CA Identity Manager

Upgrade Guide (WebSphere)

r12.5 SP10

CA Technologies Product References

This document references the following CA products:

- CA Identity Manager
- CA SiteMinder®
- CA Directory
- User Activity Reporting Module (UARM)
- 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

Providing Feedback About Product Documentation

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

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 7: Post-Upgrade Configuration 77

Appendix A: Upgrade Verification 97

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 SP10:

- 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 these versions of CA Identity Manager, upgrade to one of these versions, then upgrade to CA Identity Manager r12.5 SP10.

Note: Upgrades from ACE to r12.5 SP10 are *not* supported. Also, cross-platform upgrades (between UNIX and Windows) are not supported.

How to Upgrade CA Identity Manager

Perform the following steps to upgrade CA Identity Manager:

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

Chapter 2: Upgrade Prerequisites

This section contains the following topics:

How to Meet Prerequisites for the Upgrade

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

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

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

Check Hardware Requirements

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) 2.0 GHz (Windows or Red Hat Linux), SPARC 1.5 GHz (Solaris) or POWER4 1.1 GHz (AIX)	Dual core Intel (or compatible) 3.0 GHz (Windows or Red Hat Linux), Dual core SPARC 2.5 GHz (Solaris) POWER5 1.5 GHz (AIX)
Memory	4 GB	8 GB
Available Disk Space	4 GB	8 GB
Temp Space	2 GB	4 GB
Swap/Paging Space	2 GB	4 GB
Processor	32-bit processor and operating system for small deployments 64-bit processor and operating system for intermediate and large deployments, dual core	64-bit processor and operating system, quad core

Provisioning Server or a Standalone Connector Server

Component	Minimum	Recommended
CPU	Intel (or compatible) 2.0 GHz (Windows) SPARC 1.5 GHz (Solaris)	Dual core Intel (or compatible) 3.0 GHz (Windows) SPARC 2.0 GHz (Solaris)
Memory	4 GB	8 GB

Component	Minimum	Recommended
Available Disk Space	4 GB	8 GB
Processor	32-bit processor and operating system for small deployments 64-bit processor and operating system for intermediate and large deployments, dual core	64-bit processor and operating system, quad core

Provisioning Directory

Component	Minimum	Recommended
CPU	Intel (or compatible) 1.5 GHz (Windows) SPARC 1.0 GHz (Solaris)	Dual core Intel (or compatible) 2.5 GHz (Windows) SPARC 1.5 GHz (Solaris)
Memory	4 GB	8 GB
Available Disk Space	2 to 10 GB, depending on the number of endpoint accounts ■ Compact—Up to 10,000 accounts, 0.25 GB per 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, 64-bit operating system, and CA Directory (64 bit version) for intermediate and large deployments	64-bit processor and operating system

All Components on One System

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

Component	Minimum
CPU	Intel (or compatible) 3.1 GHz (Windows) SPARC 2.5 GHz (Solaris)
Memory	8 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, quad core
Swap/Paging Space	6 GB

Check Software Requirements

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

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

Check the following software components for required versions:

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

Back Up Custom Code

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

- C++ custom connectors
- Provisioning manager plug-ins for Java custom connectors
- Each cluster member's customizations, such as non-default ports for workflow

- Custom files inside the EAR, for example, files under the IdentityMinder.ear/custom/ directory. Do *not* back up any files under the following folders:
  - resourcesBundles
  - identitymanager
  - provisioning
- Common program exits
- Custom email templates at the following location:
  `...\IdentityMinder.ear\custom\emailTemplates`
- Universal Provisioning Option (UPO) program exits
- Pluggable Authentication Module (PAM) DLLs
- Identity Manager Server custom code, such as Event Listener class files, Business Logic Task Handler (BLTH) class files, and Logical Attribute Handler (LAH) class files, and property files at the following location:
  `...\IdentityMinder.ear\config`
- Customized skin folder at the following location:
  `...\IdentityMinder.ear\user_console.war\app\imcss\`
- Customized help, back up the help property file at the following location:
  `..\IdentityMinder.ear\config\com\netegrity\config\`

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

Apply CA Directory License Patch

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

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

You can download the patch on the CA Support site.

To locate the patch

1. Log into the support.ca.com.

   The CA Support site opens.
2. CA Licensing.

3. Click License Package 1.8 is Now Available.

   A page opens that describes the changes to the License Package, and includes a link for downloading it.

4. Follow the instruction to download and install the Windows patch.

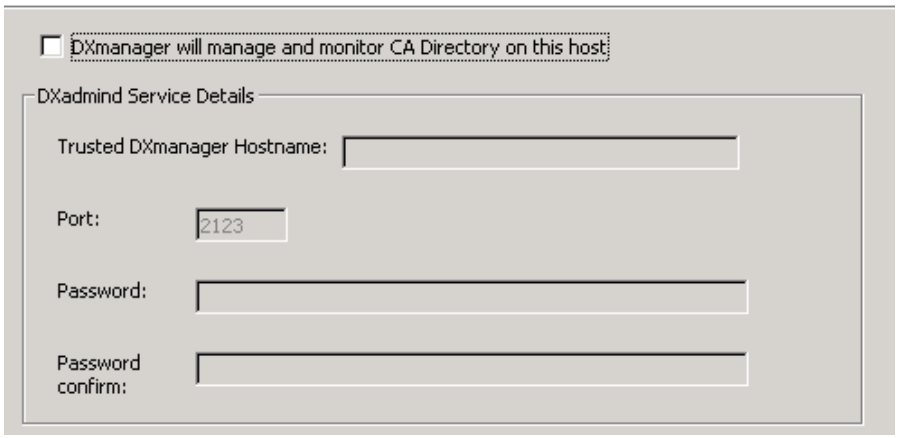
Note: You also need this patch if you plan to manually uninstall eTrust Directory r8.

Upgrade CA Directory on r12.5 or higher Systems

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

To upgrade CA Directory, navigate to the CA Directory installation folder on the CA Identity Manager media and run the dxsetup.exe file. The correct version of CA Directory is included on the CA Identity Manager installation media.

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



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

Close Option Pack Workflow Items

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

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

Install JCE Libraries for SiteMinder

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

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

WebSphere Application Server

The Identity Manager Server is a J2EE application that is deployed on a supported application server. When using WebSphere as the CA Identity Manager application server, perform the following procedures.

Upgrade WebSphere

CA Identity Manager r12.5 SP10 works with Websphere 6.1 (for an upgrade) or Websphere 7 (for a new installation or a migration of CA Identity Manager).

If you need a new version of the IBM WebSphere, install the WebSphere server as described in IBM's documentation. During the installation, perform these actions:

- Select the appropriate plug-in for your Web Server.
- Select the Server and Client options.
- Install the latest FixPack to the server and the required JDK.

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

Verify WebSphere

Use the following tests to verify that WebSphere is working:

- Test whether the WebSphere application server is installed correctly by accessing IBM's snoop utility at the following URL:

  http://*hostname*:*port*/snoop

  For example:

  http://MyServer.MyCompany.com:9080/snoop

  If WebSphere is installed correctly, the Snoop Servlet—Request Client Information page is displayed in the browser.

- If you have a web server installed, test that the WebSphere application server plug-in is installed correctly. Use IBM's snoop utility without including the application server port in the URL:

  http://*hostname*/snoop

  For example:

  http://MyServer.MyCompany.com/snoop

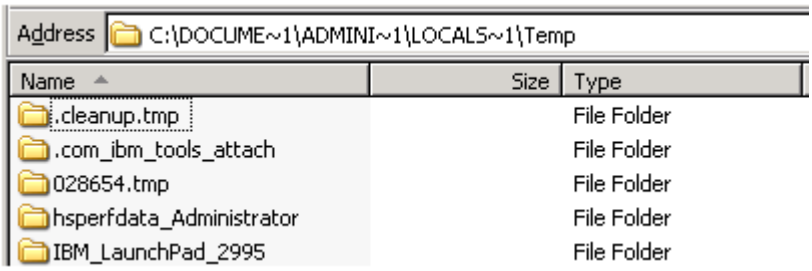
  If WebSphere is installed correctly, the same Snoop Servlet—Request Client Information page is displayed in the browser. This means that profile was created and has at least one server which is configured with the plug-in.

For additional help with WebSphere, contact IBM customer support.

Configure WebSphere for the Upgrade

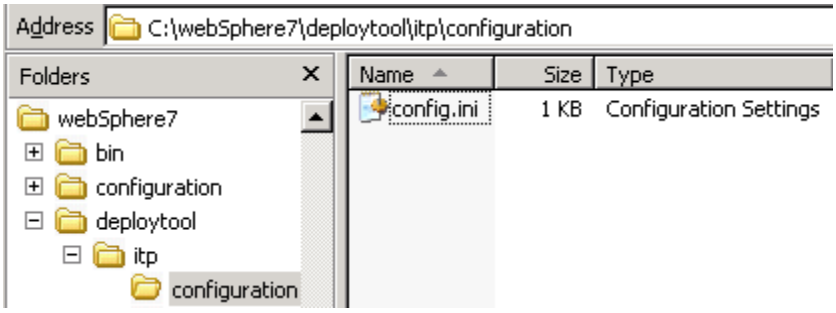
An upgrade on WebSphere may fail due to disk space errors or timeout errors. Perform the following steps to ensure that your upgrade succeeds on WebSphere.

1. Save any changes to the WebSphere configuration via the Administrative Console (Save to Master Configuration).
2. Shut down the application server.
3. Remove all files and folders in the following directories:
   - Temp Directory:
     - Unix: /tmp/*
     - Windows: %temp%

   - *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.

Enable XA Transactions for Microsoft SQL Server

If you are using WebSphere with Microsoft SQL Server, enable XA transactions on Microsoft SQL Server. CA Identity Manager needs an XA data source for the database transactions to work properly.

To enable XA Transactions for Microsoft SQL Server

1. Download the SQL Server JDBC Driver version 2.0 from Microsoft.

   Note: The download may first present an HTM file that is a license agreement for you to approve.

2. Run the program to install the JDBC driver.
3. Perform the following two procedures included in the Microsoft topic Understanding XA Transactions:
   - Running the MS DTC Service
   - Configuring the JDBC Distributed Transaction Components

   In performing these procedures, verify the following are true:
   - When you run the xa_install.sql script, make sure you get a script complete message. You can ignore the drop table errors, which appear the first time that you run the script.
   - When you add the user to the SqlJDBCXAUser role, add that user to the master database.

Configure SSL

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

Complete the Upgrade Worksheets

Provisioning Directory Information

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

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

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

- Compact—up to 10,000 accounts
- Basic—up to 400,000 accounts
- Intermediate (64 bit only)—up to 600,000 accounts
- Large (64 bit only)—more than 600,000 accounts

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

Provisioning Server Information

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

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

Java Connector Server Information

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

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

Database Connection Information

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

Field Name	Description	Your Response
Database Type	The database type (vendor/version) of the database created for task persistence, workflow, audit, reporting, object storage, and task persistence archive.	
Host Name	The hostname of the system where the database is located. **Note:** Be sure that you provide a hostname and *not* an IP address.	
Port Number	The port number of the database.	
Database Name	The database identifier.	

Field Name	Description	Your Response
Username	The username for database access. **Note:** This user must have administrative rights to the database unless you plan to import the schema manually.	
Password	The password for the user account with administrative rights.	

