

CA Identity Manager

Upgrade Guide (JBoss)

r12.5 SP7



This documentation, which includes embedded help systems and electronically distributed materials, (hereinafter referred to as the "Documentation") is for your informational purposes only and is subject to change or withdrawal by CA at any time.

This Documentation may not be copied, transferred, reproduced, disclosed, modified or duplicated, in whole or in part, without the prior written consent of CA. This Documentation is confidential and proprietary information of CA and may not be disclosed by you or used for any purpose other than as may be permitted in (i) a separate agreement between you and CA governing your use of the CA software to which the Documentation relates; or (ii) a separate confidentiality agreement between you and CA.

Notwithstanding the foregoing, if you are a licensed user of the software product(s) addressed in the Documentation, you may print or otherwise make available a reasonable number of copies of the Documentation for internal use by you and your employees in connection with that software, provided that all CA copyright notices and legends are affixed to each reproduced copy.

The right to print or otherwise make available copies of the Documentation is limited to the period during which the applicable license for such software remains in full force and effect. Should the license terminate for any reason, it is your responsibility to certify in writing to CA that all copies and partial copies of the Documentation have been returned to CA or destroyed.

TO THE EXTENT PERMITTED BY APPLICABLE LAW, CA PROVIDES THIS DOCUMENTATION "AS IS" WITHOUT WARRANTY OF ANY KIND, INCLUDING WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NONINFRINGEMENT. IN NO EVENT WILL CA BE LIABLE TO YOU OR ANY THIRD PARTY FOR ANY LOSS OR DAMAGE, DIRECT OR INDIRECT, FROM THE USE OF THIS DOCUMENTATION, INCLUDING WITHOUT LIMITATION, LOST PROFITS, LOST INVESTMENT, BUSINESS INTERRUPTION, GOODWILL, OR LOST DATA, EVEN IF CA IS EXPRESSLY ADVISED IN ADVANCE OF THE POSSIBILITY OF SUCH LOSS OR DAMAGE.

The use of any software product referenced in the Documentation is governed by the applicable license agreement and such license agreement is not modified in any way by the terms of this notice.

The manufacturer of this Documentation is CA.

Provided with "Restricted Rights." Use, duplication or disclosure by the United States Government is subject to the restrictions set forth in FAR Sections 12.212, 52.227-14, and 52.227-19(c)(1) - (2) and DFARS Section 252.227-7014(b)(3), as applicable, or their successors.

Copyright © 2011 CA. All rights reserved. All trademarks, trade names, service marks, and logos referenced herein belong to their respective companies.

CA Technologies Product References

This document references the following CA products:

- CA Identity Manager
- CA SiteMinder®
- CA Directory
- CA Enterprise Log Manager
- CA Role & Compliance Manager

Contact CA Technologies

Contact CA Support

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

- 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

Provide Feedback

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

If you would like 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 9

Supported Upgrade Paths	9
How to Upgrade CA Identity Manager	9
CA Identity Manager r12.5 SP7 Server on JBoss	10
How to Upgrade CA Identity Manager	10

Chapter 2: Upgrade Prerequisites 11

How to Meet Prerequisites for the Upgrade	11
Check Hardware Requirements	12
Check Software Requirements	14
Back Up Custom Code	14
Apply CA Directory License Patch	15
Upgrade CA Directory on r12.5 or higher Systems	16
Close Option Pack Workflow Items	16
Install JCE Libraries for SiteMinder	17
Synchronize Provisioning Role Names	17
Install JBoss	17
Configure SSL	17
Complete the Upgrade Worksheets	18
Provisioning Directory Information	18
Provisioning Server Information	19
Java Connector Server Information	19
JBoss Information	20
Database Connection Information	21
Login Information	21
SiteMinder Information	22

Chapter 3: Provisioning Components Upgrade 23

Architecture Changes	23
Upgrade the Provisioning Directory	24
Migrate the Provisioning Directory	29
Upgrade the Provisioning Server	30
Upgrade the Java Connector Server	33
Upgrade the Provisioning Manager	33
Configure a Remote Provisioning Manager	33
Upgrade Other Provisioning Components	34

Chapter 4: Upgrade on a Single JBoss Node	35
How to Migrate a Single Node Installation to JBoss 5	35
Uninstall the Identity Manager Server	35
Reinstall the Identity Manager Server on a JBoss Node	36
Upgrade the Workflow Database	39
Migrate Task Persistence Data	40
Verify the Upgraded Node	41
Chapter 5: Upgrade on a JBoss Cluster	43
Example: Identity Manager Server on a JBoss Cluster	43
How to Migrate CA Identity Manager on a JBoss Cluster	44
Uninstall the Identity Manager Server	44
Test the Default Multicast Address	45
Create the Master Node	46
Add Cluster Nodes	49
Configure the JK Connector	50
Upgrade the Workflow Database	52
Migrate Task Persistence Data	53
Start the JBoss Cluster	54
Verify the Clustered Installation	55
Chapter 6: Report Server Upgrade	57
Upgrade the Report Server	57
Copy the JDBC JAR Files	58
Deploy Default Reports	59
Chapter 7: Post-Upgrade Configuration	61
Recompile Custom Code	61
Environment Changes	63
Upgrade r12 or r12.5 Environments with Access Roles	63
Add New Roles and Tasks	64
Update System Manager Role	64
Update Roles that Manage Provisioning Roles	64
Update Existing Account Screens	65
Add New Account Screens	66
Enable Preventative Identity Policies	66
Add Delegation	67
Migrate Tasks to New Recurrence Model	67
Update Auditing Settings	68

Upgrade Workflow from CA Identity Manager r12	68
Update URI Mapping Files	70
Reapply r12 Workpoint Customizations	70
Add Sample Workflow Processes	70
Update r12 DYN Endpoint Attributes	71
Update Oracle Database with Garbage Collection Procedure	71
Upgrade SiteMinder	71

Appendix A: Upgrade Verification **73**

How to Verify the Upgrade	73
CA Directory and Provisioning Directory	74
Provisioning Server and Connector Server	74
Identity Manager Application	75
Runtime Database Schema Upgrades	75
Pending Tasks	76
Adapters	77
SiteMinder Integration	77
Report Server	78

Appendix B: UNIX, Linux, and Non-Provisioning Installations **79**

UNIX and Console Mode Installation	79
Red Hat Linux 64-bit Installation	79
Non-Provisioning Installation	80

Appendix C: Unattended Upgrades **81**

How to Perform Unattended Upgrades	81
Identity Manager Server Unattended Upgrade	81
Provisioning Components Unattended Upgrade	82

Appendix D: Manual Upgrades **83**

How to Manually Upgrade to CA Identity Manager r12.5 SP7	83
Manually Upgrade the Provisioning Directory	84
Manually Upgrade the Provisioning Server	85
Manually Upgrade the Java Connector Server	86
Manually Upgrade the Provisioning Manager	86
Manually Upgrade the Identity Manager Server	86
Upgrade the Workflow Database	87
Migrate Task Persistence Data	88

Appendix E: Log Files for the Upgrade	91
Log Files on Windows	91
Log files on UNIX	91
Index	93

Chapter 1: Upgrade Overview

This section contains the following topics:

[Supported Upgrade Paths](#) (see page 9)

[How to Upgrade CA Identity Manager](#) (see page 9)

[CA Identity Manager r12.5 SP7 Server on JBoss](#) (see page 10)

[How to Upgrade CA Identity Manager](#) (see page 10)

Supported Upgrade Paths

The following is a list of products and versions that have a supported path for an upgrade to CA Identity Manager r12.5 SP7:

- CA Identity Manager r12
- CA Identity Manager r12 with Option Pack 1

Note: If you plan to migrate CA Identity Manager r12 with Option Pack 1 to a new version of the application server, contact Customer Support for assistance. For upgrades on the same version of the application server, use the upgrade procedure in this guide.

