CA Identity Manager

Upgrade Guide

r12.5 SP5

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

This section contains the following topics:

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 SP5:

- CA Identity Manager r8.1 SP2
- CA Identity Manager r12
- CA Identity Manager r12 with Option Pack 1
- CA Identity Manager r12.5
- CA Identity Manager r12.5 SPx

If you do not currently use one of the previously listed versions of CA Identity Manager, first upgrade to one of these versions before upgrading to CA Identity Manager r12.5 SP5.

Note: Upgrades from ACE to r12.5 SP5 are *not* supported. Also, cross-platform upgrades (between UNIX and Windows) are not supported.

Upgrade Process

Perform the following steps to upgrade to CA Identity Manager r12.5 SP5.

If you currently have...	Perform these upgrade steps...
CA Identity Manager r8.1 SP2	1. Verify upgrade prerequisites. 2. Upgrade the Provisioning Server components and the Identity Manager Server. **Note:** In some cases, you need to uninstall the Identity Manager Server, upgrade your application server, then perform a *fresh* install of the Identity Manager Server. 3. Apply post-upgrade configuration changes. 4. Perform additional new feature configuration, as needed.

If you currently have...	Perform these upgrade steps...
CA Identity Manager r12 with or without Option Pack 1	1. Verify upgrade prerequisites. 2. Upgrade the Provisioning Server components and the Identity Manager Server. 3. Perform additional new feature configuration, as needed.
CA Identity Manager r12.5 or r12.5 SPx	1. Verify upgrade prerequisites. 2. Upgrade the Provisioning Server components and the Identity Manager Server. 3. Perform additional new feature configuration, as needed.

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. So 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.

Chapter 2: Upgrade Prerequisites

This section contains the following topics:

How to Meet Prerequisites for the Upgrade

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

	Step
	1. Install the CA Identity Manager Bookshelf.
	2. Check hardware and software requirements.
	3. Upgrade CA Directory.
	4. Back up custom code.
	5. (Option Pack only) Close all Option Pack workflow Items.
	6. Prepare r8.1 SP2 Environments with access roles.
	7. (WebSphere only) Configure WebSphere for the upgrade.
	8. Configure SSL, if necessary.

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.

Install the CA Identity Manager Bookshelf

For complete information about this product, install the CA Identity Manager Bookshelf, so that you can do the following:

- Use a single console to view documents published for CA Identity Manager.
- Use a single alphabetical index to find a topic in any document.
- Search all documents for one or more words.

To use the Bookshelf

1. Extract the contents of the ZIP file.
2. Choose one of the following methods:
   - Open the Bookshelf.hta file if the bookshelf is on the local system and you are using Internet Explorer.
   - Open the Bookshelf.html file if the bookshelf is on a remote system or if you are using Mozilla Firefox.

Note: The CA Identity Manager Bookshelf includes the release notes for this product. The release notes may contain additional installation and configuration information that was issued after publication of this guide.

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

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)
Memory	2 GB	4 GB
Available Disk Space	2 to 10 GB, depending on the number of endpoint accounts ■ Compact—Up to 10,000 accounts, 0.25 GB per 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 ■ 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

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:

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

Upgrade CA Directory

If you are upgrading from CA Identity Manager r12.5, you must upgrade CA Directory before upgrading CA Identity Manager. To upgrade CA Directory, navigate to the CA Directory installation folder on the CA Identity Manager media and run the dxsetup.exe file.

If you are upgrading from an earlier version of CA Identity Manager, the CA Directory upgrade is handled by the Upgrade Wizard automatically.

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

  Note: If you are upgrading from CA Identity Manager r8.1 SP2 on WebSphere, export the entire IdentityMinder.EAR to back up your customizations (see page 16).
- 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.

Back Up Customizations for WebSphere

If you are upgrading from CA Identity Manager r8.1 SP2, export your EAR to preserve any customizations that you have. Later, you use this exported EAR to copy over any customization files to the EAR for CA Identity Manager r12.5 SP5.

To back up any customizations you have on your WebSphere application server, export the IdentityMinder.EAR.

For Windows:

1. Copy the imsExport.jacl file from *was_im_tools_dir*\WebSphere-tools\ to *Websphere_home*\bin.
2. From the command line, navigate to *Websphere_home*\bin.
3. On a standalone system, be sure that the WebSphere application server is running. On a cluster, be sure that the Deployment Manager is running.
4. Run the imsExport.jacl file as follows:
   wsadmin –f imsExport.jacl *path_to_exported_ear*

   where *path to exported ear* is the full path and file name that the imsExport utility creates.

For UNIX:

1. Copy *was_im_tools_dir*\WebSphere-tools\imsExport.jacl to *Websphere_home*\bin.
2. From the command line, navigate to *Websphere_home*\bin.
3. Make sure the WebSphere application server is running.
4. Run the imsExport.jacl script, as follows:
   ./wsadmin.sh -f imsExport.jacl -conntype RMI -port 2809 *path to exported ear*

   where *path to exported ear* is the full path including the file name of the exported EAR file.

   Be sure to point to the correct RMI port when running the script.

Note: You can also export the IdentityMinder EAR using the WebSphere Administrative Console. See the WebSphere documentation for more information.

Option Pack Prerequisites

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.

Prepare r8.1 SP2 Environments with Access Roles

Before you upgrade CA Identity Manager from r8.1 SP2 , do the following for each environment with access roles:

To prepare r8.1 SP2 environments with access roles

1. Access the Identity Manager Management Console.
2. Select an environment with access roles.
3. Choose Advanced Settings, Miscellaneous.
   a. Add EnableSMRBAC to the Property Field.
   b. In the value field, enter: true.
   c. Click Add.
4. Repeat these steps for each environment with access roles.

Configure WebSphere for the Upgrade

An upgrade on WebSphere may fail due to disk space errors or timeout errors. Perform the following steps to ensure that your upgrade succeeds on WebSphere.

1. Save any changes to the WebSphere configuration via the Administrative Console (Save to Master Configuration).
2. Shut down the application server.
3. Remove the contents of the following folders:
   - Temp Directory:
     - Windows: %temp%
     - Unix: /tmp/*
   - *Websphere_home*/profiles/*WAS_PROFILE*/temp/*
   - *Websphere_home*/profiles/*WAS_PROFILE*/wstemp/*
   - *Websphere_home*/profiles/*WAS_PROFILE*/tranlog/*
   - *Websphere_home*/profiles/*WAS_PROFILE*/config/*
   - *Websphere_home*/deploytool/itp/configuration/org.*, leaving only config.ini in this directory if it exists.
4. In the *Websphere_home*/profiles/*WAS_PROFILE*/properties/soap.client.props file, set com.ibm.SOAP.requestTimeout to 1800 or higher.

Note: For more information, see your WebSphere documentation.

SSL Configuration

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.

Chapter 3: CA Identity Manager Upgrade

This section contains the following topics:

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 (see page 11).
2. Collect information (see page 19) required for the upgrade.
3. Perform the main upgrade procedures (see page 24).
4. Verify the environments (see page 46).
5. Update account screens (see page 46)
6. Upgrade the Report Server. (see page 47)
7. Upgrade SiteMinder. (see page 50)
8. Upgrade r12 or r12.5 Environments with Access Roles (see page 51)
9. Upgrade Other Provisioning Components (see page 51)
10. Recompile custom code (see page 53).

Collect Information Required for the Upgrade

Review the following sections to collect information regarding the upgrades.

Provisioning Directory Information

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

Field Name	Description	Your Response
Provisioning Directory Deployment Size	The deployment size (see page 20) that best suits your environment.	
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

When installing the Provisioning Directory, you are asked to choose a deployment size. 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 sizing guidelines with regard to your current Provisioning Directory deployment, and 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

Note: Intermediate and Large installations require 64 bit Directory installs. More details are covered under Hardware Requirements (see page 12).

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.	

Identity Manager Server Information

You must provide information for every database in your CA Identity Manager implementation, such as the databases for task persistence, workflow, audit, snapshots (reporting), and object storage. If you are upgrading an r8.1 SP2 installation, only the workflow database may exist.

Record the following database information you need during the Identity Manager Server installation:

Field Name	Description	Your Response
Database Type	The database type (vendor/version) of the database.	
Host Name	The hostname of the system where the database is located. **Note:** Ensure you provide a hostname and *not* an IP address.	
Port Number	The port number of the database.	
Service/Database Name	The database identifier.	
Username	The username for database access. **Note:** This user must have administrative rights to the database.	
Password	The password for the user account with administrative rights.	

SiteMinder Information

If you are upgrading from CA Identity Manager r8.1 SP2, your Identity Manager Directories and Environments need to be upgraded from SiteMinder into the Identity Manager object store.

