf directory: workpoint-client.properties

Add Sample Workflow Processes

To support the Escalation Process template, use the WorkPoint archive tool to import the sample workflow processes as follows:

1. In WorkPoint Designer, click Import.

   WorkPoint Designer location: *admin_tools*\Workpoint\bin

2. Navigate to *admin_tools*\workflowScripts and select 12.5to12.5SPUpgradeWFScripts.zip.

   This script imports the Escalation Process template.

3. Repeat Steps 3 through 5 for all work items.
4. Click Finish.

Note: Be sure that you have configured the WorkPoint Administrative Tools before running the WorkPoint Designer. For more information about configuring the WorkPoint Administrative Tools, see the *Configuration Guide*.

Update r12 DYN Endpoint Attributes

If you have a DYN namespace created in CA Identity Manager r12, perform the following steps to enable account management from the User Console. To do so, you remap DYN endpoint attributes to the account screen, as follows:

1. After the upgrade, open the old DYN JDBC project in Connector Xpress.
2. Map the attributes to the account screen.
3. Redeploy the metadata.
4. Run the Role Definitions Generator.
5. Copy the respective file to the application server.
6. Restart CA Identity Manager.

Note: For more information about mapping endpoint attributes using Connector Xpress, see the *Connector Xpress Guide*.

Update Oracle Database with Garbage Collection Procedure

To add the Auditing Garbage Collection stored procedure to pre-SP5 Oracle audit databases, execute the ims_oracle_audit_upgradeto_r125_SP5.sql script against your Oracle Auditing database.

Upgrade SiteMinder

If you are using SiteMinder in your environment, you can upgrade SiteMinder components either before or after you upgrade to CA Identity Manager 12.6.4.

In CA Identity Manager r12, the Servlet Filter Agent was deprecated. If you are using SiteMinder to protect CA Identity Manager, and you do not have a Web Agent installed, configure a Web Agent for CA Identity Manager 12.6.4.

Be sure to upgrade your Extensions for SiteMinder. To upgrade these extensions, run the CA Identity Manager installer on the SiteMinder Policy Server and select Extensions for SiteMinder.

Note: For more information, see the SiteMinder chapter in the *Installation Guide*.

Appendix A: Upgrade Verification

This section contains the following topics:

How to Verify the Upgrade

Verify the following CA Identity Manager components to be sure your upgrade completed successfully:

- CA Directory and Provisioning Directory
- Provisioning Server & Connector Server
- CA Identity Manager Application
- Runtime Database Schema upgrades for the following:
  - Workflow
  - Task Persistence
  - Archive
  - Auditing
  - Snapshot
- Object Store
- Pending Tasks
- Adapters
- SiteMinder Integration
- Report Server

CA Directory and Provisioning Directory

Perform the following steps to verify the upgrade of CA Directory and the Provisioning Directory.

1. Check the cadir_msi.log, located in the CA Directory installation folder, for any errors.
2. Check the imps_directory_install.log for errors, located under the *Provisioning Directory*_uninst for the user who installed the product.
3. Run the "dxserver status" command. It should return the following:

   system_name-impd-co started
   system_name-impd-inc started
   system_name-impd-main started
   system_name-impd-notify started

   If one or all of the above services are not started, run the "dxserver start all" command.

   If one or all of the above dsa services will not start, check the corresponding log file under dxserver/logs. To start a dsa service in debug mode, run the following command for the dsa that will not start: "dxserver –d start *system_name*-impd-main"
4. Verify that Ingres is not running, and that it has been uninstalled from the system.

Provisioning Server and Connector Server

Perform the following steps to verify the upgrade of Provisioning Server and Connector Server.

1. Check the imps_server_install.log and the im_connector_server_install.log for errors, located in the *Provisioning_Server*_uninst or *Connector_Server*_uninst directory.
2. Verify that both the CA Identity Manager Provisioning Service and Connector Service have started from the services window.

   If they fail to start, check the corresponding logs located in Provisioning Server Install Location/logs folder.
3. If all of the services have started, log into the Provisioning Manager, pointing to the Provisioning Server installed. Acquire and Explore/Correlate a few different endpoints to make sure the Connector Server is working properly.