WebSphere Information

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

Field Name	Description	Your Response
WebSphere Install Folder	The location of the application server home directory.	
Server Name	The name of the system on which the application server is running.	
Profile Name	The name of the profile you want to use for CA Identity Manager.	
Cell Name	The name of the cell in which the application server is located.	
Node Name	The name of the node in which the application server is located.	
Cluster Name	The cluster name for high-availability implementations. This is only needed if you plan on installing CA Identity Manager in a clustered environment.	
Access URL and port	The application URL and port number of the system that will host the Identity Manager Server (system that will host the application server).	

Login Information

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

Field Name	Description	Your Response
Username	A username that you create to log into the provisioning components.	
Provisioning Server password	A password for this Server.	
C++ Connector Server password	A password needed for this server. Each C++ Connector Server can have a unique password.	
Provisioning Directory password	A password used by Provisioning Server to connect to Provisioning Directory. For an alternate Provisioning Server, enter the Provisioning Directory password created for the primary Provisioning Server.	

SiteMinder Information

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

Field Name	Description	Your Response
Policy Server Host Name	The hostname of the SiteMinder Policy Server.	
SiteMinder Administrator Name	The administrator username for the SiteMinder Policy Server.	

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

Chapter 3: Provisioning Components Upgrade

This section contains the following topics:

Architecture Changes

For r12.5 and higher releases, CA Identity Manager includes a router DSA and a notification DSA:

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

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

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

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

Upgrade the Provisioning Directory

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

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

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

- Close cmd.exe
- Stop CA Identity Manager

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

To upgrade the Provisioning Directory

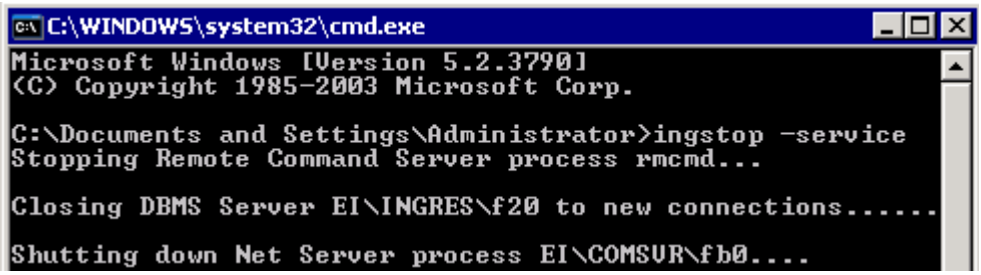
1. If you have primary and alternate Provisioning Directories, back up your primary Provisioning Directory.
2. Shut down all Provisioning Directories in your environment.
3. If you are upgrading from a release prior to CA Identity Manager r12.5, complete the following steps

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

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

   a. Stop Ingres with the following command:

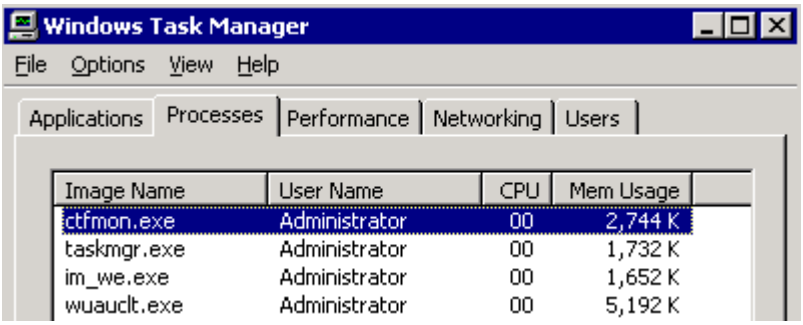
      ```
      ingstop –service
      ```



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

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

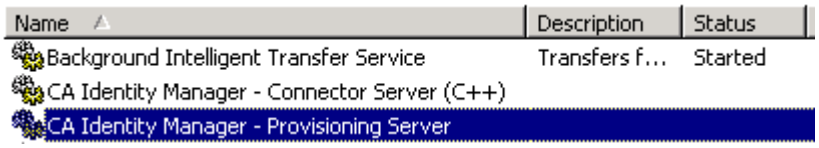
- dmfacp.exe
- dmfrcp.exe
- iidbms.exe
- iigcc.exe
- iigcn.exe
- iijdbc.exe
- iistar.exe



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

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

4. Stop the Connector Server and Provisioning Server services.

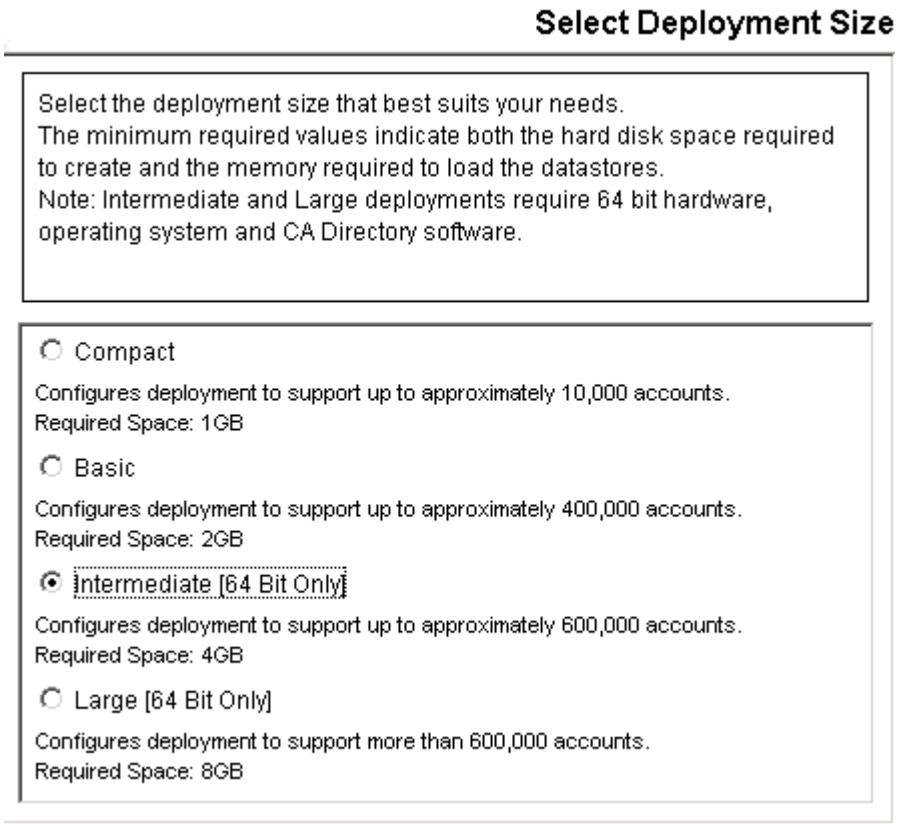


5. Choose the upgrade method for the provisioning directory:

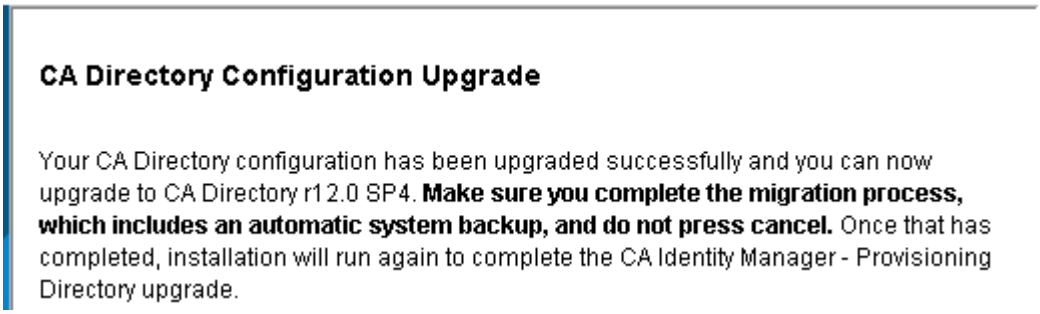
- If you are upgrading from an r12.5 or r12.5 SP release, you can upgrade using the installer, which starts the upgrade wizard.
- If you are upgrading from an r12 release, use upgrade.bat (or upgrade.sh) in the CADirectory/dxserver directory, not the Provisioning Directory setup.exe file. The upgrade.bat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

6. Answer the question about deployment size if the Select Deployment Size screen appears in your upgrade. Consider the following guidelines, while allowing room for future growth:
   - Compact—up to 10,000 accounts
   - Basic—up to 400,000 accounts
   - Intermediate (64 bit only)—up to 600,000 accounts
   - Large (64 bit only)—more than 600,000 accounts

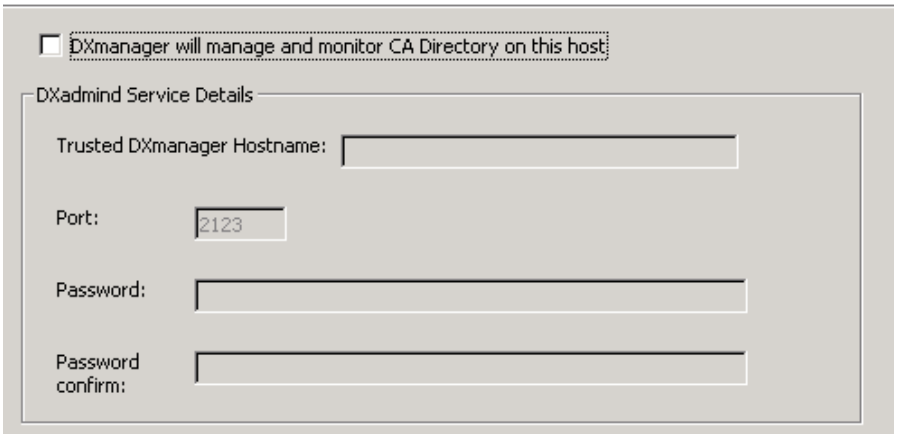
   Note: If you are installing a Provisioning Directory in an established CA Identity Manager installation, be sure to make the deployment size large enough. Otherwise, an error occurs because the data does not fit when loaded into the data files. Intermediate and Large installations require 64-bit Directory installs (either Solaris or Windows 64 bit).



7. If you are installing the Provisioning Directory in an FIPS 140-2 enabled environment, select the FIPS 140-2 Compliance mode check box during installation and provide the FIPS Key File.
8. If you are upgrading a pre-r12.5 installation, a CA Directory Upgrade Configuration appears:



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



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

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

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

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

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

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

Migrate the Provisioning Directory

When upgrading to CA Identity Manager r12.5 SP10, 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 SP10 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 SP10 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 (for a 32-bit system) or CADirectory_x64 (for a 64 bit system).

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

Note the following when upgrading the Provisioning Server:

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

To upgrade the Provisioning Server

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

   The Upgrade Wizard starts.

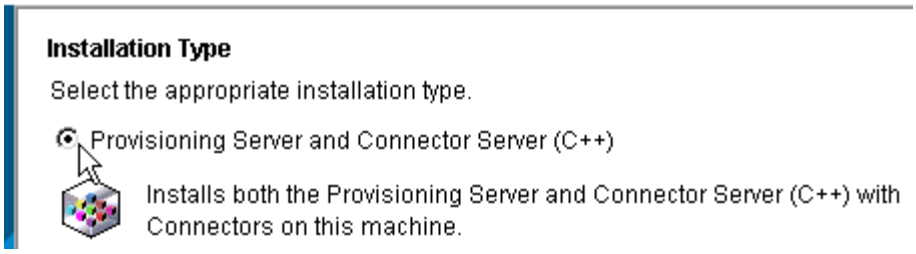
2. In the Upgrade Wizard, next to Provisioning Server, click Launch Upgrade.