Record the following migration information you need during the CA Identity Manager upgrade:

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 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 SiteMinder Agent.	
Export Location	The location where the Identity Manager Directories and Environments are exported to during migration. **Default:** C:\Documents and Settings\Administrator	

Main Upgrade Procedures

You upgrade most software components by using the Upgrade Wizard, which appears when you run the CA Identity Manager installer from the CA Identity Manager media. This wizard detects previous versions of CA Identity Manager, prompts you through the upgrade process in the correct sequence, and launches all component installers from one location. Be sure that you have 2GB of available space in the %TEMP% directory before running the upgrade wizard.

The wizard does not apply if you have certain versions of the application server. Instead, you migrate the Identity Manager Server, which means you perform an installation and reinstallation of that server.

The following sections explain the upgrade and migration procedures.

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.

Decide About Options During Upgrade

The installer performs the following tasks that you could instead choose to perform manually:

- Upgrade the workflow database—updates the workflow database schema to work with WorkPoint 3.4.2.
- Migrate task persistence—migrates all pending Identity Manager tasks from a previous version of CA Identity Manager to the upgraded version.

  Note: After the upgrade, you can migrate all other tasks (not in a pending state) by manually running the task persistence data migration. For more information, see Manual Upgrades (see page 73).
- Migrate Identity Manager Directories and Environments—migrates all directories and environments from SiteMinder to the Identity Manager object store, if upgrading from CA Identity Manager r8.1 SP2. SiteMinder objects that are no longer used are not deleted after the migration, but you can manually delete them after the upgrade.

  Note: For RDB user stores, the recreation of the directories and environments is a manual process.

If you want to perform these tasks during the upgrade, select the appropriate check box when prompted by the installer. If you would rather perform these tasks manually after the upgrade, the section Manually Upgrade the Identity Manager Server (see page 76) provides the steps you need.

Upgrade the Provisioning Directory

As of 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. For Provisioning 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 (see page 27) instead of performing an 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. Stop Ingres with the following command:
   ingstop –service(or ingstop -kill)
4. Verify that all of the following Ingres processes are stopped:
   - dmfacp.exe
   - dmfrcp.exe
   - iidbms.exe
   - iigcc.exe
   - iigcn.exe
   - iijdbc.exe
   - iistar.exe
5. Restart Ingres with the following command:
   ingstart –service
6. Verify that the Provisioning Server and Connector Server services are stopped.
7. Run the CA Identity Manager installer from the CA Identity Manager media.

   The Upgrade Wizard starts.

8. In the Upgrade Wizard, next to Provisioning Directory, click Launch Upgrade. If you have more than one Provisioning Directory, this step applies only to the primary Provisioning Directory.

   The Provisioning Directory upgrade wizard starts.

   Note the following:

   - Due to architectural changes effective 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 resumes.
   - 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.
   - 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.

9. 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*.

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.

Migrating your Provisioning Directory

When upgrading to CA Identity Manager r12.5 SP5, 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 SP5 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 -O -f *filename* -p dc=etadb -S *DSA_name database_name*
5. Stop the -main, -co, and -inc DSAs on the new host by running the following commands from a command prompt:
   dxserver stop *new_system_name-impd-main*
   dxserver stop *new_system_name-impd-inc*
   dxserver stop *new_system_name-impd-co*
6. Load the data file produced in Step 4 into all the DSAs by running the following commands from a command prompt:
   dxloaddb -s *new_system_name-impd-main* filename
   dxloaddb -s *new_system_name-impd-co* filename
   dxloaddb -s *new_system_name-impd-inc* filename

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

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

   The r12.5 SP5 Provisioning Directory is now running on the new system with all the data from the old system. The old Provisioning Directory can now be removed.

8. Uninstall and reinstall any alternate Provisioning Directories.

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

Note: Be sure to use the *new* Provisioning Directory hostname when upgrading the Provisioning Servers. The default in the upgrade installer 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. If you're not already in the Upgrade Wizard, 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:

   - If you see a Deprecated Connector Warning, be sure to consult the *Connectors Guide* for migration steps to be completed after the upgrade.
   - Choose the Custom setup type when prompted, then 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.

3. 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.

Upgrade the Identity Manager Server

The following components are upgraded with the installer:

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

All unused files will be deleted.

The following custom configuration files will be preserved:

- Policy Server connection
- Data store definitions

Select the Right Upgrade Procedure

The appropriate procedure for upgrading the Identity Manager Server depends on which version of the application server you have installed. The following tables identify the procedure that applies.

Note: For more information about supported application servers, see the CA Identity Manager support matrix on the CA Support Site. Note that cross-platform upgrades (between UNIX and Windows) are not supported.

For JBoss

Use the following table to pick the appropriate procedure.

If you have...	Configured as a...	And plan to use...	Perform this procedure...
JBoss 3.2.2 or 4.2.3	Single Node	4.2.3	Use the Upgrade Wizard (see page 31)
JBoss 4.0.5	Single Node	4.2.3	Uninstall and Reinstall the Identity Manager Server (see page 38)
JBoss 3.2.2, 4.0.5, or 4.2.3	Cluster	4.2.3	Uninstall and Reinstall the Identity Manager Server (see page 38)

For WebLogic

Use the following table to pick the appropriate procedure.

If you have...	Configured as a...	And plan to use...	Perform this procedure...
WebLogic 8.1	Single Node or Cluster	WebLogic 9.2 or 10.3	Uninstall and Reinstall the Identity Manager Server (see page 38)
WebLogic 9.2	Single Node	WebLogic 9.2	Use the Upgrade Wizard (see page 31)
WebLogic 9.2	Cluster	WebLogic 9.2	Upgrade on a WebLogic 9.2 cluster (see page 32)
WebLogic 10.3	Single Node or Cluster	WebLogic 10.3	Use the Upgrade Wizard (see page 31)

For WebSphere

Use the following table to pick the appropriate procedure.

If you have...	Configured as a...	And plan to use...	Perform this procedure...
WebSphere 6.0.2.17	Single Node or Cluster	WebSphere 6.1.0.17	Uninstall and Reinstall the Identity Manager Server (see page 38)
WebSphere 6.1.0.15	Single Node	WebSphere 6.1.0.17	Use the Upgrade Wizard (see page 31)
WebSphere 6.1.0.(15 or 17)	Cluster	WebSphere 6.1.0.17	Upgrade on a WebSphere 6.1.0.x Cluster (see page 34)

Use the Upgrade Wizard for the Identity Manager Server

Important! The upgrade wizard applies in specific situations. Use the Upgrade Wizard to upgrade the Identity Manager Server only if you were referred here by Select the Right Upgrade Procedure (see page 30).

To upgrade the Identity Manager Server

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

   The Upgrade Wizard starts.

2. Click Launch Upgrade from the Upgrade Wizard.
3. Respond to the prompts that appear.

Upgrade on a WebLogic 9.2 Cluster

Important! Use this procedure *only* if you were referred here by Select the Right Upgrade Procedure (see page 30).

Upgrading the Identity Manager server on a WebLogic 9.2 cluster depends on the current installation.

- For an 8.1 SP2 Identity Manager server, the r8.1 SP2 Identity Manager Server on WebLogic 9.2 procedure (see page 41) applies.
- For an r12 or higher Identity Manager Server, see the steps that follow.

To upgrade the Identity Manager Server r12 or higher on a WebLogic 9.2 cluster

1. Perform the prerequisite steps (see page 11).
2. Shut down all the managed nodes.
3. In the Weblogic Admin Console, under Deployments, delete castylesr5.1.1.ear.
4. Shut down the application server.
5. On the admin server, delete the castylesr5.1.1.ear folder from this location:
   bea\userprojects\domains*domain-name*\applications
6. On each node, delete the Identity Manager EAR folder from the staging area:
   bea\weblogic92\common\nodemanager\servers*server_name*\stage\
7. On each node, delete the Identity Manager EAR folder from the WebLogic cache:
   bea\weblogic92\common\nodemanager\servers*server_name*\tmp_WL_user\
8. Stop the SiteMinder services, if you are using SiteMinder.

9. Run the CA Identity Manager installer from the system where the previous CA Identity Manager installation was run.

   Note: For more information about installing on a cluster, see the *Installation Guide (WebLogic)*.

10. Start WebLogic on the Admin Server.
11. Configure each managed node using the Configure Managed Nodes procedure in the Weblogic cluster section of the *Installation Guide*.
12. On each node, verify that all subdeployments point to the JMS servers that existed prior to the upgrade.
    a. Target GeneralMonitorCFdeployment subdeployment to each of the IM JMS servers. Associate GeneralMonitorCFdeployment with these resources:
       - GeneralMonitorCF
       - IMS Events
       - Run time status
       - Server Command Topic
       - General Monitor Messages

    b. If you have workflow, set wpConnectionFactory subdeployment to point to the Workflow JMS servers.

       wpConnectionFactory associates with the resources queue/wpServAutoActQueue, queue/wpUtilQueue, queue/wpEventQueue, and jms/wpConnectionFactory.

13. Optionally, migrate the task persistence data (see page 80).
14. Restore all customizations to the cluster.
15. Update the new index.jsp.

    For more information, see the *User Console Design Guide*.