- CA Identity Manager r12.5
- CA Identity Manager r12.5 SPx

If you do not currently use one of these versions of CA Identity Manager, upgrade to one of these versions, then upgrade to CA Identity Manager r12.5 SP7.

Note: Upgrades from ACE to r12.5 SP7 are *not* supported. Also, cross-platform upgrades (between UNIX and Windows) are not supported.

How to Upgrade CA Identity Manager

Perform the following steps to upgrade CA Identity Manager:

Step
1. Be sure your systems meet all upgrade prerequisites.
2. Upgrade provisioning components.
3. Upgrade the Identity Manager Server on the node or cluster.

Step

4. Upgrade the Report Server.

5. Perform post-upgrade configuration.

CA Identity Manager r12.5 SP7 Server on JBoss

CA Identity Manager r12.5 SP7 Server is supported on 64-bit versions of JBoss 5.1 (open source) and 5.0 (Enterprise Edition).

Note: These versions are supported at the time this document is published. Be sure to verify the latest supported versions in the CA Identity Manager support matrix on the [CA Support Site](#).

Previous versions of the CA Identity Manager Server ran on 32-bit versions of JBoss. To use the Identity Manager Server r12.5 SP7, you install it on the new JBoss version, then migrate data from the previous installation to the new installation.

How to Upgrade CA Identity Manager

Perform the following steps to upgrade CA Identity Manager:

Step

1. Be sure your systems meet all upgrade prerequisites.

2. Upgrade provisioning components.

3. Upgrade the 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](#) (see page 11)
- [Check Hardware Requirements](#) (see page 12)
- [Check Software Requirements](#) (see page 14)
- [Back Up Custom Code](#) (see page 14)
- [Apply CA Directory License Patch](#) (see page 15)
- [Upgrade CA Directory on r12.5 or higher Systems](#) (see page 16)
- [Close Option Pack Workflow Items](#) (see page 16)
- [Install JCE Libraries for SiteMinder](#) (see page 17)
- [Synchronize Provisioning Role Names](#) (see page 17)
- [Install JBoss](#) (see page 17)
- [Configure SSL](#) (see page 17)
- [Complete the Upgrade Worksheets](#) (see page 18)

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. Apply the CA Directory license patch.
5. Upgrade CA Directory.
6. Install JCE if using SiteMinder.
7. Synchronize names for provisioning roles
8. Upgrade the application server if needed.
9. Configure SSL if needed.
10. 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

Identity Manager Server

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

Component	Minimum	Recommended
CPU	Intel (or compatible) 1.5 GHz (Windows or Red Hat Linux), SPARC 1.0 GHz (Solaris) or POWER4 1.1 GHz (AIX)	Dual core Intel (or compatible) 2.5 GHz (Windows or Red Hat Linux), Dual core SPARC 1.5 GHz (Solaris) POWER5 1.5 GHz (AIX)
Memory	2 GB	4 GB
Available Disk Space	2 GB	2 GB
Temp Space	2 GB	2 GB
Swap/Paging Space	2 GB	2 GB

Provisioning Server or a Standalone Connector Server

Component	Minimum	Recommended
CPU	Intel (or compatible) 1.5 GHz (Windows) SPARC 1.0 GHz (Solaris)	Dual core Intel (or compatible) 2.5 GHz (Windows) SPARC 1.5 GHz (Solaris)
Memory	2 GB	4 GB
Available Disk Space	2 GB	2 GB

Provisioning Directory

Component	Minimum	Recommended
CPU	Intel (or compatible) 1.5 GHz (Windows) SPARC 1.0 GHz (Solaris)	Dual core Intel (or compatible) 2.5 GHz (Windows) SPARC 1.5 GHz (Solaris)

Component	Minimum	Recommended
Memory	2 GB	4 GB
Available Disk Space	2 to 10 GB, depending on the number of endpoint accounts <ul style="list-style-type: none"> ■ Compact—Up to 10,000 accounts, 0.25 GB per datafile (total 1 GB) ■ Basic—Up to 400,000 accounts, 0.5 GB per datafile, (total 2 GB) ■ Intermediate (64 bit only)—Up to 600,000 accounts, 1 GB per datafile, total 4 GB ■ Large (64 bit only)—Over 600,000 accounts, 2 GB per datafile, total 8 GB 	2 to 10 GB, depending on the number of endpoint accounts <ul style="list-style-type: none"> ■ Compact—Up to 10,000 accounts, 0.25 GB per datafile (total 1 GB) ■ Basic—Up to 400,000 accounts, 0.5 GB per datafile, (total 2 GB) ■ Intermediate (64 bit only)—Up to 600,000 accounts, 1 GB per datafile, total 4 GB ■ Large (64 bit only)—Over 600,000 accounts, 2 GB per datafile, total 8 GB
Processor	32-bit processor and operating system for small deployments 64-bit processor and operating system 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) 2.0 GHz (Windows) SPARC 1.5 GHz (Solaris)
Memory	4 GB
Available Disk Space	6 to 14 GB depending on the number of accounts
Processor	64-bit processor and operating system for intermediate and large deployments
Swap/Paging Space	2 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
- Universal Provisioning Option (UPO) program exits
- Pluggable Authentication Module (PAM) DLLs
- 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.

Apply CA Directory License Patch

To upgrade CA Directory on a Windows system, you must apply a license patch for CA Directory before beginning the upgrade procedure.

If you do not apply the patch, the upgrade procedure may remove license files which are required by other CA products.

You can [download](#) the patch on the CA Support site.

To locate the patch

1. Log into the support.ca.com.
The CA Support site opens.
2. CA Licensing.
3. Click License Package 1.8 is Now Available.
A page opens that describes the changes to the License Package, and includes a link for downloading it.
4. Follow the instruction to download and install the Windows patch.

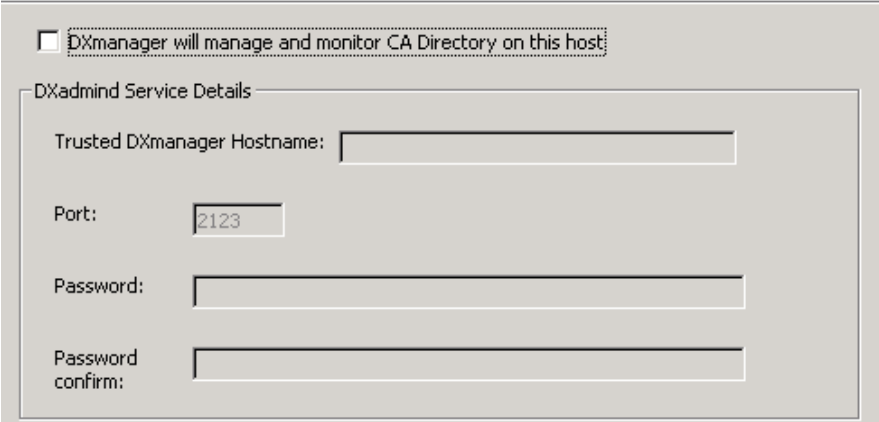
Note: You also need this patch if you plan to manually uninstall eTrust Directory r8.

