

# CA Identity Manager

## Upgrade Guide

r12.5



This documentation and any related computer software help programs (hereinafter referred to as the "Documentation") are for your informational purposes only and are subject to change or withdrawal by CA at any time.

This Documentation may not be copied, transferred, reproduced, disclosed, modified or duplicated, in whole or in part, without the prior written consent of CA. This Documentation is confidential and proprietary information of CA and may not be used or disclosed by you except as may be permitted in a separate confidentiality agreement between you and CA.

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

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

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

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

The manufacturer of this Documentation is CA.

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

Copyright © 2009 CA. All rights reserved. All trademarks, trade names, service marks, and logos referenced herein belong to their respective companies.

## CA Product References

This document references the following CA products:

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

## Contact CA

### Contact Technical Support

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

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

### Provide Feedback

If you have comments or questions about CA product documentation, you can send a message to [techpubs@ca.com](mailto:techpubs@ca.com).

If you would like to provide feedback about CA product documentation, complete our short [customer survey](#), which is also available on the CA Support website, found at <http://ca.com/docs>.



# Contents

---

<b>Chapter 1: Upgrade Overview</b>	<b>9</b>
Supported Upgrade Paths .....	9
Upgrade Process .....	9
Architecture Changes .....	10
<b>Chapter 2: Upgrade Prerequisites</b>	<b>11</b>
How to Meet Prerequisites for the Upgrade .....	11
Install the CA Identity Manager Bookshelf .....	11
Check Hardware Requirements .....	12
Check Software Requirements .....	14
Check for Cumulative Releases .....	14
Upgrade to a Supported Application Server .....	15
Configure WebSphere for the Upgrade .....	16
SSL Configuration .....	17
Back Up Custom Code .....	17
<b>Chapter 3: CA Identity Manager Upgrade</b>	<b>19</b>
How to Upgrade CA Identity Manager .....	19
Collect Information Required for the Upgrade .....	20
Provisioning Directory Information .....	20
Provisioning Server Information .....	21
Java Connector Server Information .....	22
Identity Manager Server Information .....	23
SiteMinder Information .....	24
Run the Upgrade Wizard .....	25
Upgrade the Provisioning Directory .....	25
Upgrade the Provisioning Server .....	28
Upgrade the Java Connector Server .....	29
Upgrade the Provisioning Manager .....	29
Upgrade the Identity Manager Server .....	30
Upgrade Other Provisioning Components .....	33
Recompile Custom Code .....	35
Upgrade Reporting .....	37
Upgrade the Report Server .....	37
Update the Default Reports .....	38
Upgrade SiteMinder .....	39

---

## **Chapter 4: Configuration After Upgrade from CA Identity Manager r8.1 SP2 41**

How to Perform Post-Upgrade Configuration .....	41
(WebSphere only) Enable XA Transactions .....	41
(RDB Only) Modify the User Store .....	42
(RDB Only) Recreate Directories and Environments .....	42
Upgrade Custom Workflow Scripts .....	42
Update the Proxy Forwarder .....	43
Upgrade TEWS .....	43
Specify an Inbound Administrator .....	44

## **Chapter 5: New Feature Configuration 47**

Add New Roles and Tasks .....	47
Add New Account Screens .....	48
Add Sample Workflow Processes .....	48
Add Workflow Support for AccumulatedProvisioningRolesEvent .....	49
Add Delegation .....	50
Configure IPv6 Support .....	50

## **Appendix A: Manual Upgrades 51**

How to Manually Upgrade to CA Identity Manager r12.5 .....	51
Manually Upgrade the Provisioning Directory .....	52
Manually Upgrade the Provisioning Server .....	53
Manually Upgrade the Java Connector Server .....	54
Manually Upgrade the Provisioning Manager .....	54
Manually Upgrade the Identity Manager Server .....	55
Manually Upgrade the Workflow Database .....	55
Manually Migrate Task Persistence Data .....	57
Manually Export the Directories and Environments .....	58
Manually Recreate the Identity Manager Directory .....	59
Manually Recreate the Environment .....	62
Manually Deploy CA Identity Manager on WebSphere .....	63

## **Appendix B: Unattended Upgrades 65**

How to Perform Unattended Upgrades .....	65
Identity Manager Server Unattended Upgrade .....	65
Provisioning Components Unattended Upgrade .....	66