CA Identity Manager Application

When the CA Identity Manager Application Server initially starts after the upgrade, you should see the following output in the application server logs:

```
18:41:20,132 WARN  [default] ##############################################
18:41:20,132 WARN  [default] # CA IdentityMinder 12.6.x
18:41:20,132 WARN  [default] ##############################################
18:41:20,132 WARN  [default] ---- CA IAM FW Startup Sequence Initiated. ----
18:41:20,132 WARN  [default] * Startup Step 1 : Attempting to start ServiceLocator.
18:41:20,632 WARN  [default] * Startup Step 2 : Attempting to start
PolicyServerService
18:41:20,835 WARN  [default] * Startup Step 3 : Attempting to start
ServerCommandService
18:41:21,148 WARN  [default] * Startup Step 4 : Attempting to start
EnvironmentService
18:41:21,163 WARN  [default] * Startup Step 5 : Attempting to start
CacheManagerService
18:41:21,179 WARN  [default] * Startup Step 6 : Attempting to load global plugins.
18:41:30,694 WARN  [default] * Startup Step 7 : Attempting to start
AdaptersConfigService
18:41:30,710 WARN  [default] * Startup Step 8 : Attempting to start
EmailProviderService
18:41:30,741 WARN  [default] * Startup Step 9 : Attempting to start
AuditProviderService
18:41:30,788 WARN  [default] * Startup Step 10 : Attempting to start
RuntimeStatusDetailService
.
.
18:41:31,038 WARN  [default] * Startup Step 23 : Attempting to start
GlobalInitializer plug-ins
18:41:31,038 WARN  [default] * Startup Step 24 : Attempting to start environments
18:42:15,960 WARN  [EnvironmentService] * Starting environment: XXXX
18:42:18,116 WARN  [default] * Startup Step 25 : Attempting to start SchedulerService
18:42:18,163 WARN  [default] * Startup Step 26 : Attempting to recover events and
runtime status details
18:42:18,257 WARN  [default] ---- CA IAM FW Startup Sequence Complete. ----
```

Runtime Database Schema Upgrades

The following runtime database schema will be updated after the upgrade:

- Workflow
- Task Persistence
- Archive

- Audit
- Snapshot

When the CA Identity Manager Application Server initially starts after the upgrade, you should see the following output in the application server logs:

```
17:08:22,796 WARN  [default] ##############################################
17:08:22,796 WARN  [default] # CA IdentityMinder 12.6.x
17:08:22,796 WARN  [default] ##############################################
17:08:22,953 WARN  [CreateDatabaseSchema] ****** Schema for: Task Persistence is up
to date.
17:08:23,015 WARN  [CreateDatabaseSchema] ****** Begin to create Archive database
schema.
17:08:23,218 WARN  [CreateDatabaseSchema] Archive database schema is created
successfully.
17:08:23,234 WARN  [CreateDatabaseSchema] ****** Begin to create Auditing database
schema.
17:08:23,593 WARN  [CreateDatabaseSchema] Auditing database schema is created
successfully.
17:08:23,625 WARN  [CreateDatabaseSchema] ****** Upgrading Schema for: Snapshot from
r12 to r12.5 SP2
17:08:23,891 WARN  [CreateDatabaseSchema] Snapshot database schema is created
successfully.
```

Pending Tasks

Verify that the previous version's pending tasks were migrated to CA Identity Manager 12.6.4, by doing the following:

1. Log into the User Console for the Environment that was migrated.
2. Under the System tab, run View Submitted Tasks and view all tasks whose task status is equal to 'In Progress'.
3. Additionally, approvers for any pending tasks should log into the Environment and validate that they can see their work items.

Adapters

If any deployment-specific customization includes java-based Logical Attribute Handlers, Business Logic Task Handlers, Participant Resolvers, or Event Listeners, verify that these adapter classes are loaded properly by verifying the following Startup steps have completed with no errors:

```
18:41:30,898 WARN  [default] * Startup Step 12 : Attempting to start
LogicalAttributeService
18:41:30,898 WARN  [default] * Startup Step 13 : Attempting to start BLTHService
18:41:30,898 WARN  [default] * Startup Step 14 : Attempting to start
ParticipantResolverService
18:41:30,898 WARN  [default] * Startup Step 16 : Attempting to start
EventAdapterService
```

SiteMinder Integration

Verify the following to validate that the SiteMinder integration is operational after an upgrade:

- Communication with the SiteMinder Policy Server

  Verify that Startup Step 2, as shown below, has completed with no errors:

  ```
  18:41:20,632 WARN  [default] * Startup Step 2 : Attempting to start
  PolicyServerService
  ```

- SiteMinder Authentication

  Attempt to login to the User Console, using a valid login ID and password. A successful login indicates that CA Identity Manager is communicating with SiteMinder for authentication.