Upgrade CA Directory on r12.5 or higher Systems

If you are upgrading a CA Identity Manager r12.5 SP5 or higher system, you 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.

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.

Close Option Pack Workflow Items

If you are upgrading from CA Identity Manager r12 with Option Pack 1 installed, complete all currently running workflow items generated by the Option Pack before the upgrade.

You can identify Option Pack workflow items by looking for 'UserAddAttributeValue' in the workflow description.

Install JCE Libraries for SiteMinder

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

Before you upgrade the 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.

Synchronize Provisioning Role Names

If you renamed any provisioning roles in Provisioning Manager since the last time you started the application server, restart the application server. This action updates the Identity Manager server to the correct provisioning role names, so you are ready for the upgrade.

Install JBoss

CA Identity Manager r12.5 SP7 works with JBoss 5.0 and 5.1. Therefore, you need to install a new version of JBoss if your version is before 5.0. Also, install the JDK identified in the support matrix as supporting JBoss 5.

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:

- The Identity Manager Server is a J2EE application that is deployed on a supported application server. 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/farm*.

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 Identity Manager Server. You can download the JDK from Sun's web site at the following URL:

<http://java.sun.com>

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.

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 (64 bit only)—up to 600,000 accounts
- Large (64 bit only)—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.	

Java Connector Server Information

Record the following provisioning information you need during the Java Connector Server upgrade:

Field Name	Description	Your Response
Password	The password for the Provisioning Server administrative user.	

Field Name	Description	Your Response
Component Password	The password for the Java Connector Server that the Provisioning Server uses for authentication.	

JBoss Information

Record the following JBoss information 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: <ul style="list-style-type: none">■ For a single node installation, the system that will host the Identity Manager Server (system that will host 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 <i>not</i> 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 you need during the Provisioning Components installation.

Field Name	Description	Your Response
Username	A username that you create to log into the provisioning components.	
Provisioning Server password	A password for this Server.	

Field Name	Description	Your Response
C++ Connector Server password	A password needed for this server. Each C++ Connector Server can have a unique password.	
Provisioning Directory password	A password used by Provisioning Server to connect to Provisioning Directory. For an alternate Provisioning Server, enter the Provisioning Directory password 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 will use to connect to SiteMinder.	
SiteMinder Shared Secret	The shared secret for the above Agent.	

Chapter 3: Provisioning Components Upgrade

This section contains the following topics:

[Architecture Changes](#) (see page 23)

[Upgrade the Provisioning Directory](#) (see page 24)

[Migrate the Provisioning Directory](#) (see page 29)

[Upgrade the Provisioning Server](#) (see page 30)

[Upgrade the Java Connector Server](#) (see page 33)

[Upgrade the Provisioning Manager](#) (see page 33)

[Configure a Remote Provisioning Manager](#) (see page 33)

[Upgrade Other Provisioning Components](#) (see page 34)

Architecture Changes

For r12.5 and higher releases, 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 CA Identity Manager, 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

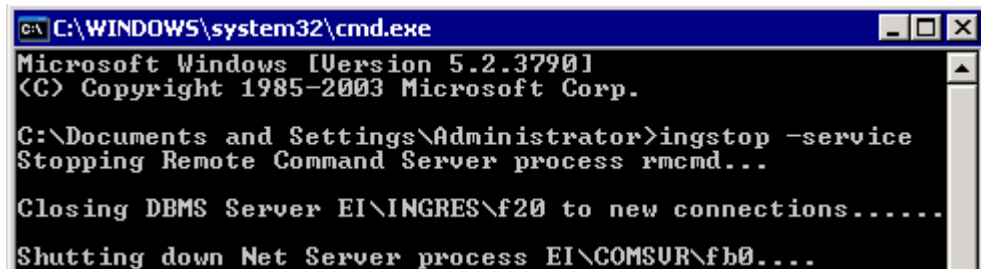
1. If you have primary and alternate Provisioning Directories, back up your primary Provisioning Directory.
2. Shut down all Provisioning Directories in your environment.
3. If you are upgrading from a release prior to CA Identity Manager r12.5, complete the following steps

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`



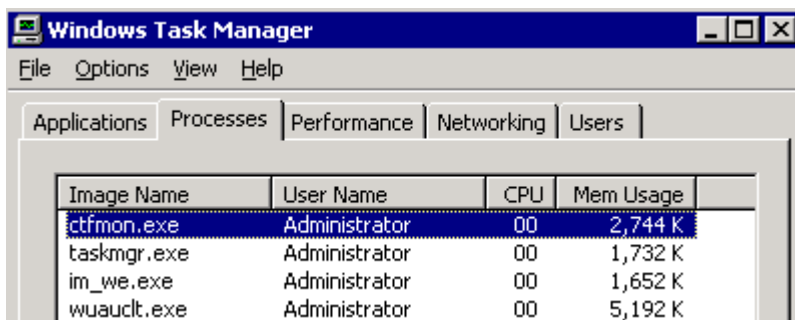
```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.

C:\Documents and Settings\Administrator>ingstop -service
Stopping Remote Command Server process rmcnd...

Closing DBMS Server EI\INGRES\f20 to new connections.....

Shutting down Net Server process EI\COMSUR\fb0....
```

- 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 and Provisioning Server and Server services.

Name	Description	Status
Background Intelligent Transfer Service	Transfers f...	Started
CA Identity Manager - Connector Server (C++)		
CA Identity Manager - Provisioning Server		

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. Consider the following guidelines, while allowing room for future growth:

- Compact—up to 10,000 accounts
- Basic—up to 400,000 accounts
- Intermediate (64 bit only)—up to 600,000 accounts
- Large (64 bit only)—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. Intermediate and Large installations require 64-bit Directory installs (either Solaris or Windows 64 bit).

Select Deployment Size

Select the deployment size that best suits your needs.
The minimum required values indicate both the hard disk space required to create and the memory required to load the datastores.
Note: Intermediate and Large deployments require 64 bit hardware, operating system and CA Directory software.