## **Appendix C: Successful Upgrade Verification 67**

How to Verify the Upgrade .....	67
CA Directory and Provisioning Directory .....	68

---

Provisioning Server and Connector Server .....	68
Identity Manager Application .....	69
Runtime Database Schema Upgrades .....	69
Object Store .....	70
Pending Tasks .....	70
Adapters .....	71
SiteMinder Integration .....	71
Report Server .....	72

<b>Index</b>	<b>73</b>
--------------	-----------



# Chapter 1: Upgrade Overview

---

This section contains the following topics:

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

[Upgrade Process](#) (see page 9)

[Architecture Changes](#) (see page 10)

## Supported Upgrade Paths

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

- eTrust Admin r8.1 SP2
- CA Identity Manager r8.1 SP2
- CA Identity Manager r12

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

## Upgrade Process

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

<b>If you currently have...</b>	<b>Perform these upgrade steps...</b>
eTrust Admin r8.1 SP2	<ol style="list-style-type: none"><li>1. Verify upgrade prerequisites.</li><li>2. Upgrade the Provisioning Server components.</li><li>3. Perform a <i>new</i> installation of the Identity Manager Server using the CA Identity Manager installer.</li><li>4. Perform additional new feature configuration, as needed.</li></ol>
CA Identity Manager r8.1 SP2	<ol style="list-style-type: none"><li>1. Verify upgrade prerequisites.</li><li>2. Upgrade the Provisioning Server components and the Identity Manager Server.</li><li>3. Apply post-upgrade configuration changes.</li><li>4. Perform additional new feature configuration, as needed.</li></ol>

<b>If you currently have...</b>	<b>Perform these upgrade steps...</b>
CA Identity Manager r12	<ol style="list-style-type: none"><li>1. Verify upgrade prerequisites.</li><li>2. Upgrade the Provisioning Server components and the Identity Manager Server.</li><li>3. Perform additional new feature configuration, as needed.</li></ol>

## Architecture Changes

In r12.5, CA Identity Manager includes a router DSA and a notification DSA:

- In r12.5, the Provisioning Server goes through a router DSA to communicate with the Provisioning Directory. In previous releases of CA Identity Manager, connections to the Provisioning Directory came directly from the Provisioning Server and were authenticated with an LDAP bind username and password.

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

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

- In r12.5, a notification DSA named `impd-notify` is added during the upgrade. If you are upgrading from r12.0, the `etaops-notify` DSA is replaced with `impd-notify` during the upgrade. Also, the `etrustadmin` DSA is replaced with `impd-main/co/inc` and the `etadmintemp` DSA is removed.

# Chapter 2: Upgrade Prerequisites

---

This section contains the following topics:

[How to Meet Prerequisites for the Upgrade](#) (see page 11)

[Install the CA Identity Manager Bookshelf](#) (see page 11)

[Check Hardware Requirements](#) (see page 12)

[Check Software Requirements](#) (see page 14)

[Check for Cumulative Releases](#) (see page 14)

[Upgrade to a Supported Application Server](#) (see page 15)

[Back Up Custom Code](#) (see page 17)

## How to Meet Prerequisites for the Upgrade

Perform the following steps to meet all prerequisites before upgrading to CA Identity Manager 12.5:

Step
1. Install the CA Identity Manager Bookshelf.
2. Check hardware and software requirements.
3. Check if a cumulative release exists.
4. Upgrade to a supported application server.
5. Back up custom code.

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

## Install the CA Identity Manager Bookshelf

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

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

### To use the Bookshelf

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

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

## Check Hardware Requirements

The following *minimum* hardware is required for each system that will host the Identity Manager Server:

- CPU: Intel (or compatible) 1.5 GHz (Windows or Linux), SPARC 1.0 GHz (Solaris) or POWER4 1.1 GHz (AIX)
- Memory: 2 GB
- Available Disk Space: 2 GB

**Note:** These hardware requirements take into account the requirements of the application server that must be installed on the system where you install the Identity Manager Server.