- Password Management

  1. Run the View Password Policies task, select an existing password policy, and verify that its content are the same as prior to the upgrade.

     If the password policies that existed prior to the upgrade are not present, see the Object Store upgrade verification steps above.

  2. Attempt to modify a user's password and be sure the password composition rules from the applicable password policy are in effect.

  3. Reset a user's password using the Reset Password Task, choosing the 'Password Must Change' option.

  4. Attempt to login with that user and verify that the login attempt is redirected to the Change Password task.

  5. Change the password and verify that the user login is successful.

Report Server

Perform the following steps to verify the upgrade of the Report Server.

1. Check the CA_Business_Intelligence_InstallLog.log and the ca-install.log for errors, located in the temp directory for the user who installed the product.
2. On Windows, check the services have started as follows:
   a. Click Start, Programs, Business Objects, start the Central Configuration Manager.
   b. Click the Manage Servers icon, a box with a checkmark in the top row of icons.
   c. Be sure that all of the services are started, with the exception of the WinHTTP Web Proxy.

      If they are not started, start them.

      If any of the services fail to start, check the corresponding logs located in the Business Objects Install location/logging folder.
3. On Solaris, check the services have started as follows:
   a. Enter this command: ps-ef | grep bobje
   b. Verify all services are started.

      See the *Business Objects Enterprise Administrator's Guide* for a list of services.
4. If all services have started, log into the Admin Launchpad, by going to the following URL:

   `http://report-server-name:port/CmcApp/logon.faces`
5. Launch the Central Management console.

Appendix B: UNIX, Linux, and Non-Provisioning Installations

For UNIX and LINUX systems and scenarios where no provisioning software is needed, some additional instructions apply.

This section contains the following topics:

UNIX and Console Mode Installation

The examples in this guide provide the Solaris executable name for the installation program. However, you may be installing on AIX or Linux.

- For AIX, use: ca-im-*release*-aix.bin
- For LINUX, use: ca-*release*-linux.bin

release represents the current release of CA Identity Manager

If you are performing an installation in console mode, such as on a UNIX workstation, you add another option to the command line.

- For the main installation, add -i console. For example:
  `./ca-im-release-sol.bin -i console`
- For installation of provisioning components, add -console to the setup command.

Red Hat Linux 64-bit Installation

If you plan to install CA Identity Manager on a Red Hat Linux 64-bit system, you need to prepare the system for the installation.

Follow these steps:

Install four 32-bit packages using the following commands:

```
yum install glibc.i686
yum install libXext.i686
yum install libXtst.i686
yum install ncurses-devel.i686
```

Note: The i686 suffix specifies that the library is 32-bit, for the x86 processor.

Alternatively, the dependencies may be resolved using Add/Remove Software, and unchecking the Only Native Packages filter option. Using this approach, you select and install the required i686 architecture dependencies.

The native ksh shell package also needs to be installed. Use the following command:

```
yum install ksh
```

Another alternative is to resolve the package dependency by using Add/Remove Software. Using this approach, you select and install the required i686 architecture dependencies ksh package.

Non-Provisioning Installation

This guide refers to the Windows and Solaris program names for the installers that provide options to install provisioning software. If you prefer to see no provisioning options, you can use these installers:

- For Windows, use IMWithoutProvisioning\ca-im-web-*release*-win.bat
- For Solaris, use IMWithoutProvisioning/ca-im-web-*release*-sol.sh

release represents the current release of CA Identity Manager.

Appendix C: Unattended Upgrades

This section contains the following topics:

How to Perform Unattended Upgrades

To enable an unattended CA Identity Manager upgrade, upgrade the CA Identity Manager Server and the Provisioning Components separately.

To perform an unattended installation of the CA Identity Manager Server, modify the settings in the im-installer.properties configuration file and run the installer against this file.

For Provisioning Components, you can generate a response file with each of the component installers, which can then be edited to perform unattended installations.

CA Identity Manager Server Unattended Upgrade

To upgrade the CA Identity Manager Server in unattended mode, run the CA Identity Manager installer against the im-installer.properties file with one of the following commands:

- **Windows:**
  `ca-im-release-win32.exe -f im-installer.properties -i silent`
- **UNIX:**
  `./ca-im-release-sol.bin -f im-installer.properties -i silent`

release represents the current SP release of CA Identity Manager.