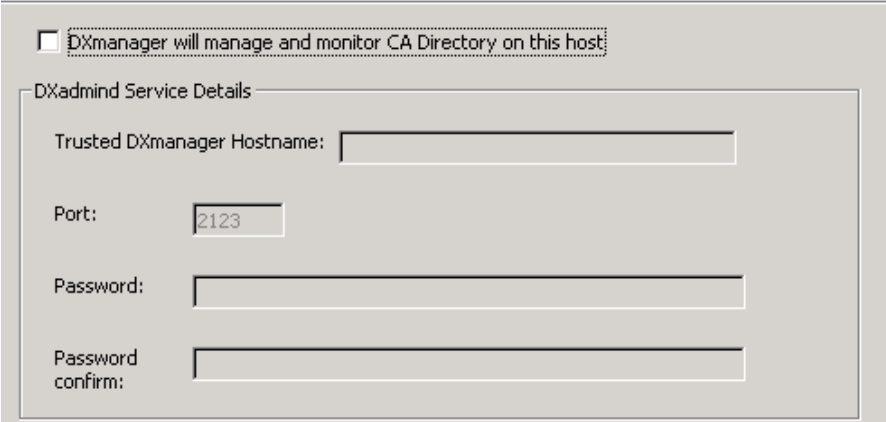
- Compact
Configures deployment to support up to approximately 10,000 accounts.
Required Space: 1GB
- Basic
Configures deployment to support up to approximately 400,000 accounts.
Required Space: 2GB
- Intermediate [64 Bit Only]
Configures deployment to support up to approximately 600,000 accounts.
Required Space: 4GB
- Large [64 Bit Only]
Configures deployment to support more than 600,000 accounts.
Required Space: 8GB

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 appears:

CA Directory Configuration Upgrade

Your CA Directory configuration has been upgraded successfully and you can now upgrade to CA Directory r12.0 SP4. **Make sure you complete the migration process, which includes an automatic system backup, and do not press cancel.** Once that has completed, installation will run again to complete the CA Identity Manager - Provisioning Directory upgrade.

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.



DXmanager will manage and monitor CA Directory on this host

DXadmind Service Details

Trusted DXmanager Hostname:

Port:

Password:

Password confirm:

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.

Provisioning Directory High Availability Configuration
If Provisioning Directory will be installed on multiple systems in a high-availability configuration, the hostnames of all additional Provisioning Directory systems must be provided.

Configure Provisioning Directory High Availability

Enter Provisioning Directory Hostname

central-reg1

Add

Provisioning Directory Hostnames

west-distr3
north-dist3

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 r12.5 SP7, you may need to migrate the Provisioning Directory to a new system to accommodate requirements for memory or a 64-bit operating system.

To migrate the Provisioning Directory to a new system

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 r12.5 SP7 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 by running the following command from a command prompt:
`dxdumpdb -0 -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`

- 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 r12.5 SP7 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.

- 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 will be set to the old hostname and must be changed.

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\dxserver.

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.

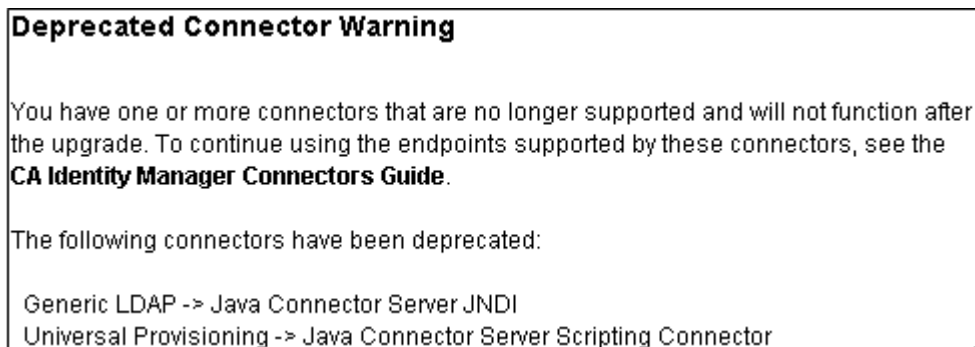
To upgrade the Provisioning Server

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.

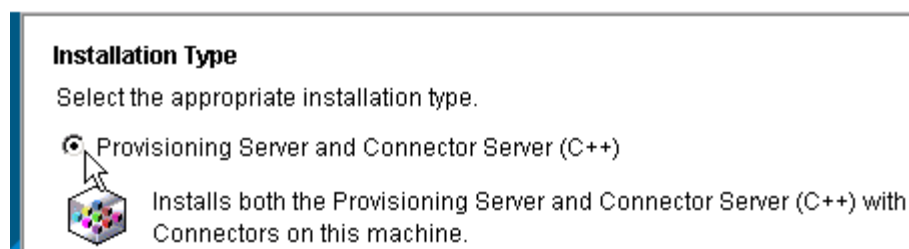


The Provisioning Server upgrade starts. Note the following:

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



4. Choose 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).



- You can select a check box during upgrade to indicate 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.
- Complete the Provisioning Domain screens.

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

Provisioning Domain Configuration

Domain is the primary administrative Provisioning Server unit.

Select a name for the domain to be managed by this Provisioning Server.
Note: Once a domain is configured its name cannot change.

Domain Name:

- Enter a password for the domain.

Username:

Password:

Confirm Password:

Description:

- Supply provisioning components passwords.

Provisioning Component Passwords

Create the required passwords. For an alternate Provisioning Server, enter the Provisioning Directory password created for the primary Provisioning Server.

	Password	Confirm Password
Provisioning Server:	<input type="password" value="*****"/>	<input type="password" value="*****"/>
C++ Connector Server:	<input type="password" value="*****"/>	<input type="password" value="*****"/>
Provisioning Directory:	<input type="password" value="*****"/>	<input type="password" value="*****"/>

- Go through the wizard and enter the information you collected for the upgrade.
Your Provisioning Server is upgraded.

Upgrade the Java Connector Server

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

When upgrading the Java Connector Server, note the following:

- Most fields are automatically populated during the Java Connector Server 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 Java Connector Server component password to what you entered in this field.

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 Identity Manager Administrative Tools on a Windows system.

To configure a remote Provisioning Manager

1. Log into 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.

SPML Manager

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

SPML Service

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

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.

GINA

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

Vista Credential Provider

Run the Vista 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.

JCS SDK

Run the JCS 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:

[How to Migrate a Single Node Installation to JBoss 5](#) (see page 35)

[Verify the Upgraded Node](#) (see page 41)

How to Migrate a Single Node Installation to JBoss 5

Perform the following steps to migrate CA Identity Manager on a node to JBoss 5:

✓	Step
1.	Uninstall the Identity Manager Server
2.	Reinstall the Identity Manager Server on the JBoss node
3.	Upgrade the workflow database
4.	Migrate task persistence data

Uninstall the Identity Manager Server

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

To uninstall the Identity Manager Server on Windows

1. Stop the SiteMinder services, if you are using SiteMinder in your environment.
2. Go to Start, Control Panel, Add/Remove Programs and select CA Identity Manager.
3. Select CA Identity Manager.
4. 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/install_config_info/im-uninstall`
2. Run the following script:
`sh uninstall.sh`
Follow the on-screen instructions.

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

Reinstall the Identity Manager Server on a JBoss Node

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

To install the new version of the Identity Manager Server on a JBoss node

1. Upgrade JBoss to v5 if it is not already installed.
2. 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`.
3. Perform a new install of the 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.

4. Select the option to install the Identity Manager Server.

Identity Manager Server

Connect to Existing SiteMinder Policy Server

Identity Manager Administrative Tools

Identity Manager Provisioning Server

Identity Manager Provisioning Directory

Extensions for SiteMinder (if SiteMinder is installed locally)

5. Supply the details for the JBoss that you collected in your [worksheet](#) (see page 18).
6. For database credentials, provide the same values that existed at the previous installation.