We *recommend* the following hardware for each system that will host the Identity Manager Server:

- CPU: Dual core Intel (or compatible) 2.5 GHz (Windows or Linux), Dual core SPARC 1.5 GHz (Solaris) or POWER5 1.5 GHz (AIX)
- Memory: 4 GB
- Available Disk Space: 2 GB

The following *minimum* hardware is required for each system that will host the Provisioning Server or standalone Connector Servers:

- CPU: Intel (or compatible) 1.5 GHz (Windows) or SPARC 1.0 GHz (Solaris)
- Memory: 2 GB
- Available Disk Space: 2 GB

We *recommend* the following hardware for each system that will host the Provisioning Server or standalone Connector Servers:

- CPU: Dual core Intel (or compatible) 2.5 GHz (Windows) or Dual core SPARC 1.5 GHz (Solaris)
- Memory: 4 GB
- Available Disk Space: 2 GB

The following *minimum* hardware is required for each system that hosts the Provisioning Directory:

- CPU: Intel (or compatible) 1.5 GHz (Windows) or SPARC 1.0 GHz (Solaris)
- Memory: 2 GB
- Available Disk Space: 2 GB to 10 GB, depending on the number of users and accounts
- 64 bit processor and operating system for intermediate and large deployments

We *recommend* the following hardware for each system that hosts the Provisioning Directory:

- CPU: Dual core Intel (or compatible) 2.5 GHz (Windows) or Dual core SPARC 1.5 GHz (Solaris)
- Memory: 4 GB
- Available Disk Space: 2 GB to 10 GB, depending on the number of users and accounts
- 64 bit processor and operating system

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

- CPU: Dual core Intel (or compatible) 2.0 GHz (Windows) or Dual core SPARC 1.5 GHz (Solaris)
- Memory: 4 GB

- Available Disk Space: 6 GB to 14 GB, depending on the number of users and accounts
- 64 bit processor and operating system for intermediate and large deployments

## Check Software Requirements

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

**Note:** For a complete list of supported platforms and versions, see the CA Identity Manager support matrix on the [CA Identity Manager support site](#).

Check the following software components for required versions:

- Java Development Kit (JDK) or Java Runtime Environment (JRE)
- Relational Database (MS SQL or Oracle)
- [Application Server](#) (see page 15)

## Check for Cumulative Releases

Check for the latest CA Identity Manager Cumulative Release (CR) at the CA Identity Manager support site. If you find a CR release for CA Identity Manager, use the installer in the CA Identity Manager CR to install or to upgrade an existing installation with the latest fixes and enhancements.

### To check for CA Identity Manager Cumulative Releases

1. In a web browser, go to the CA Identity Manager support site.
2. Login with your username and password.
3. Under Support by Product, select CA Identity Manager.
4. If a Cumulative Release (CR) exists, download it.
5. Use the instructions in this chapter to install the CA Identity Manager components on one system or several systems.

## Upgrade to a Supported Application Server

Be sure that you install an application server version that is supported by CA Identity Manager r12.5.

**Note:** For more information about supported application servers, see the CA Identity Manager Support Matrix on the [CA support site](#).

**Important!** Some version upgrades of JBoss, WebSphere, and WebLogic require a new installation, not an upgrade, of the Identity Manager Server. In these cases, you will need to uninstall the Identity Manager Server, upgrade your application server, then perform a *fresh* install of the Identity Manager Server.

Consult the following table to see if the previous upgrade restriction applies to your environment:

<b>If upgrading from this application server version...</b>	<b>To this application server version</b>	<b>Perform a new installation of the Identity Manager Server?</b>
JBoss 3.3.2	JBoss 4.2.3	No
JBoss 4.0.5	JBoss 4.2.3	Yes
WebLogic 8.1	WebLogic 9.2	Yes
WebLogic 8.1	WebLogic 10.3	Yes
WebSphere 5.1.1.x	WebSphere 6.1.0.17	Yes
WebSphere 6.0.2.17	WebSphere 6.1.0.17	Yes
WebSphere 6.1.0.15	WebSphere 6.1.0.17	No

To upgrade your application server and install a new version of the Identity Manager Server, perform the following process:

1. Back up all custom code.
2. Export your environments.

**Note:** For more information about exporting an Identity Manager environment, see the Configuration Guide.

3. Uninstall the Identity Manager Server.
4. Upgrade your application server to a supported version.

5. Perform a new install of the Identity Manager Server.

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

**Note:** If you are migrating from CA Identity Manager r8.1 SP2 or r12 and you have a different database store for task persistence, workflow, audit, and reports, update the different datasources to point to existing stores after the installation.

6. Reapply all custom code.

For all other application server upgrades, perform a normal upgrade of CA Identity Manager r12.5 as described in this guide.