   The Provisioning Server upgrade starts. Note the following:

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

4. Select the Custom setup type when prompted.

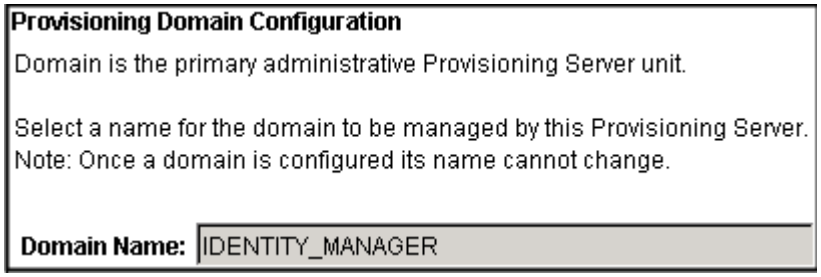
5. Select the appropriate Installation Type, depending on which components are installed on the system (Provisioning Server, C++Connector Server, or both).



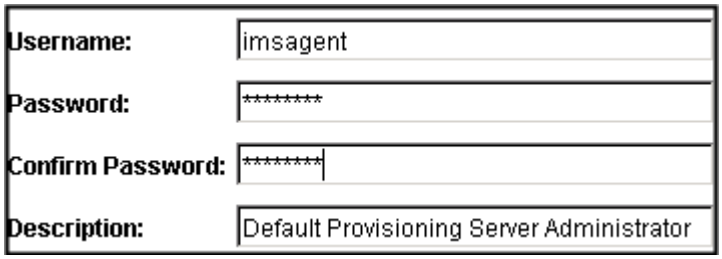
6. You can select a check box during upgrade to indicate Provisioning Directory high availability. If you select this option, supply the hostnames of any alternate Provisioning Directories and specify the primary Provisioning Directory.

7. Complete the Provisioning Domain screens.

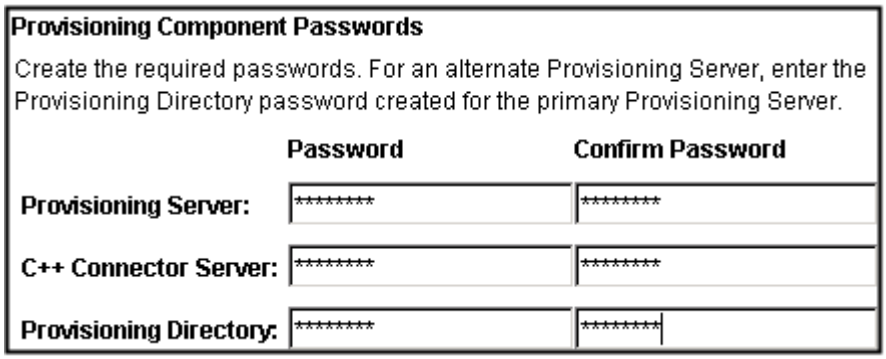
   Note: You may notice a slight delay when you click Next on the first Provisioning Domain screen.



8. Enter a password for the domain.



9. Supply provisioning components passwords.



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

    Your Provisioning Server is upgraded.

Upgrade 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.

Important! The Upgrade Wizard asks you to register the Java Connector Server so that updated metadata for existing and new connectors can be registered with the Provisioning Server.

Upgrade the Provisioning Manager

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

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

Configure a Remote Provisioning Manager

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

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

To configure a remote Provisioning Manager

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

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

Upgrade Other Provisioning Components

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

Connector Xpress

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

SPML Manager

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

SPML Service

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

Remote Agents

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

Password Sync Agents

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

GINA

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

Vista Credential Provider

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

Bulk Loader Client/PeopleSoft Feed

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

JCS SDK

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

CCI Standalone

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

Chapter 4: Upgrade on a Single WebSphere Node

This section contains the following topics:

Upgrade or Migrate a WebSphere Node

If you intend to upgrade the Identity Manager server and keep WebSphere at 6.1 or 7, you simply upgrade CA Identity Manager on the node (see page 39). However, if you have an earlier release of WebSphere, you need to migrate the Identity Manager server (see page 40) to WebSphere 7.

Upgrade the Identity Manager Server on a WebSphere Node

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

To upgrade the Identity Manager Server on a WebSphere 6.1 or 7 Node

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. Choose the Full Upgrade option.
4. Respond to the prompts that appear.

How to Migrate a Single Node Installation to WebSphere 7

Perform the following steps to migrate CA Identity Manager on a node to WebSphere 7:

✓	Step
	1. Uninstall the Identity Manager Server.
	2. Install the new version of the Identity Manager Server on WebSphere.
	3. Upgrade the workflow database (if upgrading from r12).
	4. Migrate task persistence data (if upgrading from r12).
	5. Configure workflow for your profile.
	6. Verify access to CA Identity Manager.

Uninstall the Identity Manager Server

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

To uninstall the Identity Manager Server on Windows

1. Stop the SiteMinder services, if you are using SiteMinder in your environment.

2. Go to Start, Control Panel, Add/Remove Programs and select CA Identity Manager.
3. Select CA Identity Manager.
4. Click Change/Remove.

   All non-provisioning components are uninstalled.

To uninstall CA Identity Manager components on UNIX

1. Navigate to the following location:

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

   ```
   sh uninstall.sh
   ```

   Follow the on-screen instructions.

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

Reinstall the Identity Manager Server on a WebSphere Node

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

1. Install WebSphere v7 and the required FixPacks and JDK.
2. Check that you have removed all unnecessary Websphere files (see page 18) or they may prevent the upgrade from succeeding.
3. Stop the following items:
   - WebSphere 7
   - Any previous installation of WebSphere
   - SiteMinder services if installed
4. Start the Identity Manager installation program.

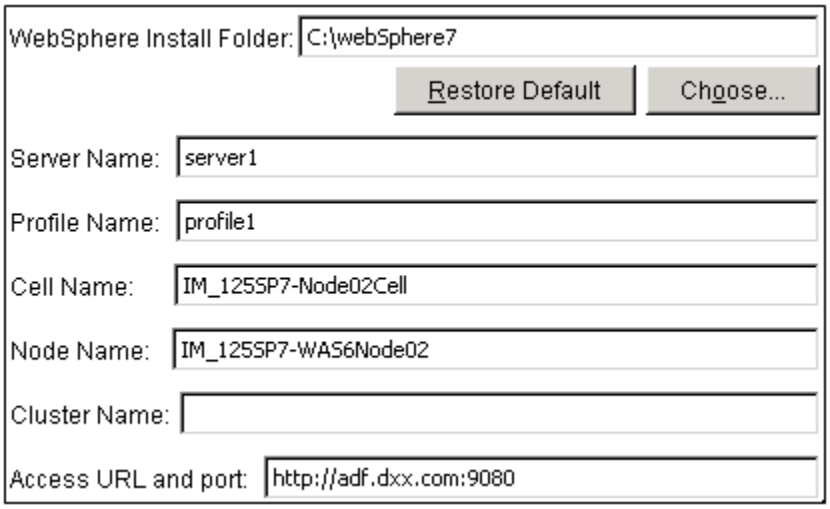
- Windows: From your installation media, run the following program:
  `ca-im-release-win32.exe`
- UNIX: From your installation media, run the installation program. For example, for Solaris:
  `ca-im-release-sol.bin`

release represents the current release of CA Identity Manager.

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

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

6. Supply the details for the websphere 7 that you created.



The WebSphere section includes these fields:

WebSphere Install Folder

The folder or directory where WebSphere is installed. You find this location in the Windows or UNIX file system.

Server Name

You find this name in the WebSphere console.

Profile Name

You find this name in the Windows or UNIX file system at the path:

was_home/profiles/*Deployment_Manager_Profile*/config/cells/

Cell Name

The deployment manager's cell which can be found in the WebSphere console.

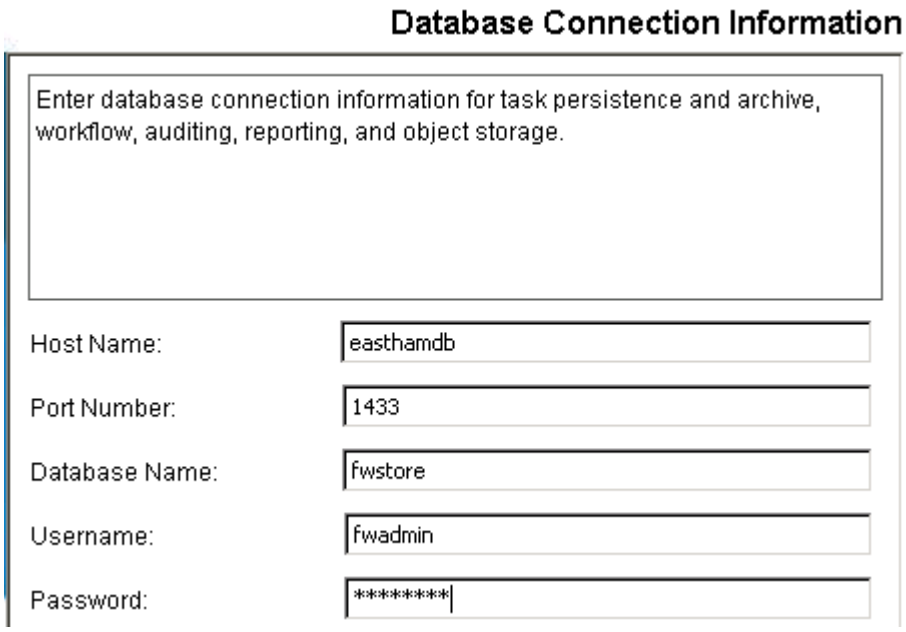
Node Name

A node that contains the Server Name you supplied on this screen. You find this name in the WebSphere console.

Access URL and port

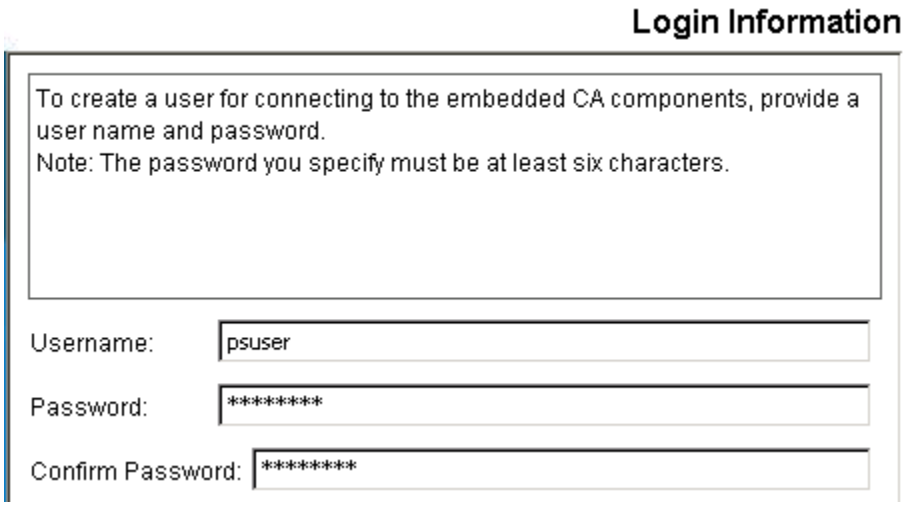
The fully-qualified system name and port number used by WebSphere.