Database Connection Information

Enter database connection information for task persistence and archive, workflow, auditing, reporting, and object storage.

Host Name:

Port Number:

Database Name:

Username:

Password:

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

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

Login Information

To create a user for connecting to the embedded CA components, provide a user name and password.
Note: The password you specify must be at least six characters.

Username:

Password:

Confirm Password:

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

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



9. 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.

10. 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
```

Upgrade the Workflow Database

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

As of CA Identity Manager r12.5, an updated version of WorkPoint Workflow was added to the installation. Update the workflow database to work with WorkPoint 3.4.2, so you can continue to use the workflow processes that you developed in WorkPoint 3.3.

To upgrade to WorkPoint 3.4.2

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\IAM Suite\Identity Manager\tools\tools\Workpoint\database
 - **UNIX:**
/opt/CA/IdentityManager/IAM_Suite/Identity_Manager/tools/Workpoint/database

2. Run the wp331_to_wp34_cnv_step1.sql script to create the new tables for Workpoint 3.4 and to add the new columns to the end of old tables.

This script also inserts rows into the WP_*_TYPE tables as needed.

3. Run the wp331_to_wp34_cnv_step2.sql script to create the stored procedures required to convert the data.

4. Run the wp331_to_wp34_cnv_step3.sql script to convert the text data to the new columns.

This script also populates the new WP_BULK_DATA table from the old WP_BULK_STORAGE table.

5. Run the wp34_20060927_add.sql script to create the new tables for Workpoint 3.4.20060927.

This script also inserts rows into the WP_INI and WP_*_TYPE tables as needed.

6. Run the wp34_20070625_add.sql script to create the new tables for Workpoint 3.4.2.20070625. This also inserts rows into the WP_INI and WP_*_TYPE tables as needed.

7. Run the wp342_20071218_add.sql script to create the new tables for Workpoint 3.4.2.20071218.

This script also inserts rows into the WP_INI and WP_*_TYPE tables as needed.

8. Save all changes to the database.

Migrate Task Persistence Data

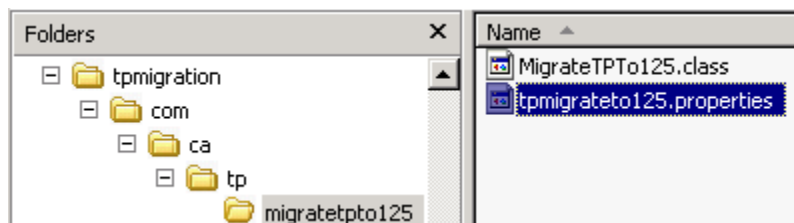
This procedure applies only if you are upgrading from CA Identity Manager r12.

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

To manually migrate task persistence data

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

`admin_tools/tpmigration/com/ca/tp/migratetp125`



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`.

```
tpmigrateto125.txt - Notepad
File Edit Format View Help
#####
# The object store is required to obtain the environment details.
#####
os.db.hostname=easthamdb.dxx.com
os.db.dbname=fwstore
os.db.username=fwadmin
os.db.password=oa01720sx
os.db.port=1433
os.db.dbType=sql2005
#####
# Task persistence data where the old and new tables are.
#####
tp.db.hostname=easthamdb.dxx.com
tp.db.dbname=fwstore
tp.db.username=fwadmin]
tp.db.password=oa01720sx
tp.db.port=1433
tp.db.dbType=sql2005
```

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 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 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:
 - 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:

[Example: Identity Manager Server on a JBoss Cluster](#) (see page 43)

[How to Migrate CA Identity Manager on a JBoss Cluster](#) (see page 44)

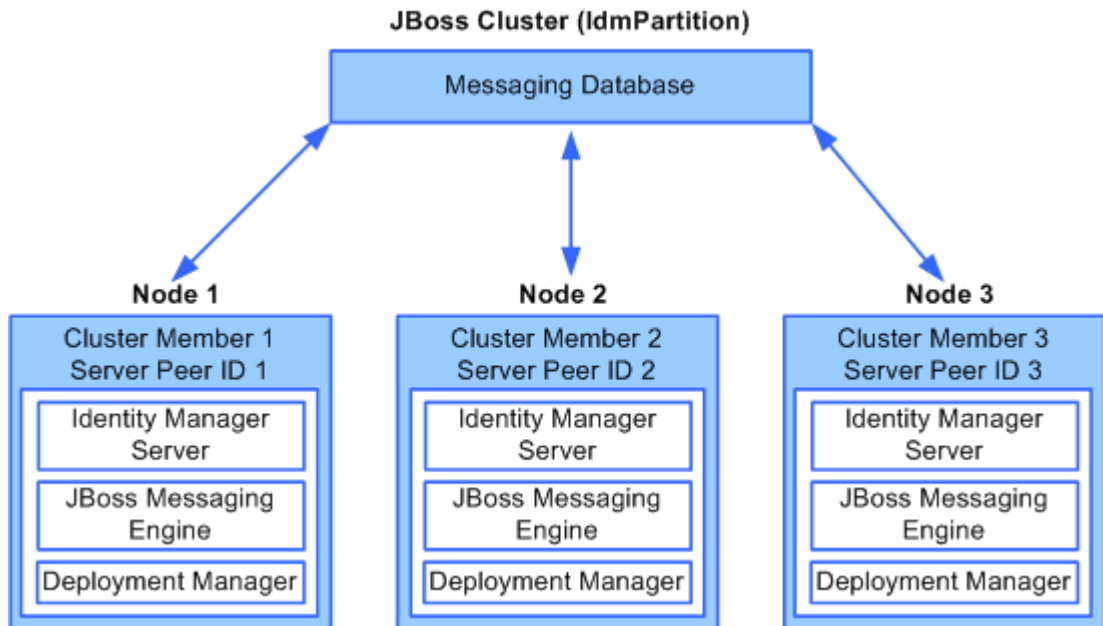
[Start the JBoss Cluster](#) (see page 54)

[Verify the Clustered Installation](#) (see page 55)

Example: Identity Manager Server on a JBoss Cluster

CA Identity Manager uses the farming method of a JBoss cluster. In this 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.

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 messaging database is a central store for cluster members to share messages and each node contains three components:

Identity Manager Server

Provides the core functionality of the product.

JBoss Messaging Engine

Provides messaging functionality for members of the cluster using JMS.


Deployment Manager

Keeps track of the cluster members and the current master node member, which is also responsible for deploying files from the master node to other nodes.

How to Migrate CA Identity Manager on a JBoss Cluster

Changing to a new version of JBoss requires a migration of the Identity Manager server, including steps for uninstalling the Identity Manager server, installing the new version of the Identity Manager server, then migrating the data.

The following procedures describe how to set up multiple JBoss application servers with the same Identity Manager application on each server. In this type of cluster, each JBoss application server acts independently of the other application servers, but they share the load through JMS messaging.

 Step
1. Uninstall the Identity Manager server.
2. Test the default mulitcast address.
3. Create the master node.
4. Add cluster nodes.
5. Configure the JK connector.
6. Upgrade the workflow database. (if upgrading from r12)
7. Migrate task persistence data. (if upgrading from r12)

Uninstall the Identity Manager Server

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

To uninstall the Identity Manager Server on Windows

1. Stop the SiteMinder services, if you are using SiteMinder in your environment.
2. Go to Start, Control Panel, Add/Remove Programs and select CA Identity Manager.
3. Select CA Identity Manager.
4. 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/install_config_info/im-uninstall
2. Run the following script:

```
sh uninstall.sh
```

Follow the on-screen instructions.

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

Test the Default Multicast Address

The run script uses a multicast address, either the default address or an alternative address supplied by your network administrator.

To test the default multicast address

1. Run sender on first node as follows:
 - a. Navigate to `jboss-home-1/server/all/lib`.
 - b. Run: `java -cp jgroups.jar org.jgroups.tests.McastSenderTest -mcast_addr 224.10.10.10 -port 5555`

2. Run receivers on other nodes in the cluster as follows:
 - a. Navigate to `jboss-home-N/server/all/lib`.
N represents the next node in the cluster.
 - b. Run: `java -cp jgroups.jar org.jgroups.tests.McastReceiverTest -mcast_addr 224.10.10.10 -port 5555`
3. 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

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

Note: On Windows, IPv6 is not supported for a JBoss cluster with the current release of the JDK. Each node must be an IPv4 system or part of an IPv4/IPv6 stack.

To create the master node

1. Install JBoss and the JDK on the computer.
2. Start the 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 collected the [information needed by the installer](#) (see page 18), such as user names, host names, and ports.

Be sure to provide the existing CA Identity Manager database credentials during the install and that all values from the previous release of CA Identity Manager are replaced with r12.5 SP7 values. If you are upgrading from CA Identity Manager r12 and you have different database stores for task persistence, workflow, audit, and reports, update the data sources to point to the separate stores.

3. Complete the Select Components section by including the Identity Manager Server and any other components that you need on this system.

4. Complete the other sections based on your requirements for the installation.
5. When you enter any password or shared secret in the installation, be sure to provide a password that you can recall when needed.

Provisioning Directory Information

The Provisioning Server stores its data in a repository called the Provisioning Directory. To configure Provisioning Directory, enter the following information.

Provisioning Directory Host:	<input type="text" value="us-west3"/>
Provisioning Directory Shared Secret:	<input type="password" value="*****"/>
Confirm Shared Secret:	<input type="password" value="*****"/>

6. 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.

JBoss Application Server Information

Enter application server information.

Note: In the Access URL and Port field, enter the fully-qualified URL including port number. In the Cluster Server Peer ID field, enter a unique Server Peer ID number between 0 and 255 for this cluster node.

JBoss Folder (no spaces):

Access URL and Port:

Cluster Installation

Cluster Server Peer ID:

7. If the multicast address test failed, perform one of the next two steps for Windows or Solaris.
8. 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`
9. 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

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.

To add a cluster node

1. Install JBoss and the JDK on the computer.
2. Install the Identity Manager server on one 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`

`spN` represents the current SP 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, perform one of the next two steps for Windows or Solaris.
7. On a Windows system, edit `run.bat` in the `jboss_home\bin` directory:
 - a. Locate the line that begins as follows:
`ARGS=%*%*`
 - b. Add a multicast address preceded by the `-u` argument as follows:
`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`

8. 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.

Configure the JK Connector

To configure the JK connector

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\IAM Suite\Identity Manager\tools\tools\samples\Cluster\JBoss\ConnectorConfiguration`
UNIX:
`/opt/CA/IdentityManager/IAM_Suite/Identity_Manager/tools/samples/Cluster/JBoss/ConnectorConfiguration`
 - b. In this file, replace `worker.workerN.*` (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.workerN.host` field with your corresponding nodes' hostnames.

For example, consider a cluster where the 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.

Upgrade the Workflow Database

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

As of CA Identity Manager r12.5, an updated version of WorkPoint Workflow was added to the installation. Update the workflow database to work with WorkPoint 3.4.2, so you can continue to use the workflow processes that you developed in WorkPoint 3.3.

To upgrade to WorkPoint 3.4.2

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\IAM Suite\Identity Manager\tools\tools\Workpoint\database
 - **UNIX:**
/opt/CA/IdentityManager/IAM_Suite/Identity_Manager/tools/Workpoint/databse

2. Run the wp331_to_wp34_cnv_step1.sql script to create the new tables for Workpoint 3.4 and to add the new columns to the end of old tables.

This script also inserts rows into the WP_*_TYPE tables as needed.

3. Run the wp331_to_wp34_cnv_step2.sql script to create the stored procedures required to convert the data.

4. Run the wp331_to_wp34_cnv_step3.sql script to convert the text data to the new columns.

This script also populates the new WP_BULK_DATA table from the old WP_BULK_STORAGE table.

5. Run the wp34_20060927_add.sql script to create the new tables for Workpoint 3.4.20060927.

This script also inserts rows into the WP_INI and WP_*_TYPE tables as needed.

6. Run the wp34_20070625_add.sql script to create the new tables for Workpoint 3.4.2.20070625. This also inserts rows into the WP_INI and WP_*_TYPE tables as needed.

7. Run the wp342_20071218_add.sql script to create the new tables for Workpoint 3.4.2.20071218.

This script also inserts rows into the WP_INI and WP_*_TYPE tables as needed.

8. Save all changes to the database.

Migrate Task Persistence Data

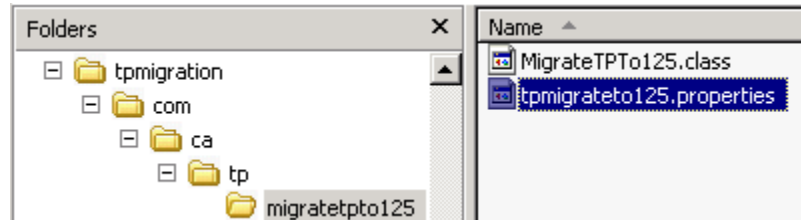
This procedure applies only if you are upgrading from CA Identity Manager r12.

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

To manually migrate task persistence data

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

`admin_tools/tpmigration/com/ca/tp/migratetp125`



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`.

```

tpmigrateto125.txt - Notepad
File Edit Format View Help
#####
# The object store is required to obtain the environment details.
#####
os.db.hostname=easthamdb.dxx.com
os.db.dbname=fwstore
os.db.username=fwadmin
os.db.password=oa01120sx
os.db.port=1433
os.db.dbType=sql2005
#####
# Task persistence data where the old and new tables are.
#####
tp.db.hostname=easthamdb.dxx.com
tp.db.dbname=fwstore
tp.db.username=fwadmin]
tp.db.password=oa01120sx
tp.db.port=1433
tp.db.dbType=sql2005

```

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 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.

To start the servers for JBoss

1. Start one of the SiteMinder Policy Servers that supports Identity Manager.
Note: If you have a Policy Server cluster, only one Policy Server should be running while you create Identity Manager directories, create or modify Identity Manager environments, or change WorkPoint settings.
2. From a command line, navigate to:
`jboss_home/bin`

3. Enter the following command to start the Identity Manager server:
 - For Windows:
run.bat -c all
 - For UNIX:
./run.sh -c all
4. Wait till you see that the server has started. This 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.

To verify the clustered installation

1. Start the databases used by the 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:
 - 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 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](#) (see page 57)

[Copy the JDBC JAR Files](#) (see page 58)

[Deploy Default Reports](#) (see page 59)

Upgrade the Report Server

Upgrade the Report Server to the supported version, CA Business Intelligence 3.2 (BusinessObjects Enterprise XI Release 3 SP3). 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.

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 SP3
```

Copy the JDBC JAR Files

To copy the JDBC JAR files

1. Navigate to the `jdbcd drivers` folder on the CA Identity Manager media, as follows:
 - Windows: `C:\Program Files\CA\IAM Suite\Identity Manager\tools\tools\lib\jdbcd drivers`
 - UNIX: `/opt/CA/IdentityManager/IAM_Suite/Identity_Manager/tools/lib/jdbcd drivers`
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`
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, CA, Report Server, 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.