Note: For more information on the im-installer.properties configuration file, see the *Installation Guide*.

Use the im_installer.properties file included for reference in the *Installation Guide* to perform an unattended upgrade. Be sure to edit the file with the information required for an upgrade.

Provisioning Components Unattended Upgrade

Locate the installer for the Provisioning Component you want to upgrade on the installation media. The following parameters are supported by the Provisioning Component installers:

-options-template *response_file_name*

Generates a template response file. This file lists the options available for the user to customize the install. It also contains the text that would be displayed during console install as comments in the response file.

-options-record *response_file_name*

Records the information entered into the user interface during an installation, and saves the information to a response file. This file can be used to perform an unattended installation. This is similar to –options-template except that the details of the response file are filled in and a full install is performed.

Once the response file is configured, use the following commands to invoke the Provisioning Component installers in unattended mode:

Provisioning Directory

```
setup.exe -silent -options response_file_name
```

Provisioning Server

```
setup.exe -silent -options response_file_name
```

Provisioning Manager

```
setup.exe -silent -options response_file_name
```

Appendix D: Manual Upgrades

This section contains the following topics:

How to Manually Upgrade to CA Identity Manager 12.6.4

If you want to upgrade to CA Identity Manager 12.6.4 manually, invoke each installer separately for each component. Each installer can be found on the CA Identity Manager media. To upgrade manually, perform the following process in the order listed.

Important! Be sure to disable all antivirus software before installation.
If antivirus software is enabled while installation takes place, problems can occur.
Remember to re-enable your antivirus protection after you complete the installation.

To upgrade manually to CA Identity Manager 12.6.4

1. Verify upgrade prerequisites.
2. Collection information for the upgrade.
3. Back up custom code.
4. Upgrade the Provisioning Directory (includes the CA Directory upgrade).
5. Upgrade the Provisioning Server (includes the C++ connector server).
6. Upgrade the Java Connector Server.
7. Upgrade the Provisioning Manager.
8. Upgrade the CA Identity Manager Server.
9. Upgrade other provisioning components.
10. Recompile custom code.
11. Upgrade the Report Server.

Manually Upgrade the Provisioning Directory

CA Directory no longer uses Ingres as a data store. Starting at CA Directory r12 SP1, a new memory-mapped file technology named DXgrid is used. For Provisioning to work with CA Identity Manager 12.6.4, upgrade the Provisioning Directory schema and CA Directory.

Note: If you want to install your Provisioning Directory on a new system, migrate the Provisioning Directory instead of performing an upgrade. See the Provisioning Components Upgrade chapter.

Important! Upgrading the Provisioning Directory must be done by running the upgrade.bat (or upgrade.sh) file located in the CADirectory/dxserver directory. Do not perform the upgrade by running the Provisioning Directory setup.exe file. The upgrade.bat script will examine your system and then upgrade CA Directory after performing any prerequisite cleanup, then the script will upgrade the Provisioning Directory.

To manually upgrade the Provisioning Directory

1. If you have primary and alternate Provisioning Directories, back up your primary Provisioning Directory.
2. Shut down all Provisioning Directories in your environment.
3. Stop Ingres with the following command:
   `ingstop –service(or ingstop -kill)`
4. Verify that all of the following Ingres processes are stopped:
   - dmfacp.exe
   - dmfrcp.exe
   - iidbms.exe
   - iigcc.exe
   - iigcn.exe
   - iijdbc.exe
   - iistar.exe
5. Restart Ingres with the following command:
   `ingstart –service`
6. Verify that the Provisioning and Connector services are stopped.
7. (Windows only) Be sure the Local Service account has read/write permissions to the folder where CA Directory will be installed.
8. Navigate to the CADirectory/dxserver folder on the CA Identity Manager installer media.

9. Run the upgrade.bat file.

   The Provisioning Directory upgrade wizard starts.

   Note the following:

   - Part of the Provisioning Directory upgrade is the upgrade of CA Directory to the latest bundled r12.0 Service Pack. Due to architectural changes in CA Directory r12 SP1 (and higher), reporting databases and unnecessary DSAs are removed before the CA Directory upgrade. Once the CA Directory upgrade completes, the Provisioning Directory upgrade will resume
   - If you are installing the Provisioning Directory in an FIPS 140-2 enabled environment, select the FIPS 140-2 Compliance mode check box during installation and provide the FIPS Key File.