16. Start all the managed nodes from the Weblogic admin console.

    Starting the server first time after the upgrade generates workpoint errors. However, proceed with this step. Deploying the application on all nodes makes modifying the configuration easier.

17. If the nodes are not running on the default port, update the workpoint-client.properties file under identityMinder.ear/config on each node. Replace localhost with the hostnames of the system where the node is installed.

Upgrade on a WebSphere 6.1.0.x Cluster

If you are upgrading from WebSphere 6.1.0.15 or 6.1.0.17, perform the appropriate procedure depending on which version of CA Identity Manager you have installed.

- Upgrade from CA Identity Manager r8.1 SP2 (see page 34)
- Upgrade from CA Identity Manager r12 (see page 37)
- Upgrade from CA Identity Manager r12.5 or r12.5 SP1 (see page 38)

Upgrade CA Identity Manager r8.1 SP2 on a WebSphere 6.1.0.15 Cluster

Use this procedure if you are upgrading CA Identity Manager r8.1 SP2 running on a WebSphere 6.1.0.15 cluster.

To upgrade from CA Identity Manager r8.1 SP2

1. Perform the prerequisite steps (see page 11).
2. Install the minimum supported version of WebSphere and the minimum supported JDK version.

   Note: See the CA Identity Manager support matrix on CA Support for the latest supported versions.
3. Remove all cluster members from the cluster except one cluster member.

   The remaining cluster member is referred to as the *primary cluster member*.
4. Shut down the remaining cluster member.
5. Stop the SiteMinder services.
6. If JAAS – J2C authentication aliases are used with Task Persistence data sources (JNDI name jdbc/idm) or Workflow data sources (JNDI name jdbc/WPDS), be sure to remove the association from those data sources, as follows:
   a. In the Administrative Console, go to Resources, JDBC, Data Sources.
   b. Open the data source.
   c. Locate the 'Component-managed authentication alias' section.
   d. Make note of the alias currently used and replace it with none.
   e. Repeat Steps a through d for the other data sources.
7. On the system where the Deployment Manager is installed, run the CA Identity Manager installer and launch the Upgrade Wizard.
8. Start the Deployment Manager.

9. If you performed Step 6, restore the JAAS – J2C authentication alias information previously used for Task Persistence data sources (JNDI name jdbc/idm) and Workflow data sources (JNDI name jdbc/WPDS), as follows:
   a. In the Administrative Console, go to Resources, JDBC, Data Sources.
   b. Open the data source.
   c. Locate the 'Component-managed authentication alias' section.
   d. Restore the alias information you noted in Step 6.
   e. Repeat Steps a through d for the other data sources.
10. Add back the cluster members, as follows:
   a. In the Administrative Console for the Deployment Manager, go to Servers, Clusters.
   b. Add a cluster member, selecting one of the nodes for which you created a profile.
   c. Repeat this procedure for each cluster member you need to add to the cluster.
11. Configure the message engines for each added cluster member that you added back to the cluster, as follows:

   Note: You do not need to configure the message engine for the primary cluster member.

   a. From the Deployment Manager, navigate to *Websphere_home*/profiles/d*eployment_manager_profile*/bin.
   b. Execute wsadmin as follows:

      For Windows:

      wsadmin -f ims6SetupClusterMember.jacl *node server cluster jndiname*

      For Unix/Solaris:

      ./wsadmin -f ims6SetupClusterMember.jacl *node server cluster jndiname*

      Note: If you want to use the existing messaging store, use the same JNDI name that you used in the previous installation. If you are creating a messaging store, enter the new jndiname for that store.

c. Verify that the script completes with a "Save the Configuration" message and no errors.

d. Repeat Steps b and c for each added cluster member.

12. Verify the message store information, as follows:

a. In the Administrative Console, go to Service Integration, IMSBus.

b. For each message engine, verify the following message store information:

- The data source JNDI name is a JNDI name of an existing data source
- The schema name is an existing schema name in the database associated with this data source.

  The default IBMWSSIB may not work, for example, 'dbo' for MS SQL.

c. Verify that the Core Group policy exists for each messaging engine, and that each cluster member has a messaging engine targeted to it through the policy's preferred server.

Note: For more information about creating core group policies, see the *Installation Guide*.

13. Configure the messaging engine stores for each cluster member, as follows:

a. In the Administrative Console, go to Service Integration, Buses, IMSBus, Messaging engines, select the messaging engine name, and click message store.

b. Change the schema name for the messaging engine store to the database schema name.

c. If you are using *existing* messaging stores, run the following commands on the database for each messaging store you reuse:

- truncate table SIB000
- truncate table SIB001
- truncate table SIB002
- truncate table SIBXACTS
- truncate table SIBKEYS
- truncate table SIBOWNER
- truncate table SIBOWNERO
- truncate table SIBCLASSMAP
- truncate table SIBLISTING

14. Update the WebSphere Path definition for each cluster member, for example, if you have clusterMember1 and clusterMember2, update as follows:
    a. In the Administrative Console, go to Application servers, clusterMember1, Server Infrastructure, Java and process definition, Process Definition, Environment Entries.
    b. Add the full path to the IdentityMinder.ear/library directory. For example, on Windows, the path may be: C:\Program Files\IBM\WebSphere\AppServer\profiles\AppSrv02\installedApps\wasserverCell01\IdentityMinder.ear/ library
    c. Repeat Steps a and b for clusterMember2.
15. Restore any customizations to the cluster (see page 45).
16. Perform post-upgrade configurations (see page 55).

Upgrade CA Identity Manager r12 on a WebSphere 6.1.0.x Cluster

Use this procedure if you are upgrading CA Identity Manager r12 running on a WebSphere 6.1.0.15 or 6.1.0.17 cluster.

To upgrade from CA Identity Manager r12

1. Perform the prerequisite steps (see page 11).
2. Install the minimum supported version of WebSphere and the minimum supported JDK version.

   Note: See the CA Identity Manager support matrix on CA Support for the latest supported versions.
3. Shut down the application server.
4. Stop the SiteMinder services, if you are using SiteMinder in your environment.
5. On the system where the Deployment Manager is installed, run the CA Identity Manager installer and launch the Upgrade Wizard.
6. Start the Deployment Manager.
7. If you are using SiteMinder, update the WebSphere Path definition for each cluster member, for example, if you have clusterMember1 and clusterMember2, update as follows:
    a. In the Deployment Manager, go to Application servers, clusterMember1, Server Infrastructure, Java and process definition, Process Definition, Environment Entries.
    b. Add the full path to the IdentityManager.ear/user_console.war/WEB-INF/lib directory. For example, on Windows, the path may be: D:\Program Files\IBM\WebSphere\AppServer\profiles\AppSrv02\installedApps\wasserverCell01\IdentityMinder.ear\user_console.war\WEB-INF\lib
    c. Repeat Steps a and b for clusterMember2.

8. After you complete the upgrade, navigate to *Websphere_home*\Application Server\profiles*dm_profile*\bin on the Deployment Manager, and run the following command against all cluster members *except* the primary cluster member:
   wsadmin -f ims6AddWfEventsJMSQueue.jacl *node server cluster*
9. Restore any customizations to the cluster (see page 45).

Upgrade CA Identity Manager r12.5 or r12.5 SPx on a WebSphere 6.1.0.x Cluster

Use this procedure if you are upgrading CA Identity Manager r12.5 or r12.5 SPx running on a WebSphere 6.1.0.15 or 6.1.0.17 cluster.

To upgrade from CA Identity Manager r12.5 or r12.5 SPx

1. Perform the prerequisite steps (see page 11).
2. Shut down the application server.
3. Install the minimum supported version of WebSphere and the minimum supported JDK version.

   Note: See the CA Identity Manager support matrix on CA Support for the latest supported versions.
4. Stop the SiteMinder services, if you are using SiteMinder in your environment.
5. On the system where the Deployment Manager is installed, run the CA Identity Manager installer and launch the Upgrade Wizard.
6. Restore any customizations to the cluster (see page 45).

   Note: If you upgraded from r12.5, update the new index.jsp. For more information, see the *User Console Design Guide*.

Uninstall and Reinstall the Identity Manager Server

Perform the appropriate procedure depending on which version of the application server is currently installed.

- JBoss (see page 39)
- WebLogic 8.1 (see page 40)
- WebLogic 9.2 (see page 41)
- WebSphere 6.0.2.17 cluster (see page 43)
- WebSphere 6.0.2.17 single node (see page 44)

Uninstall and Reinstall the Identity Manager Server on JBoss

Important! The following procedure applies in specific situations. Use this procedure to uninstall and reinstall the Identity Manager Server *only* if you were referred here by Select the Right Upgrade Procedure (see page 30).

To uninstall and reinstall the Identity Manager Server on JBoss

1. Back up all custom code (see page 15).
2. Stop the SiteMinder services, if you are using SiteMinder in your environment.
3. Uninstall the Identity Manager Server. See the Uninstallation and Installation appendix of the *Installation Guide*.