7. For database credentials, provide the same values that existed at the previous installation.



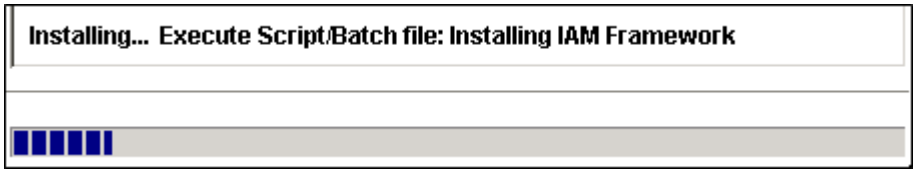
Important! If you are upgrading from CA Identity Manager r12 and you have different database stores for task persistence, workflow, audit, and reports, you will need to update the data sources manually after installation to point to the separate stores. .

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



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

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



10. When the installation completes, inspect the Install Complete message. If you see errors on the screen, note the path for the logs, which explain the errors.

If you are upgrading from CA Identity Manager r12, continue by upgrading the workflow database.

Upgrade the Workflow Database

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

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

To upgrade to WorkPoint 3.4.2

1. Locate the WorkPoint scripts in the Workpoint\database under the Administrative Tools folder. The scripts are in the following default locations:
   - **Windows:** C:\Program Files\CA\Identity Manager\IAM Suite\Identity Manager\tools\Workpoint\database
   - **UNIX:** /opt/CA/IdentityManager/IAM_Suite/Identity_Manager/tools/Workpoint/database
2. Run the wp331_to_wp34_cnv_step1.sql script to create the new tables for Workpoint 3.4 and to add the new columns to the end of old tables.

   This script also inserts rows into the WP_*_TYPE tables as needed.
3. Run the wp331_to_wp34_cnv_step2.sql script to create the stored procedures required to convert the data.
4. Run the wp331_to_wp34_cnv_step3.sql script to convert the text data to the new columns.

   This script also populates the new WP_BULK_DATA table from the old WP_BULK_STORAGE table.
5. Run the wp34_20060927_add.sql script to create the new tables for Workpoint 3.4.20060927.

   This script also inserts rows into the WP_INI and WP_*_TYPE tables as needed.
6. Run the wp34_20070625_add.sql script to create the new tables for Workpoint 3.4.2.20070625. This also inserts rows into the WP_INI and WP_*_TYPE tables as needed.
7. Run the wp342_20071218_add.sql script to create the new tables for Workpoint 3.4.2.20071218.

   This script also inserts rows into the WP_INI and WP_*_TYPE tables as needed.
8. Save all changes to the database.

Migrate Task Persistence Data

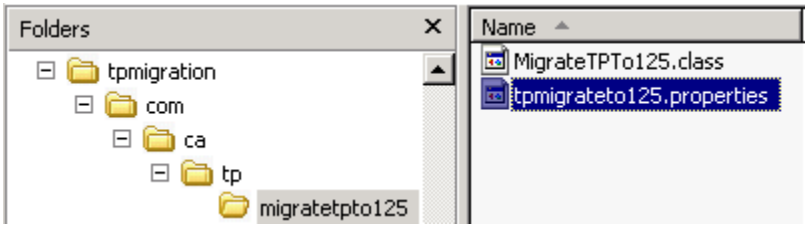
This procedure applies only if you are upgrading from CA Identity Manager r12.

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

To manually migrate task persistence data

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

   admin_tools/tpmigration/com/ca/tp/migratetpto125



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

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

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

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

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

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

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

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

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

Configure Workflow for Your Profile

If you have not used the default WebSphere profile for your installation, you configure workflow for the WebSphere Server.

To configure workflow for your WebSphere Profile

1. Start the WebSphere Console.
2. Navigate to Servers, Server Types, Application Servers, *server_name.*
3. Under Communications, Expand Ports.
4. Make note of the port used for the BOOTSTRAP_ADDRESS.

5. Edit Workpoint-client.properties file under iam_im.ear/config.

6. Locate the WebSphere section in this file.

   ```
   # java.naming.provider.url=iiop://localhost:2809
   ```

7. Replace 2809 with the profile's port that is used for the BOOTSTRAP_ADDRESS.
8. Restart this server.

Verify the Identity Manager Server Starts

To verify access to CA Identity Manager

1. Start CA Identity Manager as follows:
   - **Windows:**

     For WebSphere 6.1, click Navigate to Start, Programs, IBM WebSphere, Application Server 6.x, Profiles, Profile_Type, Start the Server

     For WebSphere 7, click Start, Programs, IBM WebSphere, Application Server Network Deployment V7.0, Profiles, Profile Name

Note: To view status information, use the First Steps console, which you access from the same location as the Start the Server command mentioned above. In the First Steps console, select Start the Server.

- **UNIX:**

  a. Navigate to *websphere_home*/profiles/*profile_name/*bin from the command line.

  b. Enter the following command:

  startserver *websphere_server*

  When you see a message that resembles the following, the server has completed its startup process:

  ```
  Server server1 is open for e-business
  ```

2. Access the Management Console and confirm the following:

   - You can access the following URL from a browser:

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

     For example:

     http://MyServer.MyCompany.com:*port-number/*iam/immanage

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

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

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

Chapter 5: Upgrade on a WebSphere Cluster

This section contains the following topics:

Upgrade or Migrate the Identity Manager Server

If you intend to upgrade the Identity Manager server on WebSphere 6.1 or 7, you can perform a simple upgrade. However, if you have an earlier release of WebSphere, you need to migrate the Identity Manager server on the cluster to WebSphere 7. See one of these topics:

- Upgrade a Cluster Installation (see page 51)
- How to Migrate a Cluster Installation to WebSphere 7 (see page 55)

Upgrade a WebSphere Cluster Installation

To upgrade a cluster while remaining on WebSphere 6.1 or 7, you perform three steps:

- Upgrade on the Deployment Manager System (see page 51)
- Configure Upgraded Cluster Members (see page 53)
- Update the plugin-cfg.xml File (see page 55)

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

Upgrade on the WebSphere Deployment Manager

Use this procedure if you are remaining on the same version of WebSphere and you are upgrading one of these installations:

- CA Identity Manager r12 or higher running on a WebSphere 6.1
- CA Identity Manager r12.5 SP7 or higher running on a WebSphere 7

To run the installer on the Deployment Manager system

1. Log in to the system with the Deployment Manager.
   - On Windows, use the Administrator account.
   - On UNIX, use the root account.
2. Start the Node Agents for the cluster members.
3. Stop the following items:
   - All cluster members
   - The WebSphere Deployment Manager
   - All SiteMinder services in your environment
4. Run the CA Identity Manager installer and select the Identity Manager Server.

   During an upgrade from r12, you have the choice to *uncheck* the automated upgrade steps for these tasks and perform them later using the Manual Upgrades appendix:

   - 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.

   We recommend leaving these options checked.

Configure Upgraded Cluster Members

After you have run the upgrade program, you configure the WebSphere cluster members.

To configure upgraded cluster members

1. Start the Deployment Manager.
2. Configure the messaging engine stores for each cluster member, as follows:
   a. In the Administrative Console, go to Service Integration, Buses, iam_im-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, truncate the database tables for each messaging store you reuse. For example, for a Microsoft SQL Server installation, you would enter:

      truncate table *IBMWSSIB*.SIB000;

      truncate table *IBMWSSIB*.SIB001;

      truncate table *IBMWSSIB*.SIB002;

      truncate table *IBMWSSIB*.SIBXACTS;

      truncate table *IBMWSSIB*.SIBKEYS;

      truncate table *IBMWSSIB*.SIBOWNER;

      truncate table *IBMWSSIB*.SIBOWNER;

      truncate table *IBMWSSIB*.SIBCLASSMAP;

      truncate table *IBMWSSIB*.SIBLISTING;

      For *IBMWSSIB*, enter the schema name of the cluster nodes in the previous installation.

   d. Set up cluster members again as follows:

      `wsadmin -f iam_im_imsSetupClusterMember.jacl` *`nodeN serverN cluster01`* `iam_im-`*`nodeN-serverN`*

   e. Note down the message store JNDI name for each message engine to make sure it exists. If any message store does not exist, create it.

      Rename the JNDI entries to this format:

      iam_im-*nodeN-serverN*

   f. Update your core group policies, so that the match criteria uses the new message engine names for each server policy you have defined.

      For example, change the IMSBus value in WSAF_SIB_MESSAGING_ENGINE to iam_im-IMSBus.

3. Restart the Node Agents on each cluster member. Wait a while for the deployment manager to update each node's installed applications. When you see castylesr5.1.1.ear and iam_im.ear appearing in the installedApps of each cluster member, proceed to the next step.

4. On each node, update the workpoint BOOTSTRAP_ADDRESS in workpoint-client.properties file.

   Edit Workpoint-client.properties file under iam_im.ear/config.

   Locate the WebSphere section in this file.

   ```
   # java.naming.provider.url=iiop://localhost:2809
   ```

   Replace 2809 with the profile's port that is used for the BOOTSTRAP_ADDRESS.

5. On UNIX, remove the .UTF8 suffix from the LANG and LC_ALL environment variables before you restart your cluster nodes. Otherwise, workpoint start up exceptions prevent the environments from starting.

6. 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 iam_im.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\wasserverCe
      ll01\iam_im.ear\user_console.war\WEB-INF\lib
      ```

   c. Repeat Steps a and b for each cluster member.

Update the plugin-cfg.xml File

You update the proxy plug-in so that WebSphere can communicate with the web server.

To update the plugin-cfg.xml file

1. Locate this line in the plugin-cfg.xml.
   ```
   <Uri AffinityCookie="JSESSIONID" AffinityURLIdentifier="jsessionid"
   Name="/idm/*"/>
   ```
2. Change idm to iam as follows:
   ```
   <Uri AffinityCookie="JSESSIONID" AffinityURLIdentifier="jsessionid"
   Name="/iam/*"/>
   ```
3. Locate this line in the file.
   ```
   <Uri AffinityCookie="JSESSIONID" AffinityURLIdentifier="jsessionid"
   Name="/idmmanage/*"/>
   ```
4. Change idmmanage to immanage as follows:
   ```
   <Uri AffinityCookie="JSESSIONID" AffinityURLIdentifier="jsessionid"
   Name="/immanage/*"/>
   ```

How to Migrate a Cluster Installation to WebSphere 7

Perform the following steps to migrate CA Identity Manager on a cluster to WebSphere 7:

✓	Step
	1. Uninstall the Identity Manager Server.
	2. Configure a WebSphere 7 cluster.
	3. Run the installation from the Deployment Manager.
	4. Add cluster members.
	5. Migrate Task Persistence data (if upgrading from r12).
	6. Update the workflow database (if upgrading from r12).
	7. Configure workflow for cluster members.
	8. Configure the proxy plug-in.

Uninstall the Identity Manager Server

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

To uninstall the Identity Manager Server on Windows

1. Stop the SiteMinder services, if you are using SiteMinder in your environment.
2. Go to Start, Control Panel, Add/Remove Programs and select CA Identity Manager.
3. Select CA Identity Manager.
4. Click Change/Remove.

   All non-provisioning components are uninstalled.

To uninstall CA Identity Manager components on UNIX

1. Navigate to the following location:

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

   ```
   sh uninstall.sh
   ```

   Follow the on-screen instructions.