## Configure WebSphere for the Upgrade

An upgrade to CA Identity Manager r12.5 on WebSphere may fail due to disk space errors or timeout errors. Perform the following steps to ensure that your upgrade to CA Identity Manager r12.5 succeeds on WebSphere.

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

**Note:** For more information, see your WebSphere documentation.

## SSL Configuration

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

## Back Up Custom Code

Before you upgrade to CA Identity Manager r12.5, be sure to back up your custom code, including the following:

- C++ custom connectors
- Provisioning manager plug-ins for Java custom connectors
- Common program exits
- Universal Provisioning Option (UPO) program exits
- Pluggable Authentication Module (PAM) DLLs
- Identity Manager Server custom code, such as Business Logic Task Handler (BLTH) class files, Logical Attribute Handler (LAH) class files, and Event Listener class files.
- Customized skin folder at this location:  
    `..\IdentityMinder.ear\user_console.war\app\imcss\`
- Customized help, back up the help property file at this location:  
    `..\IdentityMinder.ear\config\com\netegrity\config\`

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

After upgrading you need to update the new `index.jsp`. See the *User Console Design Guide*. You will also recompile all custom code using Microsoft Visual Studio 2008 SP1.



# Chapter 3: CA Identity Manager Upgrade

---

This section contains the following topics:

- [How to Upgrade CA Identity Manager](#) (see page 19)
- [Collect Information Required for the Upgrade](#) (see page 20)
- [Run the Upgrade Wizard](#) (see page 25)
- [Upgrade Other Provisioning Components](#) (see page 33)
- [Recompile Custom Code](#) (see page 35)
- [Upgrade Reporting](#) (see page 37)
- [Upgrade SiteMinder](#) (see page 39)

## How to Upgrade CA Identity Manager

Perform the following steps to upgrade to CA Identity Manager 12.5:

Step
1. Be sure your systems meet all upgrade prerequisites.
2. Collect information required for the upgrade.
3. Run the Upgrade Wizard, which upgrades the following components: <ul style="list-style-type: none"><li>■ Provisioning Directory (including CA Directory)</li><li>■ Provisioning Server (includes the C++ Connector Server)</li><li>■ Java Connector Server</li><li>■ Provisioning Manager</li><li>■ Identity Manager Server</li></ul>
4. Upgrade other provisioning components.
5. Recompile custom code.
6. Upgrade the Report Server.
7. (Optional) Upgrade SiteMinder.

**Note:** The Upgrade Wizard automatically detects previous versions of CA Identity Manager, prompts you through the upgrade process in the correct sequence, and launches all component installers from one location. To launch the Upgrade Wizard, run the CA Identity Manager installer from the CA Identity Manager media.

## Collect Information Required for the Upgrade

Review this section to collect information regarding the upgrades.

### Provisioning Directory Information

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

Field Name	Description	Your Response
Provisioning Directory Deployment Size	The <a href="#">deployment size</a> (see page 21) that best suits your environment.	
Directory Name	The directory where you want the Provisioning Directory installed.	
Trusted DXmanager Hostname	The hostname of the system with DXmanager installed, or the hostname of the primary Provisioning Directory system. <b>Note:</b> If you have an IPv6 environment, provide an IP address for this field.	
Port	The port number of the Dxadmind process that communicates with DXmanager. <b>Default:</b> 2123	
Password	The password required for Dxadmind to DXmanager authentication.	
Shared Secret	The password for the Provisioning Directory.	
Provisioning Directory	The hostnames of any alternate Provisioning	

Field Name	Description	Your Response
Hostnames	Directory systems in a high-availability configuration.	
Provisioning Server Hostnames	The hostnames of the primary Provisioning Server and any alternate Provisioning Servers already installed or to be installed.	

### Provisioning Directory Deployment Size

When installing the Provisioning Directory, you are asked to choose a deployment size. If you choose a deployment size that is too small for your environment, the existing data does not fit when loaded into the data files, and an upgrade error occurs. Consider the following sizing guidelines with regard to your current Provisioning Directory deployment, and allowing for future growth:

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

**Note:** Intermediate and Large installations require 64 bit Directory installs (either Solaris or Windows 64 bit).

### 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. <b>Default:</b> 20394	
Directory DN	The DN for binding to the Provisioning Directory. <b>Default:</b> eTDSAContainerName=DSAs,	

<b>Field Name</b>	<b>Description</b>	<b>Your Response</b>
	eTNamespaceName=Common Objects,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:

<b>Field Name</b>	<b>Description</b>	<b>Your Response</b>
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.	