   This step leaves the Identity Manager environments and directories unchanged.
4. Upgrade your application server to a supported version if it is not already installed.
5. If you are upgrading CA Identity Manager on a system which already has JBoss 4.2.3, 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.
6. Perform a new install of the Identity Manager Server.

   Note: For more information about installing on a cluster, see the *Installation Guide (JBoss).*

   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 SP5 values.

   Important! If you are upgrading from CA Identity Manager r8.1 sp2 or 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. 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
8. Upgrade the workflow database (see page 77).
9. If you are upgrading from CA Identity Manager r8.1 sp2, export the Directories and Environments (see page 78).
10. Migrate the Task Persistence data (see page 80).
11. If you are upgrading from CA Identity Manager r8.1 sp2, recreate the Directories (see page 80).

12. If you are upgrading from CA Identity Manager r8.1 sp2, recreate the Environments (see page 80).
13. Reapply all custom code.

    Note: If you are using a cluster, be sure to reapply all customizations to the cluster.
14. Start the cluster and verify the installation using the cluster section of the *Installation Guide.*

Uninstall and Reinstall the Identity Manager Server on WebLogic 8.1

Important! The following procedure applies in specific situations. Use this procedure to uninstall and reinstall the Identity Manager Server *only* if you were referred here by Select the Right Upgrade Procedure (see page 30).

To uninstall and reinstall the Identity Manager Server on a WebLogic 8.1 single node or cluster

1. Back up all custom code (see page 15).
2. Stop the SiteMinder services, if you are using SiteMinder in your environment.
3. Uninstall the Identity Manager Server. See the Uninstallation and Installation appendix of the *Installation Guide*.

   This step leaves the Identity Manager environments and directories unchanged.
4. Upgrade WebLogic to 9.2 or 10.3 if it is not already installed.
5. Perform a new install of the Identity Manager Server.

   Note: For more information about installing on a cluster, see the *Installation Guide.*

   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 SP5 values.

   Important! If you are upgrading from CA Identity Manager r8.1 sp2 or r12 and you have different database stores for task persistence, workflow, audit, and reports, update the data sources to point to the separate stores.
6. Upgrade the workflow database (see page 77).
7. If you are upgrading from CA Identity Manager r8.1 sp2, export the Directories and Environments (see page 78).
8. Migrate the Task Persistence data (see page 80).
9. If you are upgrading from CA Identity Manager r8.1 sp2, recreate the Directories (see page 80).

10. If you are upgrading from CA Identity Manager r8.1 sp2, recreate the Environments (see page 80).
11. Reapply all custom code.

    Note: If you are using a cluster, be sure to reapply all customizations to the cluster.
12. Start WebLogic and verify the installation using the procedures in the *Installation Guide.*

Uninstall and Reinstall an r8.1 SP2 Identity Manager Server on WebLogic 9.2

Important! The following procedure applies in specific situations. Use this procedure to uninstall and reinstall the Identity Manager Server *only* if you were referred here by Select the Right Upgrade Procedure (see page 30).

To uninstall and reinstall an r8.1 SP2 Identity Manager Server on WebLogic 9.2

1. Take note of the location from which the IdentityMinder, SiteMinder, and SiteMinderAgent applications were deployed to the cluster.

   The path appears in the WebLogic Admin Console under Deployments, *application_name*, Overview, Path.
2. Back up all custom code (see page 15).

   The IdentityManager.ear found in step 1 is the one to back up, not the EAR from the staging area of any managed server.
3. In the WebLogic Admin Console under Deployments, delete the IdentityMinder, SiteMinder and SiteMinderAgent applications.
4. Shut down the weblogic server.
5. On the admin server, delete the IdentityManager.ear, SiteMinder.ear, and SiteMinderAgent.ear folders from the location they were deployed from in r8.1 SP2.
6. On each node, delete the IdentityManager, SiteMinder, and SiteMinderAgent folder from the staging area. They are in the following locations:

   bea\weblogic92\common\nodemanager\servers*server_name*\stage\IdentityMinder

   bea\weblogic92\common\nodemanager\servers*server_name*\stage\SiteMinder

   bea\weblogic92\common\nodemanager\servers*server_name*\stage\SiteMinderAgent

7. Uninstall the Identity Manager Server. See the Uninstallation and Installation appendix of the *Installation Guide*.

   This step leaves the Identity Manager environments and directories unchanged.

8. If you are using a remote installation of SiteMinder and wish to continue to use it to protect your Identity Manager Environment, perform the following steps:

   a. Run the Identity Manager installer on that host to upgrade the Extensions for SiteMinder.

   b. Configure the Policy Store for CA Identity Manager.

   Note: For more information about installing on a cluster, see the *Installation Guide (Weblogic).*

9. Reinstall the Identity Manager Server, making sure you take the following actions:

   - If you plan to continue to use SiteMinder, select Connect to Existing SiteMinder Policy Store on the Select Components screen.
   - If you have different database stores for task persistence, workflow, audit, and reports, update the data sources to point to the separate stores.

10. Configure all managed nodes using the *Installation Guide* procedure. However, in the last step of the Configure Managed Nodes procedure, *replace* the existing IM_SM_PATH definition line rather than *adding* a new line at the bottom of the file.

    For example, in *WL_HOME*\weblogic92\common\bin\commEnv.cmd, the following line points to the old SiteMinder library:

    IM_SM_PATH=%WL_HOME%\common\nodemanager\lib

    Replace this line with the following line:

    IM_SM_PATH=%WL_HOME%\common\nodemanager\servers\<server>\stage\IdentityMinder\IdentityMinder.ear\library

    This complete path does not exist yet since you have not started the managed node since reinstalling Identity Manager.

11. On the Admin Server, start WebLogic.

12. In the Admin Console, start one managed node.

13. Upgrade the workflow database (see page 77).

14. Export the Directories and Environments (see page 78).

15. Migrate the Task Persistence data (see page 80).

16. Recreate the Identity Manager Directories (see page 80).

17. Recreate the Identity Manager Environments (see page 80).

    Reapply all custom code, making sure you reapply all customizations to the cluster.

18. Restart all managed nodes and verify the installation using the cluster section of the *Installation Guide*.

Uninstall and Reinstall the Identity Manager Server on a WebSphere 6.0.2.17 Cluster

Important! The following procedure applies in specific situations. Use this procedure to uninstall and reinstall the Identity Manager Server *only* if you were referred here by Select the Right Upgrade Procedure (see page 30).

To avoid port conflicts, we recommend uninstalling WebSphere 6.0 before installing the supported version of WebSphere. However, you must first back up the IdentityMinder EAR as described in Step 3 of the following procedure.

To uninstall and reinstall the Identity Manager server on WebSphere 6.0.2.17 cluster

1. Install the minimum supported version of WebSphere and the minimum supported JDK version.

   Note: See the CA Identity Manager support matrix on CA Support for the latest supported versions.

2. Create a cluster with one member.

   See the WebSphere Cluster Setup section in the *Installation Guide* for details.

3. Perform the prerequisite steps (see page 11).

   Note: Be sure to back up the IdentityMinderEAR (see page 16). Also, If the system where CA Identity Manager is to be installed contains SiteMinder and you are using CA Directory for your SiteMinder policy store, we recommend that you do *not* install the Provisioning Directory on this system.

4. Uninstall the Identity Manager Server. See the Uninstallation and Installation appendix of the *Installation Guide*.

5. If you did *not* uninstall WebSphere 6.0, stop the older version of WebSphere.

6. Start the new version of WebSphere.

   Note: If both versions of WebSphere use the same port number, they cannot be running at the same time.

7. Perform a new installation of the Identity Manager Server. Do not use existing messaging store databases with the new installation.

   Note: For more information, see How to Install CA Identity Manager on a WebSphere Cluster in the *Installation Guide*.

   Be sure to provide the existing CA Identity Manager database credentials during the install.

   Important! If you have different database stores for task persistence, workflow, audit, and reports, update the data sources to point to the separate stores.

8. Upgrade the workflow database (see page 77).

9. Export the Directories and Environments (see page 78) from the SiteMinder Policy Store.

10. Migrate the Task Persistence data (see page 80).
11. Restore all customizations to the cluster (see page 45).
12. Perform post-upgrade configurations (see page 55).

Uninstall and Reinstall the Identity Manager Server on a WebSphere 6.0.2.17 Single Node

Important! The following procedure applies in specific situations. Use this procedure to uninstall and reinstall the Identity Manager Server *only* if you were referred here by Select the Right Upgrade Procedure (see page 30).

To uninstall and reinstall the Identity Manager Server on a WebSphere 6.0.2.17 single node

1. Back up all custom code (see page 15).
2. Stop the SiteMinder services, if you are using SiteMinder in your environment.
3. Uninstall the Identity Manager Server. See the Uninstallation and Installation appendix of the *Installation Guide*.

   This step leaves the Identity Manager environments and directories unchanged.
4. Upgrade WebSphere to 6.1.0.17 if it is not already installed.
5. Perform a new install of the Identity Manager Server.