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

Configure a WebSphere v7.0 Cluster for the Upgrade

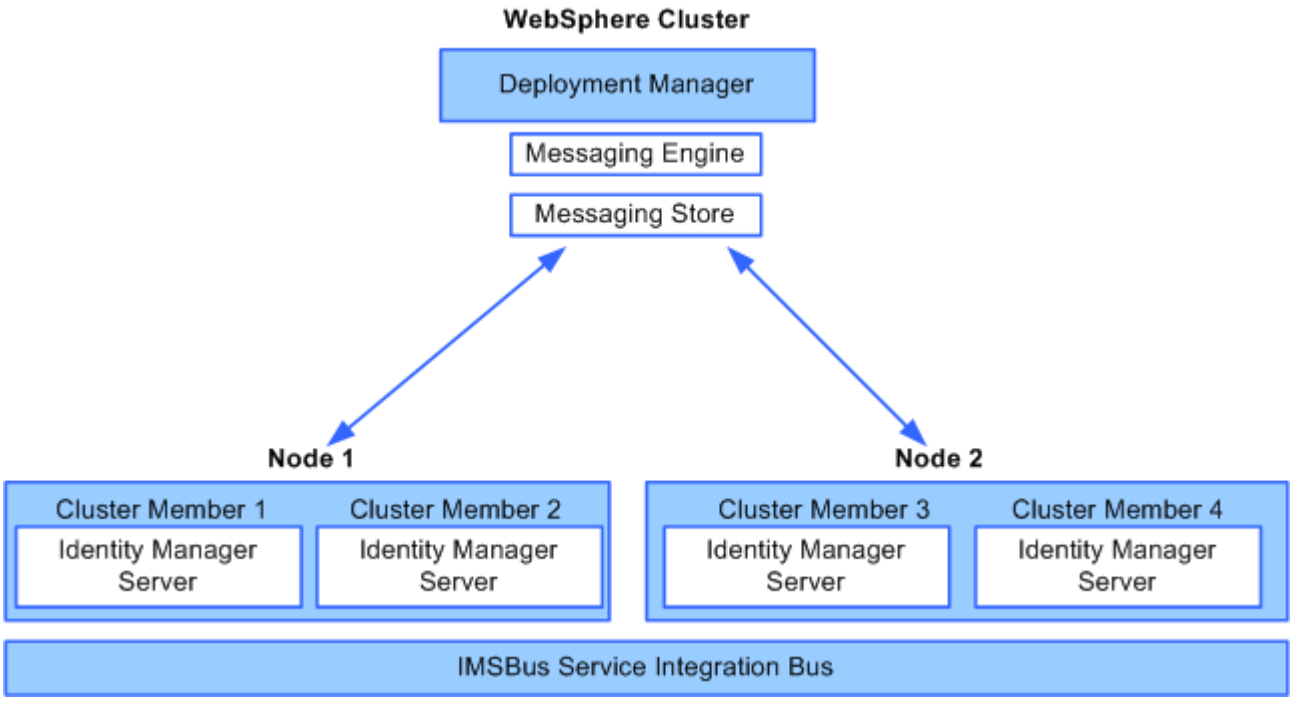
When you install software for a WebSphere cluster, you set up the following:

- One WebSphere Deployment Manager—Manages the other federated profiles in the cell through node agents.
- One or more nodes—Each node contains one or more cluster members (also called servers), which run the Identity Manager Server.
- Node agent—A process that manages communication between the Deployment Manager and the federated profile.
- Service Integration Bus—Groups resources in WebSphere to simplify administration. The WebSphere cluster is added as a member of the bus.

- Message Engine—Provides messaging functionality for members of the service integration bus. One message engine exists for the cluster.
- Message Store—Stores messages and transaction status for the message engine.
- A Web Server—Distributes the load to the appropriate server and, if SiteMinder is installed, protects access to the cluster members.

The following figure shows the relationship between the Deployment Manager, message engine, message store, nodes, and cluster members. The Identity Manager Server is installed from the Deployment Manager system to each cluster member.

Note: For more information about these components, see the WebSphere v7 System Management and Administration Redbook.



Install the Deployment Manager

You set up a WebSphere cluster in the WebSphere Administrator Console.

Note: CA Identity Manager does not support HTTP session persistence in a clustered environment.

To install WebSphere as the Deployment Manager

1. Decide which systems you plan to use for the cluster.
   a. Select a system for the WebSphere Deployment Manager. For best performance, the system should not be used as a node for cluster members.
   b. Determine the cluster member nodes.
2. Install the WebSphere Deployment Manager. Use both the installation instructions in the WebSphere v7 System Management and Administration Redbook and the following guidelines.

   During the installation, note the directory where you install the Deployment Manager.

   a. Install the IBM WebSphere Application Server Network Deployment software on the Deployment Manager system.

      When the installation completes, you are prompted to configure a *profile*, a WebSphere runtime environment.

   b. Run the Profile Creation Wizard to create the profile for the Deployment Manager system. When you are prompted to select a profile type, select the Deployment Manager profile.

   c. Start the Deployment Manager using one of the following methods:
      - Run the StartManager.bat (Windows)
      - StartManager.sh (Solaris) from a command prompt.

        The *websphere_home*/profiles/*profile_name/*bin folder contains the scripts.

If you registered the Deployment Manager as a Windows Service, use Windows Services to start the Deployment Manager.

Install WebSphere 7 on each Node

On each system that you have used for a cluster member, install WebSphere 7.

To install WebSphere on each Cluster Member system

1. Install the IBM WebSphere Application Server Network Deployment software on each cluster member.
2. Use the Profile Creation Wizard to create a default profile for each node.

   You use this profile to configure a connection to the Deployment Manager.
3. Start each node as follows:
   a. Navigate to *was_home*\WebSphere\AppServer\bin on the system where the managed node is located.
   b. Execute the startNode.bat\.sh command.
4. Confirm that a single cell has all the nodes associated with it at this location:
   was_home/profiles/*Deployment_Manager_Profile*/config/cells/*Cell_Name*/Nodes/

   You should see all federated nodes displayed as folder names.

Creation of profiles may sometimes fail if the bootstrap ports (default: 2809) are not unique. You can check for an error message in the pctLog.txt file in the created profiles' logs folder. For example:

```
(Oct 10, 2007 6:45:55 PM), Install,
com.ibm.ws.install.ni.ismp.actions.ISMPWSProfileLaunchAction, err, INSTCONFFAILED:
Cannot complete required configuration actions after the installation. The
configuration failed. The installation is not successful. Refer to C:\Program
Files\IBM\WebSphere\AppServer\logs\wasprofile\wasprofile_create_CustomIMFromNode.
log for more details.
```

Inspecting the wasprofile_create_CustomIMFromNode.log shows that this failure was due to Bootstrap ports that is not unique.

Create the Cluster with One Member

You now configure the cluster with a single member. The other cluster members are added in a subsequent procedure after you install CA Identity Manager.

To create the cluster with one member

1. In the Administrative Console, verify that the nodes show a Synchronized status.
2. Use the Create New Cluster wizard to create the cluster with one member.

   Note the cluster name and the server node name that you create in using this wizard. The server node is the cluster member node.
3. Stop the cluster member, but leave the Node Agents running.

Objects Created by the Installation

You install Identity Manager as described in the following procedure. During the installation, the following EARs are installed on the cluster domain:

- iam_im.ear
- ca-stylesr5.1.1.ear

When you supply a cluster name during the installation, these primary resources are configured:

- Distributed queues/topics targeted to the cluster
- Connection factories targeted to the cluster
- Data sources targeted to cluster
- iam_im-IMSBus, the Service Integration Bus for CA Identity Manager
- Message engine store for the cluster
- Core group policies used by the message engine

Run the Installation from the Deployment Manager

Once you have created the WebSphere cluster, you can install CA Identity Manager on it. Installer fields that require a hostname and port number should *not* use localhost.

Note: At previous releases of CA Identity Manager, creating a message store and message engine was a manual process. At this release, you create an empty message store database and supply that database name when you run the CA Identity Manager installer. WebSphere then populates the message store table, creates the message engine, and deploys the CA Identity Manager application ear and binaries to each node in the cluster.

To install CA Identity Manager on the Deployment Manager system

1. Perform these steps if you are using Microsoft SQL server:
   a. Open SQL Management Studio.
   b. Locate the user who owns the message store database.
   c. Set that user's default schema to dbo.
2. Log into the system with the Deployment Manager.
   - On Windows, log in as the Windows Administrator.
   - On UNIX, log in as root.
3. Stop the first cluster member, the only cluster member that you have configured so far.

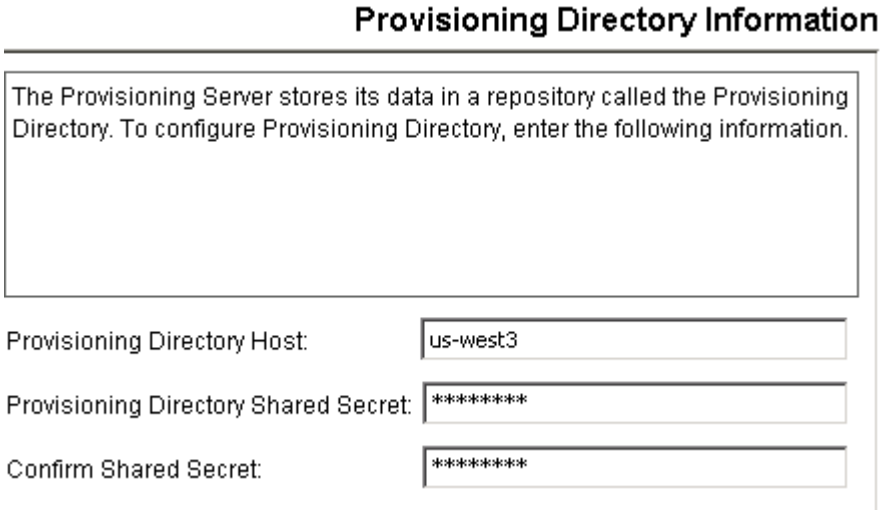
4. Start the Node Agent for that cluster member.
5. Stop the WebSphere Deployment Manager.
6. On the system that hosts the Deployment Manager, run the CA Identity Manager installation.
   - Windows: From your installation media, run the following program:
     `ca-im-release-win32.exe`
   - UNIX: From your installation media, run the installation program. For example, for Solaris:
     `ca-im-release-sol.bin`

   release represents the current release of CA Identity Manager.

   Important! Be sure that you have the collected the information needed by the installer, such as user names, host names, and ports.
7. Complete the Select Components section by including the Identity Manager Server and any other components that you need on this system.

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

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



9. Complete the other sections based on your requirements for the installation.

   The WebSphere section includes these fields:

   WebSphere Install Folder

   The folder or directory where WebSphere is installed. You find this location in the Windows or UNIX file system.

   Server Name

   The first cluster member in the WebSphere cluster. You find this name in the WebSphere console.

   Profile Name

   The deployment manager profile. You find this name in the Windows or UNIX file system at the path:

   was_home/profiles/*Deployment_Manager_Profile*/config/cells/

   Cell Name

   The deployment manager's cell which can be found in the WebSphere console.