## Identity Manager Server Information

You must provide information for every database in your CA Identity Manager implementation, such as the databases for task persistence, workflow, audit, snapshots (reporting), and object storage.

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

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

## SiteMinder Information

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

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

Field Name	Description	Your Response
Policy Server Host Name	The hostname of the SiteMinder Policy Server.	
SiteMinder Administrator Name	The administrator username for the SiteMinder Policy Server.	
SiteMinder Administrator Password	The administrator user password for the SiteMinder Policy Server.	
SiteMinder Agent Name	The name of the SiteMinder Web Agent.	
SiteMinder Shared Secret	The shared secret for the Web Agent, located in the SmHost.conf file.	
Export Location	The location where the Identity Manager Directories and Environments are exported to during migration. <b>Default:</b> C:\Documents and Settings\Administrator	

## Run the Upgrade Wizard

To launch the Upgrade Wizard, run the CA Identity Manager installer from the CA Identity Manager media.

**Note:** Be sure that you have 1GB of available space in the %TEMP% directory before running the upgrade wizard.

The Upgrade Wizard automatically detects previous versions of CA Identity Manager, prompts you through the upgrade process in the correct sequence, and launches all component installers from one location.

**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.

## Upgrade the Provisioning Directory

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

**Note:** If you want to install your Provisioning Directory on a new system, [migrate the Provisioning Directory](#) (see page 27) instead of performing an upgrade.

### To upgrade the Provisioning Directory

1. If you have primary and alternate Provisioning Directories, back up your primary Provisioning Directory.
2. Shut down all Provisioning Directories in your environment.
3. Stop Ingres with the following command:  
`ingstop -service(or ingstop -kill)`
4. Verify that all of the following Ingres processes are stopped:
  - dmfacp.exe
  - dmfrcp.exe
  - iibms.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. Run the CA Identity Manager installer from the CA Identity Manager media.  
The Upgrade Wizard starts.
8. In the Upgrade Wizard, next to Provisioning Directory, click Launch Upgrade.  
If you have more than one Provisioning Directory, this step applies only to the primary Provisioning Directory.

The Provisioning Directory upgrade wizard starts.

Note the following:

- Part of the Provisioning Directory upgrade is the upgrade of CA Directory to r12 SP1. Due to architectural changes in CA Directory r12 SP1, 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.
9. Go through the wizard and enter the information you collected for the upgrade. Select a Typical installation type when prompted during the CA Directory upgrade.

The Provisioning Directory and CA Directory are upgraded.

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

After the upgrade completes, you can find CA Directory r12 SP1 documentation in the following locations:

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

## Migrating your Provisioning Directory

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

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

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

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

- Uninstall and reinstall any alternate Provisioning Directories.

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

**Note:** Be sure to use the *new* Provisioning Directory hostname when upgrading the Provisioning Servers. The default in the upgrade installer will be set to the old hostname and must be changed.

## Upgrade the Provisioning Server

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

The component CA Directory installer is located on the CA Identity Manager media, under CADirectory\dxserver.

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

Note the following when upgrading the Provisioning Server:

- Before installing the Provisioning Server, uninstall and reinstall any alternate Provisioning Directories if they exist. For more information, see the *Installation Guide*.
- If have more than one Provisioning Server, upgrade the primary first, then upgrade all alternate Provisioning Servers.

### To upgrade the Provisioning Server

- If you're not already in the Upgrade Wizard, run the CA Identity Manager installer from the CA Identity Manager media.

The Upgrade Wizard starts.

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

The Provisioning Server upgrade starts. Note the following:

- If you see a Deprecated Connector Warning, be sure to consult the *Connectors Guide* for migration steps to be completed after the upgrade.

- Choose the Custom setup type when prompted, then select the appropriate Installation Type, depending on which components are installed on the system (Provisioning Server, C++Connector Server, or both).
  - You can select a check box during upgrade to indicate Provisioning Directory high availability. If you choose this option, you must supply the hostnames of any alternate Provisioning Directories and specify the primary Provisioning Directory.
3. Go through the wizard and enter the information you collected for the upgrade.  
Your Provisioning Server is upgraded.