To deploy the default reports

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
```

Chapter 7: Post-Upgrade Configuration

This section contains the following topics:

[Recompile Custom Code](#) (see page 61)

[Environment Changes](#) (see page 63)

[Update URI Mapping Files](#) (see page 70)

[Reapply r12 Workpoint Customizations](#) (see page 70)

[Add Sample Workflow Processes](#) (see page 70)

[Update r12 DYN Endpoint Attributes](#) (see page 71)

[Update Oracle Database with Garbage Collection Procedure](#) (see page 71)

[Upgrade SiteMinder](#) (see page 71)

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:

- PAM

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

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

- Program Exits

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

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

- Custom Java Connectors

The CA Identity Manager r12.5 SP7 Java Connector Server 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 *Programming Guide for Java Connector Server*.

- 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 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, is 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 normally.

Environment Changes

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

Add New Roles and Tasks

To add new tasks and roles to an environment after the upgrade, use the Management Console to import a new role definitions file. Different role definition files exist to upgrade your environment from different releases of CA Identity Manager and for environments that may or may not have organization support.

To add new roles and tasks

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 appropriate role definitions file to add the new roles and tasks.

For example, for provisioning capabilities, select one of the Provisioning options with or without Organization support.

6. Click Finish.
7. To view and access any new tasks, assign them to the appropriate admin role.

Note: For more information about importing roledefinitions.xml files in the Management Console, see the *Configuration Guide*.

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.

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
- OpenVMS
- 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 section titled How you Generate CA Identity Manager User Console Account Screens in 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

Support for new endpoints was added in CA Identity Manager r12.5, r12.5 SP1, and r12.5 SP3. To manage accounts on those endpoints, you add the new account management screens to the User Console.

To add new account management 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 add.
6. Click Finish.

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-12.5SP1-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-12.5SP1-EnvironmentSettings.xml file under *admin_tools\Updates\Environment-Settings*.
5. Click Finish.

Add Delegation

If you enable delegation in an 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 `AccumulatedProvisioningRolesEvent`, 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\IAM Suite\Identity Manager\tools\tools
- **UNIX:** /opt/CA/IdentityManager/IAM_Suite/Identity_Manager/tools

To enable workflow for the `AccumulatedProvisioningRolesEvent`

1. For an existing environment, import the appropriate upgrade Role Definitions file (`Upgrade-12-to-12.5SP-RoleDefinitions.xml` or `Upgrade-12-to-12.5SP-RoleDefinitions.xml`) in the Management Console, Role and Task Settings.

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.

2. Restart the application server.
3. Verify that the Approve Accumulated Provisioning Roles task exists by using View Admin Task.
4. Run the `Archive.bat` program, which is located in the *admin_tools*\Workpoint\bin folder.
5. Import the `AccumulatedProvisioningRolesApproveProcess.zip`, which is located in the *admin_tools*\Workpoint\bin folder.
6. Open `Designer.bat` to verify that this process definition now exists.

Workflow now supports the `AccumulatedProvisioningRolesEvent`.

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	<code>http://hostname:port/iam/im/aliases</code>	<code>http://hostname:port/idm/aliases</code>
Management Console	<code>http://hostname:port/iam/immanagement</code>	<code>http://hostname:port/idmmanagement</code>

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 CA Identity Manager.

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 r12.5 SP7.

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](#) (see page 73)
- [CA Directory and Provisioning Directory](#) (see page 74)
- [Provisioning Server and Connector Server](#) (see page 74)
- [Identity Manager Application](#) (see page 75)
- [Runtime Database Schema Upgrades](#) (see page 75)
- [Pending Tasks](#) (see page 76)
- [Adapters](#) (see page 77)
- [SiteMinder Integration](#) (see page 77)
- [Report Server](#) (see page 78)

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
- 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 temp directory 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 completely 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 temp directory for the user who installed the product.
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.

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 Identity Manager 12.5.x.x.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 Identity Manager 12.5.x.x.xxx
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 CA Identity Manager version's pending tasks were migrated to CA Identity Manager r12.5 SP7, by doing the following:

1. Log into the User Console for the Identity Manager 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 Identity Manager 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](#) (see page 79)

[Red Hat Linux 64-bit Installation](#) (see page 79)

[Non-Provisioning Installation](#) (see page 80)

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-12.5-spW-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 create a symbolic link to work around a CryptoJ failure. Create a link as follows:

```
ln -s /dev/urandom /dev/random
```

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-win32.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](#) (see page 81)

[Identity Manager Server Unattended Upgrade](#) (see page 81)

[Provisioning Components Unattended Upgrade](#) (see page 82)

How to Perform Unattended Upgrades

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

To perform an unattended installation of the 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.

Identity Manager Server Unattended Upgrade

To upgrade the 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-r12.5spN-win32.exe -f im-installer.properties -i silent
```

- **UNIX:**

```
./ca-im-r12.5spN-sol.bin -f im-installer.properties -i silent
```

`spN` 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 r12.5 SP7](#) (see page 83)

[Manually Upgrade the Provisioning Directory](#) (see page 84)

[Manually Upgrade the Provisioning Server](#) (see page 85)

[Manually Upgrade the Java Connector Server](#) (see page 86)

[Manually Upgrade the Provisioning Manager](#) (see page 86)

[Manually Upgrade the Identity Manager Server](#) (see page 86)

How to Manually Upgrade to CA Identity Manager r12.5 SP7

If you want to upgrade to CA Identity Manager r12.5 SP7 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 r12.5 SP7

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 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 r12.5 SP7, 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`
 - `ijdbc.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 the Provisioning 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 the Provisioning Server 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 the Java Connector Server

Perform the following process to manually upgrade the Java Connector Server.

To manually upgrade the Java Connector Server

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 Java Connector Server 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 Identity Manager Server

To upgrade the Identity Manager Server manually, run the Upgrade Wizard, upgrade the 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.

As of CA Identity Manager r12.5, an updated version of WorkPoint Workflow was added to the installation. Update the workflow database to work with WorkPoint 3.4.2, so you can continue to use the workflow processes that you developed in WorkPoint 3.3.

To upgrade to WorkPoint 3.4.2

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\IAM Suite\Identity Manager\tools\tools\Workpoint\database
- **UNIX:**
/opt/CA/IdentityManager/IAM_Suite/Identity_Manager/tools/Workpoint/databse

2. Run the wp331_to_wp34_cnv_step1.sql script to create the new tables for Workpoint 3.4 and to add the new columns to the end of old tables.