   Node Name

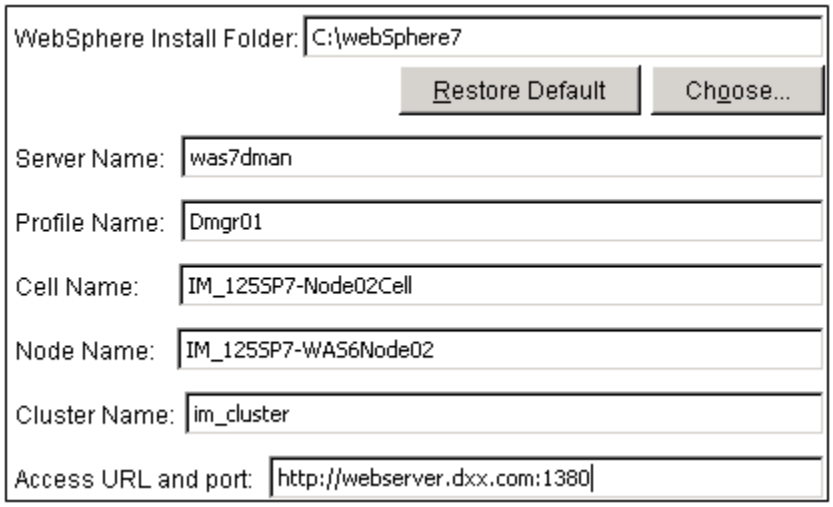
   A node that contains the Server Name you supplied on this screen. You find this name in the WebSphere console.

   Cluster Name

   The name of the cluster. You find this name in the WebSphere console.

Access URL and port

The URL and port number of the Web Server used for load balancing.



10. Complete the Message Store section. The installer creates a JDBC data source as the Message Engine message store based on the following information you provide:
    - Hostname
    - Port
    - Database name

      Enter the message store database.
    - Username

      Enter the user who owns the message store database.
    - Password
    - Schema name

      For Microsoft SQL Server, enter dbo.

      For Oracle, enter the user who owns the message store database.

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

Important! Do not start the cluster yet, as it will not function. Complete the remaining procedures, which conclude with the steps to start the cluster.

Add Cluster Members

You can now add members to the cluster using the first cluster member as a template.

To add cluster members

1. In the Administrative Console for the Deployment Manager, go to Servers, Clusters.
2. Add a cluster member, selecting one of the nodes for which you created a profile.
3. Copy sqljdbc.jar (for Microsoft SQL Server) or ojdbc14.jar (for Oracle) to the cluster member from the deployment manager system.

   On the deployment manager system, the JAR file is in the WAS_INSTALL_ROOT/lib directory. You copy it to the same folder on the system for this cluster member.
4. Repeat this procedure for each cluster member added to the cluster.

Upgrade the Workflow Database

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

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

To upgrade to WorkPoint 3.4.2

1. Locate the WorkPoint scripts in the Workpoint\database under the Administrative Tools folder. The scripts are in the following default locations:
   - **Windows:** C:\Program Files\CA\Identity Manager\IAM Suite\Identity Manager\tools\Workpoint\database
   - **UNIX:** /opt/CA/IdentityManager/IAM_Suite/Identity_Manager/tools/Workpoint/database
2. Run the wp331_to_wp34_cnv_step1.sql script to create the new tables for Workpoint 3.4 and to add the new columns to the end of old tables.

   This script also inserts rows into the WP_*_TYPE tables as needed.
3. Run the wp331_to_wp34_cnv_step2.sql script to create the stored procedures required to convert the data.
4. Run the wp331_to_wp34_cnv_step3.sql script to convert the text data to the new columns.

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

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

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

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

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

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

8. Save all changes to the database.

Migrate Task Persistence Data

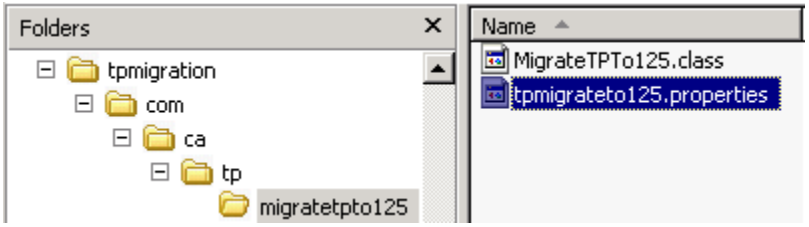
This procedure applies only if you are upgrading from CA Identity Manager r12.

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

To manually migrate task persistence data

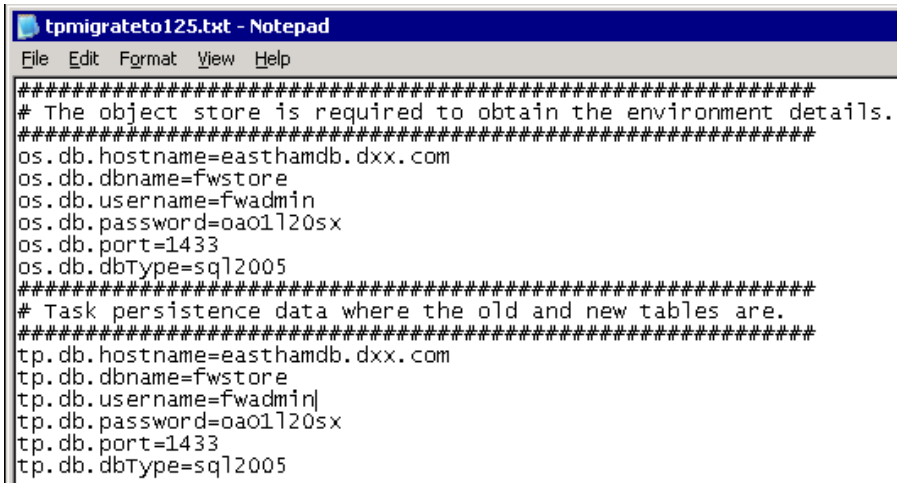
1. Find the tpmigration125.properties file in the following location:

   admin_tools/tpmigration/com/ca/tp/migratetpto125



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

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



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

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

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

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

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

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

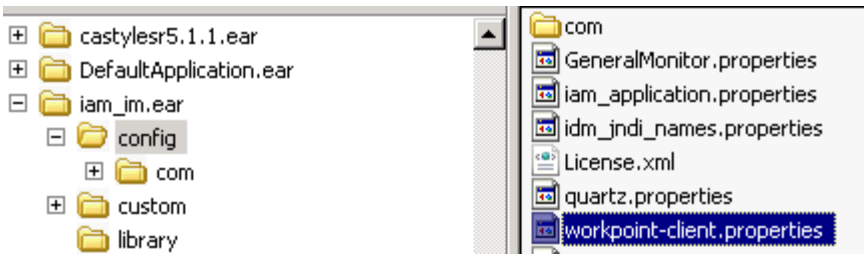
   The migration starts. After the migration completes, the status indicates how many tasks were migrated.
6. Be sure to verify that no errors appeared.
7. Repeat steps 4 and 5, but use the -pending option instead of All for task state.

Configure Workflow for Cluster Members

From the Deployment Manager system where you installed CA Identity Manager, you configure workflow for each cluster member.

To configure workflow for cluster members

1. Start the WebSphere Console.
2. Navigate to Servers, Server Types, Application Servers, *server_name.*
3. Under Communications, Expand Ports.
4. Make a note of the value for the BOOTSTRAP_ADDRESS port.
5. Edit the workpoint-client.properties file under iam_im.ear/config.



6. Locate the WebSphere section in this file.
7. Replace 2809 (the default port) with the profile's port that is used for the BOOTSTRAP_ADDRESS.
8. Repeat this procedure for each cluster member.
9. Restart the cluster members.

Configure the Proxy Plug-In for the Web Server

You install the proxy plug-in so that WebSphere can communicate with the web server.

To configure the proxy plug-in for the web server

1. See the WebSphere v7 System Management and Administration Redbook for instructions about installing the proxy plug-in for the web server. The chapter on Session Management discusses this plug-in.
2. Restart the Web server to activate the plug-in.
   - For IIS Web Servers—In the master WWW service, be sure that the WebSphere plug-in (sePlugin) appears after the SiteMinder Web Agent plug-in and that the WebSphere plug-in started successfully.
   - For Sun Java System Web Servers—Be sure that the WebSphere plug-in (libns41_http.so) is loaded after the SiteMinder Web Agent plug-in (NSAPIWebAgent.so)

     For Sun Java System 6.0 Web Servers, check the order of plug-ins in <*sun_java_home*>/https-*instance*/config/magnus.conf.

     For Sun Java System 5.x Web Servers, copy the following lines from <*iplanet_home*>/https-*instance*/config/magnus.conf to <*iplanet_home*>/https-*instance*/config/obj.conf

     ```
     Init fn="load-modules" funcs="as_init,as_handler,as_term"
     shlib="/export/WebSphere/AppServer/bin/libns41_http.so"
     Init fn="as_init"
     bootstrap.properties="/export/WebSphere/AppServer/config/cells/plugin-cfg
     .xml"
     ```

     Add the following after AuthTrans fn="SiteMinderAgent" in the obj.conf file:

     ```
     Service fn="as_handler"
     ```
   - For Apache Web Servers— In the Dynamic Shared Object (DSO) Support section of *Apache_home*/config/httpd.conf, be sure that the SiteMinder Web Agent plug-in (mod2_sm.so)is loaded before the WebSphere plug-in (mod_ibm_app_server_http.so).

Start the WebSphere Cluster

To start the WebSphere cluster, you start the Deployment Manager and then start each managed node.

To start the WebSphere cluster

1. Start a Policy Server that supports CA Identity Manager.

   Note: If you have a Policy Server cluster, only one Policy Server should be running while you create Identity Manager directories, create or modify Identity Manager environments, or change WorkPoint settings.

2. Run the Deployment Manager.

3. On the first managed node, complete the following steps:

   a. Navigate to *was_home*\WebSphere\AppServer\bin.

   b. Execute the startNode.bat\.sh command.

      The first managed node starts.

4. Repeat step 3 on each node in the cluster.

5. Start each cluster member in Servers, Clusters, *cluster_name*, Cluster Members in the WebSphere Administrative Console on the Deployment Manager.

6. Verify that the messaging engine for the cluster is running in Service integration, Buses, iam_im-IMSBus, Messaging Engines in the WebSphere Admin Console on the Deployment Manager.

7. If you have installed a SiteMinder Web Agent, start the Web Server where you installed the SiteMinder Web Agent and the application server proxy plug-in.

Verify the Clustered Installation

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

To verify the clustered installation

1. Start any extra Policy Servers and CA Identity Manager nodes that you stopped.

2. Access the Identity Manager Management Console as follows:

   ```
   http://host_name:port/iam/immanage
   ```

host_name

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

port

Defines the application server port.

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

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

Chapter 6: Report Server Upgrade

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

This section contains the following topics:

Upgrade the Report Server

Upgrade the Report Server to the supported version, CA Business Intelligence 3.2 (BusinessObjects Enterprise XI Release 3 SP3). Previous versions of this software are not supported.

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

To upgrade the Report Server

1. Exit all applications that are running.
2. Log in to the CA Support site.
3. Go to the Download Center.
4. Under Products, click CA Identity Manager and the current release.
5. Download the CA Business Intelligence Common Reporting package and unzip it.