## Upgrade the Java Connector Server

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

When upgrading the Java Connector Server, note the following:

- Most fields are automatically populated during the Java Connector Server upgrade. You should only need to supply passwords during the upgrade.
- When providing the component password during the upgrade, you can supply any password that is at least 6 characters long. The installer resets the Java Connector Server component password to what you entered in this field.

## Upgrade the Provisioning Manager

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

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

## Upgrade the Identity Manager Server

**Note:** (WebSphere only) Before you upgrade the Identity Manager Server on WebSphere, be sure that you perform the necessary [prerequisite steps](#) (see page 16).

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 new 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
- Custom code

## Upgrade an Identity Manager Server on a JBoss Cluster

### To upgrade the Identity Manager Server on a JBoss cluster

1. Shut down the application server.
2. Stop the SiteMinder services, if you are using SiteMinder in your environment.
3. Back up the *jboss\_home*\server\all directory on all nodes.
4. Overwrite the *jboss\_home*\server\all directory with only fresh JBoss installation files.
5. Run the CA Identity Manager installer from the server where the previous CA Identity Manager installation was run.

6. Use the CA Identity Manager installer from the cluster domain using the same steps you would use for a new installation.
7. After you complete the upgrade, install the latest version of the JK Connector and be sure that the `workers.properties` file has the following parameters set:  
`worker.worker.ping_mode=A`  
`worker.worker.fail_on_status=400,404,500,503`  
`worker.worker.recovery_options=28`

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

### Upgrade an Identity Manager Server on a WebLogic Cluster

#### To upgrade the Identity Manager Server on a WebLogic cluster

1. On each node, delete the Identity Manager EAR content from the staging area:  
`bea\weblogic92\common\nodemanager\servers\Server_name\stage\IdentityMinder\IdentityMinder.ear*`
2. Shut down the application server.
3. Stop the SiteMinder services, if you are using SiteMinder in your environment.
4. Use the CA Identity Manager installer from the cluster domain using the same steps you would use for a new installation.

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

### Upgrade an Identity Manager Server on a WebSphere Cluster

Depending on which version of WebSphere you upgraded from, perform one of the following procedures:

#### If you upgraded WebSphere from 6.0.2.17 or 5.x

1. Be sure you [migrated the WebSphere EAR](#) (see page 63) for CA Identity Manager from the old to the new version of WebSphere.
2. Be sure the WebSphere application server is running.
3. Navigate to `websphere_home\bin` and run the Cleanup script as follows:
  - **Windows:** `wsadmin -f uninstallCleanup.jacl websphere_node`
  - **Unix:** `./wsadmin.sh -f uninstallCleanup.jacl websphere_node`
4. Go to Service Integration, Buses and delete the IMSBus.
5. Repeat Steps 3 and 4 for each server in the cluster.

6. In the file system, navigate to *Websphere\_home*\profiles\*websphere\_profile*\databases\ and remove *com.ibm.ws.sib* if it exists.
7. Shut down the application server.
8. Stop the SiteMinder services, if you are using SiteMinder in your environment.
9. Run the CA Identity Manager installer on the Deployment Manager, using the same steps you would use for a *new* installation.

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

10. After you complete the upgrade, navigate to *websphere\_home*\bin and run the following command on any additional nodes in the cluster:  
`ims6AddWfEventsJMSQueue.jacl node server cluster`

#### **If you upgraded WebSphere from 6.1.0.15**

1. Shut down the application server.
2. Stop the SiteMinder services, if you are using SiteMinder in your environment.
3. Run the CA Identity Manager installer and use the Upgrade Wizard.
4. After you complete the upgrade, navigate to *websphere\_home*\bin and run the following command on any additional nodes:  
`ims6AddWfEventsJMSQueue.jacl node server cluster`

### **Verify the Upgraded Cluster**

When you have completed all steps using an application server cluster, check that the installation was successful.

#### **To verify the clustered installation**

1. Start the Management Console as follows:

`http://host_name:port/idmmanage`

##### **host\_name**

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

##### **port**

Defines the application server port.

2. If you migrated an Identity Manager environment, access the environment as follows:
  - a. Enter the URL for the Identity Manager environment.
  - b. Verify that you are prompted for the appropriate credentials.

- c. Log in using the account with the System Manager role.
  - d. Verify the correct roles are assigned to this account.
3. If these steps succeeded, start any extra Policy Servers and CA Identity Manager nodes that you stopped.