10. Go through the wizard and enter the information you collected for the upgrade. Select a Typical installation type when prompted during the CA Directory upgrade.

    The Provisioning Directory and CA Directory are upgraded.

Note: You can select a check box during upgrade to configure Provisioning Directory high availability. If you choose this option, you must supply the hostnames of any alternate Provisioning Directories and specify the primary Provisioning Directory. When the upgrade completes, uninstall and reinstall any alternate Provisioning Directories. For more information, see the *Installation Guide*.

For details on using CA Directory, you can find CA Directory documentation at support.ca.com.

Manually Upgrade the Provisioning Server

Important! The Provisioning Server uses an instance of CA Directory to communicate with the Provisioning Directory. Be sure to upgrade CA Directory on the Provisioning Server system, using the CA Directory component installer, *before* upgrading the Provisioning Server.

To manually upgrade the Provisioning Server

1. (Windows only) Be sure the Local Service account has read/write permissions to the folder where CA Directory will be installed.
2. Navigate to the Provisioning/ProvisioningServer folder on the CA Identity Manager installer media.
3. Run the setup file.
4. Go through the wizard and enter the information you collected for the upgrade.

   Your Provisioning Server is upgraded.

Manually Upgrade CA IAM CS

Perform the following process to manually upgrade the CA IAM CS.

To manually upgrade CA IAM CS

1. Navigate to the Provisioning/ConnectorServer folder on the CA Identity Manager installer media.
2. Run the setup file.
3. Go through the wizard and enter the information you collected for the upgrade.

   Your CA IAM CS is upgraded.

Manually Upgrade the Provisioning Manager

Perform the following process to manually upgrade the Provisioning Manager.

To manually upgrade the Provisioning Manager

1. Navigate to the Provisioning/ProvisioningManager folder on the CA Identity Manager installer media.
2. Run the setup file.
3. Go through the wizard and enter the information you collected for the upgrade.

   Your Provisioning Manager is upgraded.

Manually Upgrade the CA Identity Manager Server

To upgrade the CA Identity Manager Server manually, run the Upgrade Wizard, upgrade the CA Identity Manager Server, and *uncheck* the automated upgrade steps. Instead, perform the following processes manually:

1. Upgrade the Workflow database.
2. Migrate task persistence data.

Upgrade the Workflow Database

This procedure applies only if you are upgrading from CA Identity Manager r12.

To work with WorkPoint 3.4.2, you update the workflow database, so you can continue to use the workflow processes that you developed in WorkPoint 3.3.

Follow these steps:

1. Locate the WorkPoint scripts in the Workpoint\database under the Administrative Tools folder. The scripts are in the following default locations:
   - **Windows:** C:\Program Files\CA\Identity Manager\IAM Suite\Identity Manager\tools\Workpoint\database
   - **UNIX:** /opt/CA/IdentityManager/IAM_Suite/Identity_Manager/tools/Workpoint/database
2. Run the following scripts:

   wp331_to_wp34_cnv_step1.sql

   This script creates the tables for Workpoint 3.4, adds columns the old tables, and inserts rows into the WP_*_TYPE tables.

   wp331_to_wp34_cnv_step2.sql

   This script creates the stored procedures that are required to convert the data.

   wp331_to_wp34_cnv_step3.sql

   This script converts the text data to columns and populates the new WP_BULK_DATA table from the old WP_BULK_STORAGE table.

   wp34_20060927_add.sql

   This script creates the tables for Workpoint 3.4.20060927 and inserts rows into the WP_INI and WP_*_TYPE tables.

   wp34_20070625_add.sql

   This script creates the tables for Workpoint 3.4.2.20070625 and inserts rows into the WP_INI and WP_*_TYPE tables.

   wp342_20071218_add.sql

   This script creates the tables for Workpoint 3.4.2.20071218 and inserts rows into the WP_INI and WP_*_TYPE tables.

   wp342b_to_wp342c.sql

   This script adds tables and rows to support the completion code.

   wp342c_to_wp342d.sql

   This script updates field lengths and scripts.

wp342d_to_wp342e.sql

This script adds index definitions.