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

   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 SP5 values.

   Important! If you are upgrading from CA Identity Manager r8.1 sp2 or r12 and you have different database stores for task persistence, workflow, audit, and reports, update the data sources to point to the separate stores.
6. Upgrade the workflow database (see page 77).
7. If you are upgrading from CA Identity Manager r8.1 sp2, export the Directories and Environments (see page 78).
8. Migrate the Task Persistence data (see page 80).
9. If you are upgrading from CA Identity Manager r8.1 sp2, recreate the Directories (see page 80).
10. If you are upgrading from CA Identity Manager r8.1 sp2, recreate the Environments (see page 80).
11. Reapply all custom code.
12. Start the application server and verify the installation using the *Installation Guide.*

Restore Cluster Customizations on WebSphere

When you upgrade a cluster on WebSphere, be sure to restore all customizations to that cluster after the upgrade.

To restore cluster customizations on WebSphere

1. Navigate to *deployment_manager_dir*\bin.
2. Be sure the Deployment Manager is running.
3. Export the deployed CA Identity Manager application, as follows:

   For Windows:

   wsadmin -f imExport.jacl IdentityMinder *path-to-exported-ear*

   For Unix/Solaris:

   ./wsadmin -f imExport.jacl *path-to-exported-ear*

   where *path-to-exported-ear* is the full path, including the file name of the exported EAR file.
4. Copy any saved customization files from your old EAR to the appropriate folder in the exported EAR for CA Identity Manager r12.5 SP5. For example, copy any saved emailTemplates from the old EAR into the new, exported EAR's IdentityMinder.ear\custom\emailTemplates folder.
5. Copy the ims6Upgrade.jacl script from *Websphere_home*\WebSphere-tools to the *deployment_manager_dir*\bin directory where:
   - *Websphere_home* is the directory where WebSphere is installed.
   - *deployment_manager_dir* is the location where the Deployment Manager is installed.
6. On the Deployment Manager, deploy the updated IdentityMinder EAR, as follows:
   a. From the command line, navigate to the following location:

      deployment_manager_dir \bin.

   b. Be sure that the Deployment Manager is running.

   c. Run the ims6Upgrade.jacl script, as follows:

      Note: The ims6Upgrade.jacl script can take several minutes to execute.

      For Windows:

      wsadmin -f ims6Upgrade.jacl *path-to-copied-ear cluster_name*

      For UNIX/Solaris:

      ./wsadmin -f ims6Upgrade.jacl path-to-copied-ear *cluster_name*

      where *path-to-copied-ear* is full path including the file name for the IdentityMinder EAR that you copied to the Deployment Manager system.

   Note: After the upgrade, update the new index.jsp. For more information, see the *User Console Design Guide.*

Verify the Environments

When you have completed the main upgrade procedures, check that you can see the environments.

Important! If you are upgrading from CA Identity Manager r8.1 sp2, be sure to follow the post-upgrade configuration steps (see page 55) before verifying the upgrade.

To verify the environments

1. Start the Management Console as follows:

   http://host_name:port/idmmanage

   host_name

   Defines the fully-qualified host name for the server where Identity Manager is installed

   port

   Defines the application server port.

2. If you migrated an Identity Manager environment, access the environment as follows:

   a. Enter the URL for the Identity Manager environment.

   b. Verify that you are prompted for the appropriate credentials.

   c. Log in using the account with the System Manager role.

   d. Verify the correct roles are assigned to this account.

3. If these steps succeeded, start any extra Policy Servers and CA Identity Manager nodes that you stopped.

   Note: If you still need to make changes to an Identity Manager environment, skip this step until you are done.

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.

Upgrade Reporting

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

Upgrade the Report Server

If you are upgrading from a version of CA Identity Manager prior to r12.5, upgrade to a supported version of the Report Server.

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. Download the CA Business Intelligence Common Reporting package and unzip it.

   The CA Business Intelligence Common Reporting is available for download on the CA Support site, under CA Identity Manager product downloads.

   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 ensure that you execute the installation media from the VM folder.
3. Navigate to Disk1\InstData\VM and double-click the installation executable.

   The installer starts and prompts you for a locale.
4. Choose Update as the Installation Type when prompted.
5. Accept default settings during the rest of the installation.
6. Click Install.

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

To verify the upgrade of the Report Server

1. Check the ca-install.log file in the Report Server install folder. The file should contain the following:

   Patch boeXIR2_SP4 installed successfully.
2. Check the Patch.properties file in the Report Server install folder. The file should contain the following:

   [boeXIR2_SP4]

Update the Default Reports

Update the default reports to reflect changes made to reports for CA Identity Manager r12.5 SP5.

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

To update the default reports

1. Unzip the importbiarfilestool.zip file on the machine where the Report Server is installed. This tool can be found in the following location:

   admin_tools\BIARTool

   Important! Unzip this file to the root folder of the drive where the Report Server (Business Objects) is installed.

2. Run the following file in the import-biar-tool folder:

   importIMBIARFiles.bat

   Note: Before running the previous file, ensure that the JAVA_HOME variable is set correctly and that you have JDK1.5 installed.

   Provide the following information needed to import the default reports:

   - Report Server Root Folder—location of the business objects install folder, for example, E:\Program Files\CA\SC\CommonReporting\BusinessObjects
   - Enterprise 1.5
   - Reporting Database Type—1=MSSQL, 2=Oracle

     Note: This is the database that the Report Server (CA Business Intelligence) uses to store its own data.
   - Reporting Database User—user created for the Report Database
   - Reporting Database Password—password for the user created in Report Database
   - Reporting Database DSN Name—the ODBC DSN name created
   - Reporting Database Name—the Report Database name
   - Reporting Server Administrator Name—The default is Administrator. If you have a different administrator name, provide it here.
   - Reporting System Password—reporting administrator's password entered during the installation

- BIAR File Location—use one of the following:
  - *admin_tools*\imrexport\ReportDefinitions\IM Standard Reports\Ms-SQL_Reports\ms-sql_reports.biar
  - *admin_tools*\imrexport\ReportDefinitions\IM Standard Reports\Oracle Reports\oracle_reports.biar

The default reports are imported in the IM Reports folder of the Report Server.

Note: After the import completes, you are asked if you want to remove the biekInstall.properties file. BiekInstall.properties contains sensitive information, such as user passwords. This file is not used again by the tool, but it can be kept for future reference.

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 SP5.

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*.

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.

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.

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 SP5 Java Connector Server is compatible with the CA Identity Manager r8.1 SP2 and 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.

Chapter 4: Configuration After Upgrade from CA Identity Manager r8.1 SP2

This section contains the following topics:

How to Perform Post-Upgrade Configuration

Perform the following configuration steps after upgrading from CA Identity Manager r8.1 SP2:

	Step
	1. (WebSphere only) Enable XA transactions.
	2. (RDB only) Modify the RDB user store and recreate Directories and Environments.
	3. Upgrade custom workflow scripts.
	4. Update the application server proxy forwarder.
	5. Upgrade TEWS.
	6. Specify an Inbound Administrator.

(WebSphere only) Enable XA Transactions

When using WebSphere with Microsoft SQL, enable XA transactions. CA Identity Manager needs an XA data source for the database transactions to work properly. For more information about enabling XA transactions on Microsoft SQL Server, go to http://msdn.microsoft.com/en-us/library/aa342335.aspx http://msdn.microsoft.com/en-us/library/aa342335.aspx.

Note: Be sure to use JDBC driver version 1.2 compatible DLL files when enabling XA transactions.

(RDB Only) Modify the User Store

If you are using a relational database user store, edit the generated directory.xml after the upgrade.

To modify an RDB user store

1. Modify the directory.xml file that you exported from CA Identity Manager r8.1 SP2. Add the configured JDBC data source information as the first element of <Provider>. For example,

   ```
   <Provider userdirectory="rdb_orgless" type="RDB">
   <JDBC datasource=" jdbc/userstore "/>
   ```

2. Remove the maxrows attribute from the DirectorySearch element.
3. If your RDB user store supports Organizations, run the following script located in the *admin_tools*\samples\NeteAutoRdb\Organization\ directory:
   - **SQL:** mssql-orgpath-addon-upgrade-8-to-r12.sql
   - **ORACLE:** oracle-orgpath-addon-upgrade-8-to-r12.sql

Recreate Directories and Environments

The Directories (see page 80) and Environments (see page 83) were automatically exported during the upgrade. However, you need to manually recreate the Directories and Environments after the upgrade. To do this, see the Manual Upgrades section of this guide.