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

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

   `export CASHCOMP=current-installation-location`

   For example:

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

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

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

To verify the upgrade of the Report Server

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

```
Version=BusinessObjects Enterprise XI Release 3 SP3
```

Copy the JDBC JAR Files

To copy the JDBC JAR files

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

3. Open the CRConfig.xml file, found in the following location:
   - Windows: CA\SC\CommonReporting3\common\4.0\java
   - UNIX: /opt/CA/SharedComponents/CommonReporting3/bobje/java
4. Add the location of the JDBC JAR files to the Classpath. For example:
   - Windows: <Classpath>report_server_home\common\4.0\java\lib\sqljdbc.jar; report_server_home\ common\4.0\java\lib\ojdbc14.jar …</Classpath>
   - UNIX: <Classpath>${BOBJEDIR}/java/lib/sqljdbc.jar:${BOBJEDIR}/java/lib/ojdbc14.jar: …</Classpath>
5. Save the file.
6. Restart the Report Server as follows:
   - For Windows, do the following:
     a. Go to Start, Program Files, BusinessObjects XI 3.1, BusinessObjects Enterprise, Central Configuration Manager.

        The Central Configuration Manager opens.

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

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

Deploy Default Reports

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

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

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

To deploy the default reports

1. Gather the following information about the Report Server:
   - Hostname
   - Administrator name

- Administrator password
- Snapshot database type

2. Copy all content from the Reports installer-root-directory/disk1/cabi/biconfig folder to the *im_admin_tools_dir*/ReportServerTools folder.
3. Set the JAVA_HOME variable to the 32-bit version of the JDK1.5 you installed.
4. Run one of the following commands:
   - For a Microsoft SQL Snapshot Database:

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

   - For an Oracle Snapshot Database:

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

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

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

BusinessObjects XI 3.x Post-Installation Step

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

Follow these steps:

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

   Input.*report_server_hostname*.InputFileRepository
5. Click Save.
6. Under the Server Name column, search for Output File Repository server and double-click the name.

7. In the Server Name text box, enter the following:

   Output.*report_server_hostname*.OutputFileRepository

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

Chapter 7: Post-Upgrade Configuration

This section contains the following topics:

Recompile Custom Code

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

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

The following custom code must be recompiled:

- 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 SP10 Java Connector Server is compatible with the CA Identity Manager r12 JCS SDK connector code.

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

- Custom C++ Connectors

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

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

To recompile custom connector code

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

   The installer detects the previous SDK version and updates it. Any files or folders, such as custom code placed in the Provisioning SDK admin folder, is preserved.
3. If the original custom code makefiles did not use eta.dep, update the makefiles as follows:
   a. Replace the exception handling flag from /GX to /EHsc.
   b. Remove /YX from the compiler command line option.
   c. Add the following to the compile flag:
      `/D "_CRT_SECURE_NO_WARNINGS" /D "_CRT_NON_CONFORMING_SWPRINTFS" /D "_USE_32BIT_TIME_T"`
   d. Set the correct versions in the makefile, as follows:
      - APPVER = 6.0
      - _WIN32_IE = 0x0700
   e. Add the following to the compile flag:
      `/D "_BIND_TO_CURRENT_VCLIBS_VERSION"`

      This tells the compiler to use VS.2008 SP1 libraries and dlls.
   f. Merge the built EXE and DLL files with the manifest file.
   g. Update the connector source and remove references to obsolete MFC functions.
4. Build the new connector for this release of CA Identity Manager. Refer to Microsoft's web site if there are compilation errors.
5. Deploy the connector normally.

Migrate Option Pack 1 Functionality

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

1. Replace certain Option Pack files to work with WebSphere.
2. Update the Option Pack folder path.
3. Import new role definitions.
4. Run the Option Pack Migration task.
5. Perform the manual steps for Option Pack migration.
6. Verify the Option Pack migration.

Replace Option Pack Files on WebSphere 6.1

If you upgraded the Identity Manager server on WebSphere 6.1, you need to replace some files.

To replace Option Pack files for WebSphere 6.1

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.

Replace Option Pack Files on WebSphere 7

If you migrated the Identity Manager server to WebSphere 7, you need to replace some files.

To replace Option Pack files for WebSphere 7

1. If you installed the Identity Manager server on a different system from the system with the Option Pack 1, copy the folder "c:\program files\ca\option pack" from the Option Pack system to c:\OP on the local system.
2. Start a command line prompt.
3. Change to the following directory:

   websphere_home\AppServer\profiles*profile_name*\installedApps*node_name*\iam_im.ear\user_console.war\WEB-INF\lib
4. Copy the following JAR files to the current directory:
   - OP\install\Lib\option-pack.jar
   - OP\install\Lib\spring*.jar
   - OP\install\Lib\commons-*.jar
   - OP\install\Lib\axis*.jar
   - OP\install\Lib\sun*.jar
   - OP\install\Lib\wsdl*.jar
   - OP\install\Lib\x*.jar
5. Restart WebSphere.

Update the Option Pack Folder Path

Update the path of the Option Pack folder for the Identity Manager Server to start successfully.

Update the Option Pack folder path

1. Create a data sourse with the name jdbc/IDFocus pointing to Option pack data base in application server console.
2. Update the JVM arguments in application server console.
   a. Open the WebSphere console.
   b. Click on WebSphere application servers under Server Types.
   c. Click on Server.
   d. Expand the Java and Process Management in 'Server Infrastructure.
   e. Click on Process definition.
   f. Click on Java Virtual Machine.
   g. Update Generic JVM arguments with the following:
   `-DidFocusHomeDir=C:\OP`

Import New Role Definitions

In the Management Console, import the new role definition files for the environment you want to upgrade.

To import the new role definition files

1. In the Management Console, click Environments.
2. Select the environment.
3. Go to Role and Task Settings.
4. Click Import.
5. Scroll up to see the role definition files listed under Category: Upgrade to SP.

   Multiple role definitions files are listed for import.

6. Select the Upgrade-OptionPack1-to-12.5SP-RoleDefinitions file.

   This file adds the Option Pack Migration task to the Option Pack tab in the User Console.

7. Select a second role definitions file, one of the four Upgrade-12-to-12.5SP-RoleDefinitions files.

   Select a file based on if you have a Provisioning Server and an organization in your user store.

8. Click Finish.

9. 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 82).

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 84) 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 SP10. For more information about creating account screens in CA Identity Manager r12.5 SP10, see the *Administration Guide*.

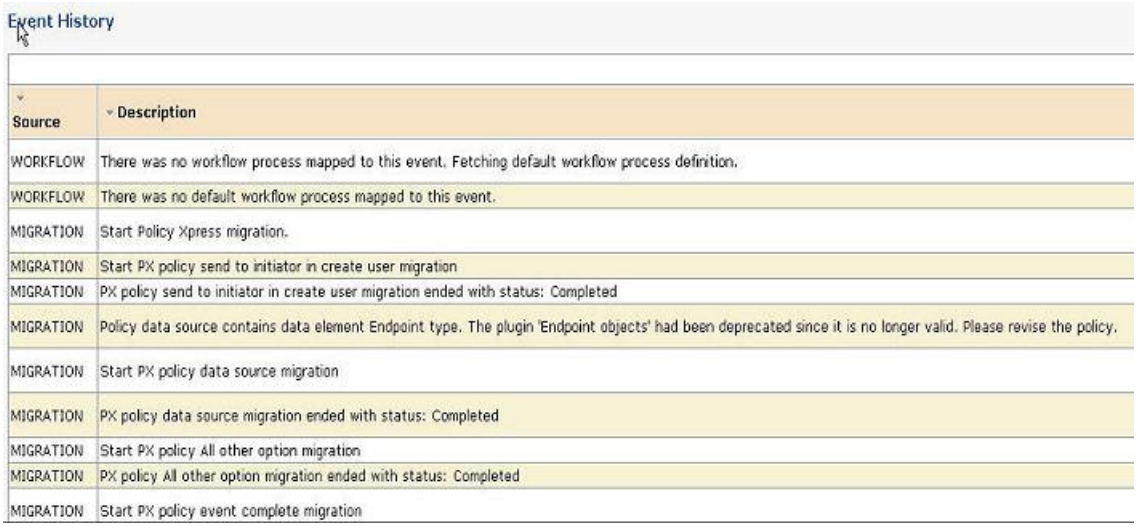
  Note: Any Policy Xpress policies with account management categories, such as User defined, Screen Builder Policies, and AD Account Management Screens, will not be migrated.
- SOD policies that existed in the Option Pack are no longer supported. For more information about SOD and preventative identity 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 SP10. 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

Perform the Manual 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 CA Identity Manager r12.5 SP10, 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 SP10. 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 94) 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 Features in this Release

Use the table below to access Option Pack 1 functionality in CA Identity Manager r12.5 SP10.

Functionality in Option Pack 1...	**Location in CA Identity Manager r12.5 SP10...**
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*.

Environment Changes

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

Upgrade r12 or r12.5 Environments with Access Roles

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

To upgrade environments with access roles

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

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

Update Role Definitions

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

Follow these steps:

1. In the Management Console, click Environments.
2. Select the environment.
3. Go to Role and Task Settings.
4. Click Import.
5. Scroll up to see role definition files under the heading, Category: Upgrade to SP.

6. Select a *single* role definitions file based on the following table:

Role Definitions File	Source for Upgrade	Provisioning Server	Organization in User Store
Upgrade-12-to-12.5SP-RoleDefinitions-NoOrganization.xml	r12	No	No
Upgrade-12-to-12.5SP-RoleDefinitions-Organization.xml	r12	No	Yes
Upgrade-12-to-12.5SP-RoleDefinitions-ProvisioningNoOrganization.xml	r12	Yes	No
Upgrade-12-to-12.5SP-RoleDefinitions-ProvisioningOrganization.xml	r12	Yes	Yes
Upgrade-12.5-to-12.5SP-RoleDefinitions-NoOrganization.xml	r12.5 or higher	No	No
Upgrade-12.5-to-12.5SP-RoleDefinitions-Organization.xml	r12.5 or higher	No	Yes
Upgrade-12.5-to-12.5SP-RoleDefinitions-ProvisioningNoOrganization.xml	r12.5 or higher	Yes	No
Upgrade-12.5-to-12.5SP-RoleDefinitions-ProvisioningOrganization.xml	r12.5 or higher	Yes	Yes

   For example, if the Identity Manager environment was created for r12.5 SP2, it uses a provisioning server, and the Identity Manager user store has a flat hierarchy (no organization), select the following file:

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

   Note: Other role definition files on this page apply for different procedures, such as adding Smart Provisioning.Those files are not part of the current procedure.

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

Update System Manager Role

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

Update Roles that Manage Provisioning Roles

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

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

Update Existing Account Screens

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

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

  Note: All dynamic connector account screens need to be recreated after the upgrade. For more information about generating new account screens for these connectors, see the section titled How you Generate CA Identity Manager User Console Account Screens in the *Connector Xpress Guide*.

To update existing account screens

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

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

Add New Account Screens

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

Follow these steps:

1. In the Management Console, click Environments.
2. Select the environment.
3. Click Role and Task Settings.
4. Click Import.
5. Scroll up to see the heading Category: EndpointType.

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

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

Add Delegation

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

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

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

Migrate Tasks to New Recurrence Model

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

To switch to the global recurrence model

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

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

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

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

g. Click Submit.

3. Remove existing recurrence tabs, as follows:

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

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

c. Select the Tabs tab.

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

e. Click Submit.

Update Auditing Settings

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

To update audit settings for an environment

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

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

5. Change this line to the following:

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

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

Upgrade Workflow from CA Identity Manager r12

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

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

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

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

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

The Administrative Tools are placed in the following default locations:

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

To enable workflow for the AccumulatedProvisioningRolesEvent

1. In the Management Console, select an environment.
2. Click Role and Task Settings.
3. Import the appropriate Upgrade-12-to-12.5SP-RoleDefinitions.xml file (either the Organization or NoOrganization version).