This script also inserts rows into the WP_*_TYPE tables as needed.

3. Run the wp331_to_wp34_cnv_step2.sql script to create the stored procedures required to convert the data.

4. Run the wp331_to_wp34_cnv_step3.sql script to convert the text data to the new columns.

This script also populates the new WP_BULK_DATA table from the old WP_BULK_STORAGE table.

5. Run the wp34_20060927_add.sql script to create the new tables for Workpoint 3.4.20060927.

This script also inserts rows into the WP_INI and WP_*_TYPE tables as needed.

6. Run the wp34_20070625_add.sql script to create the new tables for Workpoint 3.4.2.20070625. This also inserts rows into the WP_INI and WP_*_TYPE tables as needed.

7. Run the wp342_20071218_add.sql script to create the new tables for Workpoint 3.4.2.20071218.

This script also inserts rows into the WP_INI and WP_*_TYPE tables as needed.

8. Save all changes to the database.

Migrate Task Persistence Data

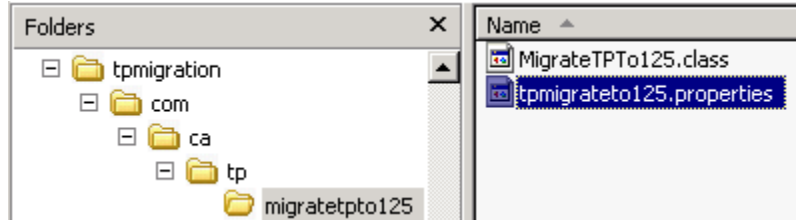
This procedure applies only if you are upgrading from CA Identity Manager r12.

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

To manually migrate task persistence data

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.

```
tpmigrateto125.txt - Notepad
File Edit Format View Help
#####
# The object store is required to obtain the environment details.
#####
os.db.hostname=easthamdb.dxx.com
os.db.dbname=fwstore
os.db.username=fwadmin
os.db.password=oa01720sx
os.db.port=1433
os.db.dbType=sql2005
#####
# Task persistence data where the old and new tables are.
#####
tp.db.hostname=easthamdb.dxx.com
tp.db.dbname=fwstore
tp.db.username=fwadmin]
tp.db.password=oa01720sx
tp.db.port=1433
tp.db.dbType=sql2005
```

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 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](#) (see page 91)

[Log files on UNIX](#) (see page 91)

Log Files on Windows

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

C:\Program Files\CA\IAM Suite\Identity Manager\tools

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

C:\Program Files\CA\Identity Manager\install_config_info

On a 64-bit windows system, the default location is:

C:\Program Files (x86)\CA\Identity Manager\install_config_info

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

A

- Adapters • 76
- Add Cluster Nodes • 49
- Add Delegation • 67
- Add New Account Screens • 66
- Add New Roles and Tasks • 64
- Add Sample Workflow Processes • 70
- Apply CA Directory License Patch • 15
- Architecture Changes • 23

B

- Back Up Custom Code • 14

C

- CA Directory and Provisioning Directory • 74
- CA Identity Manager r12.5 SP7 Server on JBoss • 10
- CA Technologies Product References • 3
- Check Hardware Requirements • 12
- Check Software Requirements • 14
- Close Option Pack Workflow Items • 16
- Complete the Upgrade Worksheets • 18
- Configure a Remote Provisioning Manager • 33
- Configure SSL • 17
- Configure the JK Connector • 50
- Contact CA Technologies • 3
- Copy the JDBC JAR Files • 58
- Create the Master Node • 46

D

- Database Connection Information • 20
- Deploy Default Reports • 59

E

- Enable Preventative Identity Policies • 66
- Environment Changes • 63
- Example
 - Identity Manager Server on a JBoss Cluster • 43

H

- How to Manually Upgrade to CA Identity Manager r12.5 SP7 • 83
- How to Meet Prerequisites for the Upgrade • 11

- How to Migrate a Single Node Installation to JBoss 5 • 35
- How to Migrate CA Identity Manager on a JBoss Cluster • 44
- How to Perform Unattended Upgrades • 81
- How to Upgrade CA Identity Manager • 9, 10
- How to Verify the Upgrade • 73

I

- Identity Manager Application • 75
- Identity Manager Server Unattended Upgrade • 81
- Install JBoss • 17
- Install JCE Libraries for SiteMinder • 17

J

- Java Connector Server Information • 19
- JBoss Information • 20

L

- Log Files for the Upgrade • 91
- Log files on UNIX • 91
- Log Files on Windows • 91
- Login Information • 21

M

- Manual Upgrades • 83
- Manually Upgrade the Identity Manager Server • 86
- Manually Upgrade the Java Connector Server • 86
- Manually Upgrade the Provisioning Directory • 84
- Manually Upgrade the Provisioning Manager • 86
- Manually Upgrade the Provisioning Server • 85
- Migrate Task Persistence Data • 40, 53, 88
- Migrate Tasks to New Recurrence Model • 67
- Migrate the Provisioning Directory • 29

N

- Non-Provisioning Installation • 80

P

- Pending Tasks • 76
- Post-Upgrade Configuration • 61
- Provisioning Components Unattended Upgrade • 82
- Provisioning Components Upgrade • 23
- Provisioning Directory Information • 18

Provisioning Server and Connector Server • 74
Provisioning Server Information • 19

R

Reapply r12 Workpoint Customizations • 70
Recompile Custom Code • 61
Red Hat Linux 64-bit Installation • 79
Reinstall the Identity Manager Server on a JBoss Node • 36
Report Server • 78
Report Server Upgrade • 57
Runtime Database Schema Upgrades • 75

S

SiteMinder Information • 21
SiteMinder Integration • 77
Start the JBoss Cluster • 54
Supported Upgrade Paths • 9
Synchronize Provisioning Role Names • 17

T

Test the Default Multicast Address • 45

U

Unattended Upgrades • 81
Uninstall the Identity Manager Server • 35, 44
UNIX and Console Mode Installation • 79
UNIX, Linux, and Non-Provisioning Installations • 79
Update Auditing Settings • 68
Update Existing Account Screens • 65
Update Oracle Database with Garbage Collection Procedure • 71
Update r12 DYN Endpoint Attributes • 71
Update Roles that Manage Provisioning Roles • 64
Update System Manager Role • 64
Update URI Mapping Files • 70
Upgrade CA Directory on r12.5 or higher Systems • 16
Upgrade on a JBoss Cluster • 43
Upgrade on a Single JBoss Node • 35
Upgrade Other Provisioning Components • 34
Upgrade Overview • 9
Upgrade Prerequisites • 11
Upgrade r12 or r12.5 Environments with Access Roles • 63
Upgrade SiteMinder • 71
Upgrade the Java Connector Server • 33
Upgrade the Provisioning Directory • 24

Upgrade the Provisioning Manager • 33
Upgrade the Provisioning Server • 30
Upgrade the Report Server • 57
Upgrade the Workflow Database • 39, 52, 87
Upgrade Verification • 73
Upgrade Workflow from CA Identity Manager r12 • 68

V

Verify the Clustered Installation • 55
Verify the Upgraded Node • 41