Upgrade Custom Workflow Scripts

If you developed custom workflow scripts using the Workflow API in previous versions of CA Identity Manager, do the following:

- Change all occurrences of ClientContextEJB to ClientContext. For example, if you have custom code that resembles the following:

  ```
  public void approvalRequired(ClientContextEJB clientContext,
  SymbolTable symbolTable,
  JobData ThisJobData) throws Exception
  ```

  change it as follows:

  ```
  public void approvalRequired(ClientContext clientContext,
  SymbolTable symbolTable,
  JobData ThisJobData) throws Exception
  ```

- Change the method signature used to generate the workflow context. For example, if you have custom code that resembles the following:

  ```
  JobUserDataTable imsIdUD = job.getUserData("ims-id");
  imsId = (String)imsIdUD.getVariableValue();
  WorkflowContext workflowContext = (new
  WorkflowCallbackHelper()).generateWorkflowContext(imsId);
  ```

  change it as follows:

  ```
  JobUserDataTable imsIdUD = job.getUserData("ims-id");
  imsId = (String)imsIdUD.getVariableValue();
  envOid = (String)job.getUserData("ime-id").getVariableValue();
  WorkflowContext workflowContext = (new
  WorkflowCallbackHelper()).generateWorkflowContext(imsId,envOid);
  ```

Update the Proxy Forwarder

CA Identity Manager r12 introduced a new CA styles EAR. To support this, change the web server plug-in that is used to forward to the application server, by adding a redirection to /castylesr5.1.1 in addition to /idm in the http proxy forwarder.

Note: For more information about the Proxy Plug-in, see the *Installation Guide*.

Upgrade TEWS

In CA Identity Manager r12, the WSDL file configuration changed. When upgrading from a pre-r12 version of CA Identity Manager, change the WSDL file to work with r12.5 SP5.

To recreate the WSDL files

1. Generate the WSDL file in CA Identity Manager r12.5 SP5.
2. Keep the following code segments unchanged:
   - _PND__PND_objectType
   - _PND__PND_friendlyName (when it is used as password policy friendly name)
   - _PND__PND_regExValue
   - _PND__PND_bNoMatch
   - _PND__PND_passwordPolicyOid
3. Remove any other "_PND__PND_" from the customized web service code. Capitalize the first character after "_PND__PND_". For example, ViewAccessRoleSearchResultResultItem_PND__PND_friendlyName should be changed to ViewAccessRoleSearchResultResultItemFriendlyName.
4. Six method names in six WSDL classes have changed. Modify the customized web service code appropriately if these classes are referenced. The method list is as follows:

If you had this method in CA Identity Manager r8.1 SP2...	Use this method in CA Identity Manager r12.5 SP5...
setName()	setEventName()
getName()	getEventName()
setTag()	setTabTag()
getTag()	getTabTag()
setWorkflow()	setWorkflowProcess()
getWorkflow()	getWorkflowProcess()

The six WSDL classes are as follows:

- CreateAdminTaskEventsTabEventCurrentvalue
- CreateAdminTaskEventsTabEventModify
- ModifyAdminTaskEventsTabEventCurrentvalue
- ModifyAdminTaskEventsTabEventModify
- ViewAdminTaskEventsTabEventCurrentvalue
- ViewAdminTaskEventsTabEventModify

5. Save the WSDL file.

Specify an Inbound Administrator

If you have provisioning enabled in your environment, verify that you have specified an Inbound Administrator.

To specify an Inbound Administrator

1. In the Management Console, click on the Environment.
2. Under the Provisioning Server property, click configure (green arrow) to configure the Provisioning Directory.
3. Under Provisioning Properties, check that the Inbound Administrator field is populated.
4. If there is no Inbound Administrator, specify one before continuing the upgrade.

Chapter 5: New Feature Configuration

This section contains the following topics:

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 exists to upgrade your environment from different releases of CA Identity Manager and for environments that may or may not have an organization.

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.
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*.

Migrate Option Pack 1 Functionality

If you upgraded from CA Identity Manager r12 with Option Pack 1 installed, perform the following steps:

1. (WebSphere Only) Replace necessary Option Pack files to complete the migration.
2. Import the Option Pack Migration task.
3. Run the Option Pack Migration task located under the Option Pack tab.
4. (WebLogic Only) Update the Option Pack path.
5. Complete the manual steps associated with Option Pack migration.
6. Verify the Option Pack migration.

(WebSphere Only) Replace Necessary Option Pack Files

1. Start the application server.
2. In the Administrative Console, do the following:
   a. Go to Applications, Enterprise Applications.
   b. Select IdentityMinder.
   c. Click Update.
   d. Select Replace, add, or delete multiple files.
   e. Select Local file system.
   f. Click Browse and select the *option_pack_home*/install/WebSphere/additional.zip file.
   g. Click Next to update IdentityMinder, as follows:
      - Click OK to update.
      - Wait until the console shows Update of IdentityMinder has ended.
      - Click Save.
3. Repeat Step two using the *im_home*/IAM Suite/Identity Manager/tools/OPMigrationTool/user_console.update.zip file.
4. Restart the application server.
5. Check the WebSphere SystemOut.log file and be sure that no exceptions are listed.

Import the Option Pack Migration Task

In the Management Console, import the Upgrade-OptionPack1-to-12.5SP1-RoleDefinitions file for the environment you want to upgrade. Importing this role definitions file adds the Option Pack Migration task to the Option Pack tab in the User Console.

To import the Option Pack migration task

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 Upgrade-OptionPack1-to-12.5SP1-RoleDefinitions file.
6. Click Finish.
7. Restart the environment.

Once you import the Option Pack role definitions file, go to the Option Pack tab in the User Console and run the Option Pack Migration task (see page 63).

Run the Migration Task

In the User Console, go to the Option Pack tab and run the Option Pack Migration task. This task migrates the following Option Pack functionality into CA Identity Manager:

- Scheduled Task (now Bulk Tasks) definitions
- Reverse Sync configurations
- Policy Xpress policies and Policy Xpress user data
- Email configurations
- Option Pack out of office delegation

Note: Run the migration task on *every* environment you want to upgrade.

Once you run the Option Pack Migration task, perform the post-upgrade manual steps (see page 66) to complete the Option Pack migration.

Functionality Changes Due to Migration

When you migrate the Option Pack 1 functionality to CA Identity Manager, some of the functionality changes and some configurations must be recreated. Note the following changes when migrating:

- Email configurations are changed in that dynamic email content and dynamic recipients are of the Custom type.
- Workflow configurations have changed, therefore all workflow configurations you defined in the Option Pack must be recreated.
- Delegation has changed in that you can no longer assign different approvers per attribute. If your Option Pack delegation configurations were set to 'All', they are moved to the CA Identity Manager delegation model. If there is no 'All' configuration, the first approver is selected for all approvals in the configuration.
- Option Pack account screens are replaced with account screens for CA Identity Manager r12.5 SP5. For more information about creating account screens in CA Identity Manager r12.5 SP5, see the *Administration Guide*.

  Note: Any Policy Xpress policies with account management categories, such as User defined, Screen Builder Policies, and AD Account Management Screens, will not be migrated.
- SOD policies that existed in the Option Pack are no longer supported. For more information about SOD and preventative identity policies in CA Identity Manager, see the *Implementation Guide*.

View Migration Details

When you run the Option Pack Migration task, it appears in View Submitted Tasks. To view the migration details, drill into the task and click the Event named Option Pack Migration. These details describe the Option Pack components that are migrated, and outline any outstanding issues that occur during migration that may require additional manual steps.

We recommend reviewing these details to identify which components require manual updates to work in CA Identity Manager r12.5 SP5. For example, changes to Policy Xpress policies that used plug-ins that no longer exist in this release.

The following graphic shows an example of the migration details that appear in View Submitted tasks:


Event History

Source	Description
WORKFLOW	There was no workflow process mapped to this event. Fetching default workflow process definition.
WORKFLOW	There was no default workflow process mapped to this event.
MIGRATION	Start Policy Xpress migration.
MIGRATION	Start PX policy send to initiator in create user migration
MIGRATION	PX policy send to initiator in create user migration ended with status: Completed
MIGRATION	Policy data source contains data element Endpoint type. The plugin 'Endpoint objects' had been deprecated since it is no longer valid. Please revise the policy.
MIGRATION	Start PX policy data source migration
MIGRATION	PX policy data source migration ended with status: Completed
MIGRATION	Start PX policy All other option migration
MIGRATION	PX policy All other option migration ended with status: Completed
MIGRATION	Start PX policy event complete migration

(WebLogic Only) Update Option Pack Path

If you are using WebLogic, update the path of the Option Pack folder for the Identity Manager Server to start successfully.

Update the Option Pack folder path

1. Go to *weblogic_home*\user_projects\domains*domain_name*\bin.
2. Open the setDomainEnv.cmd.bak file and copy the line starting with “set JAVA_OPTIONS=%JAVA_OPTIONS% -DidFocusHomeDir”.
3. Edit the setDomainEnv.cmd file and paste the copied line from Step 2 above the line saying “set JAVA_OPTIONS=%JAVA_OPTIONS%”.