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

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

   Workflow now supports the AccumulatedProvisioningRolesEvent.

Update URI Mapping Files

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

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

Reapply r12 Workpoint Customizations

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

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

Add Sample Workflow Processes

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

1. In WorkPoint Designer, click Import.

   WorkPoint Designer location: *admin_tools*\Workpoint\bin
2. Navigate to *admin_tools*\workflowScripts and select 12.5to12.5SPUpgradeWFScripts.zip.

   This script imports the Escalation Process template.

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

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

Update r12 DYN Endpoint Attributes

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

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

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

Update Oracle Database with Garbage Collection Procedure

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

Upgrade SiteMinder

If you are using SiteMinder in your environment, you can upgrade SiteMinder components either before or after you upgrade 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 SP10.

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

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

Appendix A: Upgrade Verification

This section contains the following topics:

How to Verify the Upgrade

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

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

CA Directory and Provisioning Directory

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

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

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

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

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

Provisioning Server and Connector Server

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

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

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

Identity Manager Application

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

```
18:41:20,132 WARN  [default] ##############################################
18:41:20,132 WARN  [default] # CA Identity Manager 12.5.x.x.x
18:41:20,132 WARN  [default] ##############################################
18:41:20,132 WARN  [default] ---- CA IAM FW Startup Sequence Initiated. ----
18:41:20,132 WARN  [default] * Startup Step 1 : Attempting to start ServiceLocator.
18:41:20,632 WARN  [default] * Startup Step 2 : Attempting to start
PolicyServerService
18:41:20,835 WARN  [default] * Startup Step 3 : Attempting to start
ServerCommandService
18:41:21,148 WARN  [default] * Startup Step 4 : Attempting to start
EnvironmentService
18:41:21,163 WARN  [default] * Startup Step 5 : Attempting to start
CacheManagerService
18:41:21,179 WARN  [default] * Startup Step 6 : Attempting to load global plugins.
18:41:30,694 WARN  [default] * Startup Step 7 : Attempting to start
AdaptersConfigService
18:41:30,710 WARN  [default] * Startup Step 8 : Attempting to start
EmailProviderService
18:41:30,741 WARN  [default] * Startup Step 9 : Attempting to start
AuditProviderService
18:41:30,788 WARN  [default] * Startup Step 10 : Attempting to start
RuntimeStatusDetailService
.
.
.
18:41:31,038 WARN  [default] * Startup Step 23 : Attempting to start
GlobalInitializer plug-ins
18:41:31,038 WARN  [default] * Startup Step 24 : Attempting to start environments
18:42:15,960 WARN  [EnvironmentService] * Starting environment: XXXX
18:42:18,116 WARN  [default] * Startup Step 25 : Attempting to start SchedulerService
18:42:18,163 WARN  [default] * Startup Step 26 : Attempting to recover events and
runtime status details
18:42:18,257 WARN  [default] ---- CA IAM FW Startup Sequence Complete. ----
```

Runtime Database Schema Upgrades

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

- Workflow
- Task Persistence
- Archive

- Audit
- Snapshot

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

```
17:08:22,796 WARN  [default] ##############################################
17:08:22,796 WARN  [default] # CA Identity Manager 12.5.x.x.xxx
17:08:22,796 WARN  [default] ##############################################
17:08:22,953 WARN  [CreateDatabaseSchema] ****** Schema for: Task Persistence is up
to date.
17:08:23,015 WARN  [CreateDatabaseSchema] ****** Begin to create Archive database
schema.
17:08:23,218 WARN  [CreateDatabaseSchema] Archive database schema is created
successfully.
17:08:23,234 WARN  [CreateDatabaseSchema] ****** Begin to create Auditing database
schema.
17:08:23,593 WARN  [CreateDatabaseSchema] Auditing database schema is created
successfully.
17:08:23,625 WARN  [CreateDatabaseSchema] ****** Upgrading Schema for: Snapshot from
r12 to r12.5 SP2
17:08:23,891 WARN  [CreateDatabaseSchema] Snapshot database schema is created
successfully.
```

Pending Tasks

Verify that the previous CA Identity Manager version's pending tasks were migrated to CA Identity Manager r12.5 SP10, by doing the following:

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

Adapters

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

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

SiteMinder Integration

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

- Communication with the SiteMinder Policy Server

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

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

- SiteMinder Authentication

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

- Password Management

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

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

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

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

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

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

Report Server

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

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

      If they are not started, start them.

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

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

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

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

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

This section contains the following topics:

UNIX and Console Mode Installation

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

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

release represents the current release of CA Identity Manager

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

- For the main installation, add -i console. For example:
  `./ca-im-12.5-sp*N*-sol.bin -i console`
- For installation of provisioning components, add -console to the setup command.

Red Hat Linux 64-bit Installation

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

Follow these steps:

1. Create a symbolic link to work around a CryptoJ failure. Use the following command:
   ```
   ln –s /dev/urandom /dev/random
   ```
2. Install four 32-bit packages using the following commands:

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

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

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

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

Alternatively, the package dependency may be resolved using Add/Remove Software. Using this approach, you select and install the required i686 architecture dependencies required ksh package.

Non-Provisioning Installation

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

- For Windows, use IMWithoutProvisioning\ca-im-web-*release*-win32.bat
- For Solaris, use IMWithoutProvisioning/ca-im-web-*release*-sol.sh

release represents the current release of CA Identity Manager.

Appendix C: Unattended Upgrades

This section contains the following topics:

How to Perform Unattended Upgrades

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.

Provisioning Components Unattended Upgrade

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

-options-template *response_file_name*

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

-options-record *response_file_name*

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

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

Provisioning Directory

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

Provisioning Server

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

Provisioning Manager

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

Appendix D: Manual Upgrades

This section contains the following topics:

How to Manually Upgrade to CA Identity Manager r12.5 SP10

If you want to upgrade to CA Identity Manager r12.5 SP10 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 SP10

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

Manually Upgrade the Provisioning Directory

CA Directory no longer uses Ingres as a data store. Starting at CA Directory r12 SP1, a new memory-mapped file technology named DXgrid is used. For Provisioning to work with CA Identity Manager r12.5 SP10, upgrade the Provisioning Directory schema and CA Directory.

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

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

To manually upgrade the Provisioning Directory

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

9. Run the upgrade.bat file.

   The Provisioning Directory upgrade wizard starts.

   Note the following:

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

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

    The Provisioning Directory and CA Directory are upgraded.

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

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

Manually Upgrade the Provisioning Server

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

To manually upgrade the Provisioning Server

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

   Your Provisioning Server is upgraded.

Manually Upgrade the Java Connector Server

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

To manually upgrade the Java Connector Server

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

   Your Java Connector Server is upgraded.

Manually Upgrade the Provisioning Manager

Perform the following process to manually upgrade the Provisioning Manager.

To manually upgrade the Provisioning Manager

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

   Your Provisioning Manager is upgraded.

Manually Upgrade the Identity Manager Server

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

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

Upgrade the Workflow Database

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

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

To upgrade to WorkPoint 3.4.2

1. Locate the WorkPoint scripts in the Workpoint\database under the Administrative Tools folder. The scripts are in the following default locations:
   - **Windows:** C:\Program Files\CA\Identity Manager\IAM Suite\Identity Manager\tools\Workpoint\database
   - **UNIX:** /opt/CA/IdentityManager/IAM_Suite/Identity_Manager/tools/Workpoint/database
2. Run the wp331_to_wp34_cnv_step1.sql script to create the new tables for Workpoint 3.4 and to add the new columns to the end of old tables.

   This script also inserts rows into the WP_*_TYPE tables as needed.
3. Run the wp331_to_wp34_cnv_step2.sql script to create the stored procedures required to convert the data.
4. Run the wp331_to_wp34_cnv_step3.sql script to convert the text data to the new columns.

   This script also populates the new WP_BULK_DATA table from the old WP_BULK_STORAGE table.
5. Run the wp34_20060927_add.sql script to create the new tables for Workpoint 3.4.20060927.

   This script also inserts rows into the WP_INI and WP_*_TYPE tables as needed.
6. Run the wp34_20070625_add.sql script to create the new tables for Workpoint 3.4.2.20070625. This also inserts rows into the WP_INI and WP_*_TYPE tables as needed.
7. Run the wp342_20071218_add.sql script to create the new tables for Workpoint 3.4.2.20071218.

   This script also inserts rows into the WP_INI and WP_*_TYPE tables as needed.
8. Save all changes to the database.

Migrate Task Persistence Data

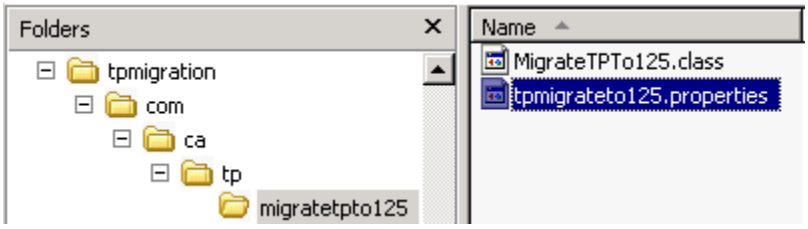
This procedure applies only if you are upgrading from CA Identity Manager r12.

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

To manually migrate task persistence data

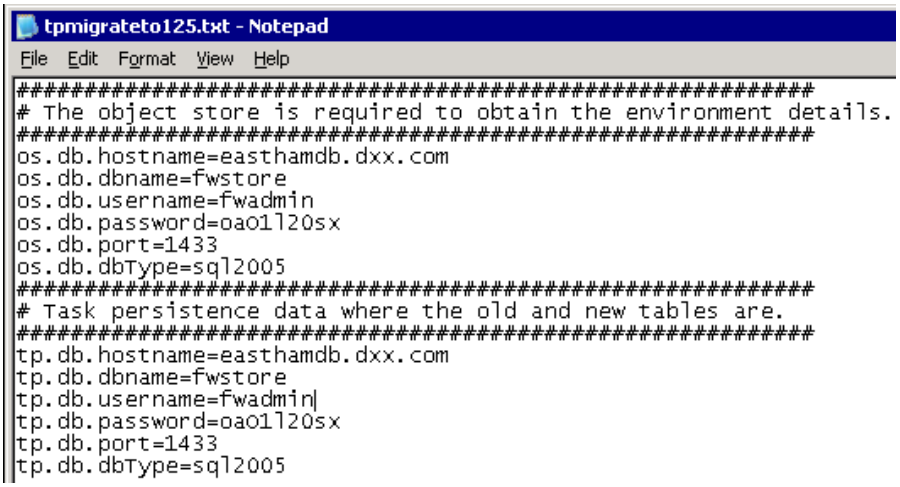
1. Find the tpmigration125.properties file in the following location:

   admin_tools/tpmigration/com/ca/tp/migratetpto125



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

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



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

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

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

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

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

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

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

Appendix E: Log Files for the Upgrade

This section contains the following topics:

Log Files on Windows

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

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

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

- C:\Program Files\CA\Identity Manager\install_config_info (32-bit system)
- C:\Program Files (x86)\CA\Identity Manager\install_config_info (64-bit system)

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

Example:

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

Log files on UNIX

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

/opt/CA/IdentityManager/

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

/opt/CA/IdentityManager/install_config_info

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

Index

N

O

P

R

S

U

V

W