3. Save all changes to the database.

Migrate Task Persistence Data

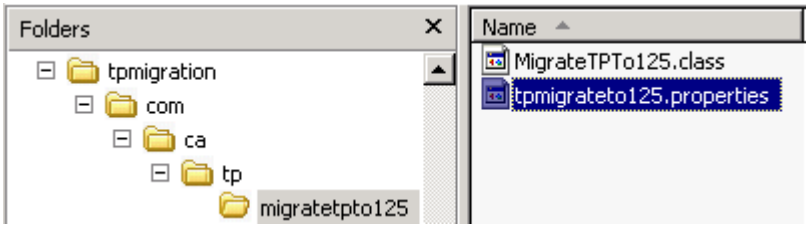
This procedure applies only if you are upgrading from CA Identity Manager r12.

You can manually migrate tasks, depending on task state or date range, by running the task persistence data migration tool.

Follow these steps:

1. Find the tpmigration125.properties file in the following location:

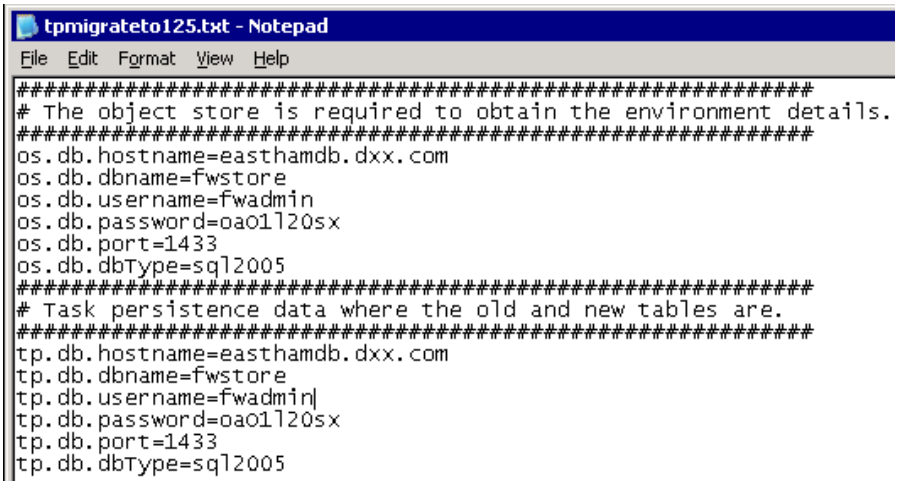
   admin_tools/tpmigration/com/ca/tp/migratetpto125



2. Update this file with the object store and task persistence information for your database.

   Note: For any supported version of SQL Server, enter sql2005.

Equation 3: The user views sections to change in the tipmigrateto125.properties file.



3. Be sure that the environment variable JAVA_HOME is set.
4. From a command line, navigate to *admin_tools*/tpmigration and run the task persistence migration tool as follows:
   - For Windows:
     `runmigration.bat`
   - For UNIX:
     `runmigration.sh`
5. Enter the following information:
   a. For the environment protected Alias, enter all.

      Note: If you do not specify all, only one environment can be entered.

   b. For task state, enter All (with a Capital A).
      Note: If you do not specify All, only one task state can be entered.

   c. For the version to migrate from, enter 2 for 12.0.

   d. Date range for the tasks to be migrated (y/n).

      Note: If you choose 'y', enter a Start Date (mm/dd/yy) and End Date (mm/dd/yy).

   The migration starts. After the migration completes, the status indicates how many tasks were migrated.
6. Be sure to verify that no errors appeared.
7. Repeat steps 4 and 5, but use the -pending option instead of All for task state.

Appendix E: Log Files for the Upgrade

This section contains the following topics:

Log Files on Windows

If you encounter issues during CA Identity Manager installation, see this log file:

C:\Program Files\CA\Identity Manager\IAM Suite\Identity Manager\caiamsuite.log

The CA Identity Manager Server installer logs are written to the following default location:

C:\Program Files (x86)\CA\Identity Manager\install_config_info (64-bit system)

The Provisioning installer logs are written to the user's Temp directory and copied to the *Install-Directory*_uninst directory.

Example:

C:\Documents and Settings*user*\Local Settings\Temp\imps_server_install.log

Log files on UNIX

If you encounter any issues while performing a CA Identity Manager installation, see the caiamsuite.log file in this location:

/opt/CA/IdentityManager/

The CA Identity Manager Server installer logs are written to the following default location:

/opt/CA/IdentityManager/install_config_info

The Provisioning installer logs are written to the user's Temp directory.

Index

N

P

R

S

T

U

V