   The setDomainEnv.cmd file should read as follows:

   set JAVA_OPTIONS=%JAVA_OPTIONS% -DidFocusHomeDir="<OP home folder>".
   set JAVA_OPTIONS=%JAVA_OPTIONS%

Post-Upgrade Manual Option Pack Migration Steps

You complete the Option Pack migration by performing the following manual steps:

- Workflow Configuration

  Because workflow is different between Option Pack 1 and the CA Identity Manager r12.5 SP5, all workflow configurations must be recreated.

  Note the following when recreating your workflow processes:

  1. A new global workflow setting exists in the CA Identity Manager r12.5 SP5. To access the global workflow setting, go to System, Configure Global Policy Based Workflow for Events.
  2. When creating new workflow processes, consider the type of event used. User attribute changes are related to Create/Modify User events. Account changes are related to the Create/Modify event for the dedicated event.
  3. When modifying objects that are associated with accounts, such as Active Directory Groups, the objects behave differently when assigning the object to a user, versus modifying the object itself. When assigning these objects to a user, the system generates different events that connect the object and the account, therefore creating a relationship between the object and the account. Consider these differences when creating new workflow processes. To see all events associated with a task, view the admin task and click the Events tab.
  4. A new Escalation Process template for workflow is available. Follow the sample workflow process (see page 69) upgrade steps to import the template.

- WorkPoint Change

  In the WorkPoint Designer, remove the StateWorkpointListener agent from any process where you manually added it.

- Reverse Sync Workflow Settings

  Reverse Sync policies that contained a workflow action are migrated so that workflow is now configured as part of the policy. These migrated policies are automatically created using a default workflow process. Edit any policy that had a workflow process associated with it, and recreate the workflow configuration as necessary. We recommend using single-step approvals for Reverse Sync workflow.

- Reverse Sync Scheduling

  In the Option Pack, Reverse Sync had a definition component and a scheduling component. The definitions have been migrated, but Reverse Sync is no longer scheduled as a separate task. To schedule Reverse Sync, create an Explore and Correlate definition and schedule it normally.

  Note: For more information about Explore and Correlate, see the *Administration Guide*.

- Scheduled Tasks (now Bulk Tasks)

  In the Option Pack, Scheduled Tasks had a definition component and a scheduling component. The definitions have been migrated, but the scheduling has not been migrated. Go to System, Bulk Tasks, Execute Bulk Task to run or schedule a bulk task definition.

- Policy Xpress Plug-ins Removed

  The "Has Account Attribute Changed" and "Endpoint Objects" plug-ins were removed from Policy Xpress. If you had any Policy Xpress policies in the Option Pack that used these plug-ins, revise them to work with the new account structure in Policy Xpress. Also, update any data elements and actions around account attributes with newly required details.

- Remaining Option Pack Data

  After migrating the Option Pack, the following data is no longer used and can be removed:

  - the Option Pack folder under the Identity Manager folder
  - the Option Pack database and data source
  - the Option Pack Migration task and Option Pack tab in the User Console

Verify the Option Pack Migration

Perform the following steps to verify that the Option Pack migration was successful.

1. Check the application server log files after the upgrade. Address any errors that appear.
2. Verify the new tasks in CA Identity Manager. Log in to the User Console as a user with the System Manager role and check for any new tasks, such as the Policy Xpress tasks under Policies.
3. Verify that any Option Pack 1 tasks are gone.

   Note: Check this step in every Option Pack environment that you upgraded.
4. Review the migration task details in View Submitted Tasks.
5. Verify that new objects pertaining to the old Option Pack functionality have been created CA Identity Manager.

Finding Option Pack Functionality in CA Identity Manager r12.5 SP5

Use the table below to access Option Pack 1 functionality in CA Identity Manager r12.5 SP5.

Functionality in Option Pack 1...	Location in CA Identity Manager r12.5 SP5...
Email Notifications	Go to System, Email.
Policy Xpress	Go to Policies, Policy Xpress.
Reverse Sync New/Modify	Go to the Endpoint tab.
Scheduled Tasks	Go to System, Bulk Tasks.
SOD	Go to Policies, Manage Identity Policies. **Note:** For more information about this change in functionality, see the documentation on preventative identity policies.
Workflow	To map an event to a workflow process, use the Management Console or associate the event with policy-based workflow approval policies in a specific task. For global event level policy-based workflow, in the User Console, go to System, Configure Global Policy Based Workflow for Events.

Note: For more information about any of the previous functionality, see the *Administration Guide*.

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 Sample Workflow Processes

To support Template-method workflow, Task-level workflow, and 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 81to12UpgradeWFScripts.zip.

   This script imports the Template-method and Task-level workflow processes.
3. Select one work item.
4. Click Import.
5. Answer the prompts, as follows:
   - Are you importing in to empty DB tables: No
   - This import will: treat all objects as new objects
   - If Duplicate Name or reference is encountered: Rename the imported Name or Reference to be unique
6. Repeat Steps 3 through 5 for all work items.
7. Navigate to *admin_tools*\workflowScripts and select 12.5to12.5SPUpgradeWFScripts.zip.

   This script imports the Escalation Process template.

8. Repeat Steps 3 through 5 for all work items.
9. 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*.

Add Workflow Support for AccumulatedProvisioningRolesEvent

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

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

To approve or reject individual actions within the AccummulatedProvisioningRolesEvent, an approver uses a specific approval screen that lets him select an Approve or Reject radio 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-8.1-to-12.5SP-RoleDefinitions.xml, 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.

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.

Configure IPv6 Support

If you are installing on a JBoss system that supports IPv6, some configuration is required.

To configure IPv6 on a JBoss application server

1. Open the run_idm.bat/sh file located in *jboss_installation*\bin.
2. Uncomment *one* of the following properties in the JAVA_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"
3. Save the file.

Appendix A: Manual Upgrades

This section contains the following topics:

How to Manually Upgrade to CA Identity Manager r12.5 SP5

If you want to upgrade to CA Identity Manager r12.5 SP5 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 SP5

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. If upgrading from CA Identity Manager r8.1 SP2, perform the post-upgrade configuration steps.
10. Upgrade other provisioning components.
11. Recompile custom code.
12. 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 SP5, 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 (see page 27) instead of performing an upgrade.

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

To manually upgrade the Provisioning Directory

1. If you have primary and alternate Provisioning Directories, back up your primary Provisioning Directory.
2. Shut down all Provisioning Directories in your environment.
3. Stop Ingres with the following command:
   ingstop –service(or ingstop -kill)
4. Verify that all of the following Ingres processes are stopped:
   - dmfacp.exe
   - dmfrcp.exe
   - iidbms.exe
   - iigcc.exe
   - iigcn.exe
   - iijdbc.exe
   - iistar.exe
5. Restart Ingres with the following command:
   ingstart –service
6. Verify that the Provisioning and Connector services are stopped.
7. (Windows only) Be sure the Local Service account has read/write permissions to the folder where 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.
3. If upgrading from CA Identity Manager r8.1. SP2, do the following:
   a. Manually export the Directories and Environments.
   b. Perform the configuration after an upgrade from CA Identity Manager r8.1 SP2 (see page 55).
   c. Recreate the Directories and Environments.

Manually Upgrade the Workflow Database

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 after upgrading CA Identity Manager.

After updating the workflow database, you can continue to use the workflow processes that you developed in WorkPoint 3.3.

To upgrade to WorkPoint 3.4.2

1. 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.

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

3. 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.

4. 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.

5. 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.

6. 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.

7. Save all changes to the database.

Note: The WorkPoint scripts are located in Administrative Tools folder\Workpoint\database. 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

Manually Export the Directories and Environments

As of CA Identity Manager r12, objects previously stored in the SiteMinder Policy Store need to be moved to a relational database object store. SiteMinder objects that are no longer used are not deleted after the migration, but you can manually delete them after the upgrade.

Use the Migration Tool (imsconfig.bat/imsconfig.sh) to export your Directory and Environment configurations. Then, use the Management Console to re-import the configurations into CA Identity Manager.

Important! Do not use the Export button under Environments in the Management Console when performing an upgrade. This button is for exporting CA Identity Manager r12 environments only.

Note: Be sure that your SiteMinder Policy Server is running before attempting to export a Directory or Environment.

To export a Directory and Environment

1. Navigate to the following directory:
   admin_tools\81to12Migration-tool\
2. Be sure that the IM_ROOT variable in the imsconfig script points to the correct location, as follows:
   - Windows: IM_ROOT=*admin_tools*\81to12Migration-tool\lib
   - Unix: IM_ROOT=*admin_tools*/81to12Migration-tool/lib

   where *admin_tools* is the location of the tools for CA Identity Manager r12.5 SP5.
3. Export a Directory by running the following command:
   imsconfig -h *policy_server_hostname* -a *agent_name* -s *agent_shared_secret* -u siteminder_super_user_name -p siteminder_super_user_password -d *im_directory* -x *folder_name*

   policy_server_hostname

   Specifies the hostname of the system with the Policy Server installed.

   agent_name

   Defines the agent.

   agent_shared_secret

   Defines the agent's shared secret.

   siteminder_super_user_name

   Defines the SiteMinder administrator.

   siteminder_super_user_password

   Defines the SiteMinder administrator password.

im_directory

Defines the name of the CA Identity Manager directory to export.

folder_name

Defines the name of the folder where you'd like the Migration Tool to place the generated directory.xml file.

The Directory configuration is exported into the standard directory.xml file.

4. Export an Environment by running the following command:
imsconfig -h *policy_server_hostname* -a *agent_name* -s *agent_shared_secret* -u siteminder_super_user_name -p siteminder_super_user_password -e *im_environment* -m *folder_name*

policy_server_hostname

Specifies the hostname of the system with the Policy Server installed.

agent_name

Defines the agent.

agent_shared_secret

Defines the agent's shared secret.

siteminder_super_user_name

Defines the SiteMinder administrator.

siteminder_super_user_password

Defines the SiteMinder administrator password.

im_environment

The name of the CA Identity Manager environment to export.

folder_name

The name of the folder where you'd like the r12 Migration Tool to place the generated ZIP file.

The Environment configuration is exported into an *environmentname*_environment.zip file, which contains the following three environment settings XML files:

- *environmentname*_environment_roles.xml—environment role definitions
- *environmentname*_environment_settings.xml—environment settings not included with the role definitions
- *environmentname*_environment.xml—general environment information

Manually Migrate Task Persistence Data

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. Set up the task persistence database migration, by updating the tpmigration125.properties file with the object store and task persistence information including the store values. The tpmigration125.properties file is located in the following location:

   admin_tools/tpmigration/com/ca/tp/migratetpto125

2. Be sure that the environment variable JAVA_HOME is set.
3. 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
4. Enter the following information:
   - Environment protected Alias ('all' for all environments).

     Note: If you do not specify all, only one environment can be entered.
   - Task state.
     Note: If you do not specify all, only one task state can be entered.
   - CA Identity Manager version to migrate from (1-8.x, 2-12.0).
   - Date range for the tasks to be migrated (y/n).

     Note: If you choose 'y', you must 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.

Manually Recreate the Identity Manager Directory

When doing a manual upgrade of the Identity Manager Server, manually recreate the Directory and re-import the information into the object store, using the Management Console.

Recreate the Directory on JBoss

To recreate the Directory on JBoss

1. (RDB Only) Create the data source as follows:
   a. Using the task persistence data source as a template (imtaskpersistencedb-ds.xml), create a userstore-ds.xml data source descriptor file and put it in the *jboss_home*/server/default/deploy directory.
   b. Change the JNDIName in the data source descriptor to a unique name, for example, jdbc/userstore.
   c. Change the DatabaseName, User, and Password in the data source descriptor to the appropriate values for the userstore database.
2. In the Management Console, click Directories.
3. Click New.
4. Import the previously exported directory.xml to create an Identity Manager Directory.
5. Click Next.
6. Verify the directory settings and click Finish.

   The old directory is recreated for CA Identity Manager r12.5 SP5.

Note: For more information about creating new Identity Manager Directories, see the *Configuration Guide*.

Recreate the Directory on WebLogic

To recreate the Directory on WebLogic

1. (RDB Only) Create the data source as follows:
   a. Within the WebLogic Administrative Console, create a userstore data source descriptor.
   b. Change the JNDIName in the data source descriptor to a unique name, for example, jdbc/userstore.
   c. Change the DatabaseName, User, and Password in the data source descriptor to the appropriate values for the userstore database.
   d. Disable Support Global Transactions on the data source.
2. In the Management Console, click Directories.
3. Click New.
4. Import the previously exported directory.xml to create an Identity Manager Directory.

5. Click Next.
6. Verify the directory settings and click Finish.

   The old directory is recreated for CA Identity Manager r12.5 SP5.

Note: For more information about creating new Identity Manager Directories, see the *Configuration Guide*.

Recreate the Directory on WebSphere

To recreate the Directory on WebSphere

1. (RDB Only) Create the data source as follows:
   a. Within the WebSphere Administrative Console, create a userstore data source descriptor.
   b. Change the JNDIName in the data source descriptor to a unique name, for example, jdbc/userstore.
   c. Change the DatabaseName, User, and Password in the data source descriptor to the appropriate values for the userstore database.
   d. Depending on your database, do one of the following:
      - **SQL:** Be sure that the data source is XA, and create a property for the data source called *enable2phase* and set it to true.
      - **Oracle:** Be sure that the data source is XA.
2. In the Management Console, click Directories.
3. Click New.
4. Import the previously exported directory.xml to create an Identity Manager Directory.
5. Click Next.
6. Verify the directory settings and click Finish.

   The old directory is recreated for CA Identity Manager r12.5 SP5.

Note: For more information about creating new Identity Manager Directories, see the *Configuration Guide*.

Manually Recreate the Environment

When doing a manual upgrade of the Identity Manager Server, manually recreate the Environment and reimport the information into the object store, using the Management Console.

Note: If you are upgrading from CA Identity Manager r12 and you implemented some of the account management preview functionality for certain endpoint types, remove all data (tabs and screens) related to those endpoint types from the roledefinition.xml file before importing it into CA Identity Manager r12.5 SP5. To access your provisioning information and the new CA Identity Manager functionality for these endpoint types, import the specific endpoint type roledefinition.xml file after recreating the environment.

Important! If you want to continue to use SiteMinder to protect your Identity Manager Environment, change the agent name in the *environmentname*_environment.xml within the exported ZIP file *before* importing the environment into CA Identity Manager r12.5 SP5. This agent name must be the same agent specified in the SiteMinder realm that protected the CA Identity Manager r8.1 SP2 Environment. For example,

```
<?xml version="1.0" encoding="UTF-8"?>
<ImsEnvironment name="neteauto_rdb_orgless" directory="neteauto_rdb_orgless" provisioningdirectory="eta"
alias="neteautordb" publicalias="neteautoprdb_public" publicuser="2" jobtimeout="15"
basedir="http://baseidm.dev.com:9080/idm" agent="iis6webagent"
imstemplatefile="neteauto_rdb_orgless_environment_roles.xml"
envsettingsfile="neteauto_rdb_orgless_environment_settings.xml"
oid="35-bb06e65d-b7d7-4c0d-9d5a-f15021ae210d" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="imsconfig://schema/ImsEnvironment.xsd"/>
```

To recreate the environment

1. In the Management Console, go to Environments.
2. Click the Import button.
3. Browse for the following ZIP file created during the environment export:
   ims_env_name.zip
4. Click Finish.

   CA Identity Manager recreates the environment.

Note: If the connection to your task persistence database goes down during the recreation of the environment, or your task persistence data is not completely migrated over to CA Identity Manager r12.5 SP5, you can use the Migrate button on the Environment page in the Management Console to restart the migration process. Restarting this process does not duplicate tasks that have already been migrated.

Appendix B: Unattended Upgrades

This section contains the following topics:

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-r12.5sp*N*-win32.exe -f im-installer.properties -i silent
- **UNIX:**
  ./ca-im-r12.5sp*N*-sol.bin -f im-installer.properties -i silent

sp*N* 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.

Note: Currently we do not support unattended upgrade when CA Identity Manager has been deployed manually to the WebSphere application server. Running the unattended installation for WebSphere will perform a fresh install instead of 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 C: Upgrade Verification

This section contains the following topics:

How to Verify the Upgrade

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

- CA Directory and Provisioning Directory
- Provisioning Server & Connector Server
- 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
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
18:41:30,882 WARN  [default] * Startup Step 11 : Attempting to start PasswordService
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 15 : Attempting to start NotificationRuleService
18:41:30,898 WARN  [default] * Startup Step 16 : Attempting to start EventAdapterService
18:41:30,898 WARN  [default] * Startup Step 17 : Attempting to start TaskService
18:41:30,913 WARN  [default] * Startup Step 18 : Attempting to start WorkflowCallbackService
18:41:30,929 WARN  [default] * Startup Step 19 : Attempting to start WorkflowService
18:41:30,944 WARN  [default] * Startup Step 20 : Attempting to start EventService
18:41:31,023 WARN  [default] * Startup Step 21 : Attempting to start AdminService
18:41:31,038 WARN  [default] * Startup Step 22 : Attempting to start GeneralMonitorAdmin
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.
```

Object Store

Verify that CA Identity Manager r8.1 SP2 objects were successfully imported into an object store for CA Identity Manager r12.5 SP5, by checking that the set of directory and environment objects listed in the Management Console matches the set in the CA Identity Manager r8.1 SP2 store.

Pending Tasks

Verify that the previous CA Identity Manager version's pending tasks were migrated to CA Identity Manager r12.5 SP5, 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. From Start, Programs, Business Objects, start the Central Configuration Manager. 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. If all of the services have started, log into the Admin Launchpad, by going to the following URL: http://ls3:8080/businessobjects/enterprise115/adminlaunch.
4. Launch the Central Management console.

Index

N

O

P

R

S

U

V