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

### Optional Upgrade Tasks

The following are optional tasks that can be done during an upgrade:

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

**Note:** After the upgrade, you can migrate all other tasks (not in a pending state) by manually running the task persistence data migration. For more information, see the Manual Upgrades section of this guide.

- Migrate Identity Manager Directories and Environments—migrates all directories and environments from SiteMinder to the Identity Manager object store, if upgrading from CA Identity Manager r8.1 SP2. SiteMinder objects that are no longer used are not deleted after the migration, but you can manually delete them after the upgrade.

**Note:** For RDB user stores, the re-creation of the directories and environments is a manual process.

If you want to perform these tasks during the upgrade, select the appropriate check box when prompted. If you would rather do these tasks manually after the upgrade has completed, see the Manual Upgrades chapter of this guide.

## 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**

Existing remote agents have been certified with CA Identity Manager r12.5, however, if you want IPv6 support, you will need to upgrade your agents. Run the specific agent installer from the Provisioning Component media (under \RemoteAgent) to upgrade these components.

### **Password Sync Agents**

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

### **GINA**

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

### **Vista Credential Provider**

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

### **Bulk Loader Client/PeopleSoft Feed**

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

### **JCS SDK**

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

### **CCI Standalone**

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

## Recompile Custom Code

When you upgrade the Provisioning Server to CA Identity Manager r12.5, 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 Java Connector Server is compatible with the CA Identity Manager r8.1 SP2 and r12 JCS SDK connector code.

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

- Custom C++ Connectors

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

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

### To recompile custom connector code

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

The installer detects the previous SDK version and updates it. Any files or folders, such as custom code placed in the Provisioning SDK admin folder, is preserved.

3. If the original custom code makefiles did not use eta.dep, update the makefiles as follows:

- a. Replace the exception handling flag from /GX to /EHsc.

- b. Remove /YX from the compiler command line option.

- c. Add the following to the compile flag:

```
/D "_CRT_SECURE_NO_WARNINGS" /D "_CRT_NON_CONFORMING_SWPRINTFS" /D  
"_USE_32BIT_TIME_T"
```

- d. Set the correct versions in the makefile, as follows:

- APPVER = 6.0

- \_WIN32\_IE = 0x0700

- e. Add the following to the compile flag:

```
/D "_BIND_TO_CURRENT_VCLIBS_VERSION"
```

This tells the compiler to use VS.2008 SP1 libraries and dlls.

- f. Merge the built EXE and DLL files with the manifest file.

- g. Update the connector source and remove references to obsolete MFC functions.

4. Build the new r12.5 connector. Refer to Microsoft's web site if there are compilation errors.
5. Deploy the connector normally.

## Upgrade Reporting

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

### Upgrade the Report Server

For CA Identity Manager r12.5, upgrade to a supported version of the Report Server.

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

#### To upgrade the Report Server

1. Exit all applications that are running.
2. Download the CA Business Intelligence Common Reporting package and unzip it.

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

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

3. Navigate to Disk1\InstData\VM and double-click the installation executable. The installer starts and prompts you for a locale.
4. Choose Update as the Installation Type when prompted.
5. Accept default settings during the rest of the installation.
6. Click Install.

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

### To verify the upgrade of the Report Server

1. Check the ca-install.log file in the Report Server install folder. The file should contain the following:  
Patch boeXIR2\_SP4 installed successfully.
2. Check the Patch.properties file in the Report Server install folder. The file should contain the following:  
[boeXIR2\_SP4]

## Update the Default Reports

CA Identity Manager r12.5 includes new default reports.

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

### To update the default reports

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

*admin\_tools\BIARTool*

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

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

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

Provide the following information needed to import the default reports:

- Report Server Root Folder—location of the business objects install folder, for example, E:\Program Files\CA\SC\CommonReporting\BusinessObjects
- Enterprise 1.5
- Reporting Database Type—1=MSSQL, 2=Oracle  
**Note:** This is the database that the Report Server (CA Business Intelligence) uses to store its own data.
- Reporting Database User—user created for the Report Database
- Reporting Database Password—password for the user created in Report Database
- Reporting Database DSN Name—the ODBC DSN name created
- Reporting Database Name—the Report Database name

- Reporting Server Administrator Name—The default is Administrator. If you have a different administrator name, provide it here.
- Reporting System Password—reporting administrator’s password entered during the installation
- BIAR File Location—use one of the following:
  - `admin_tools\imlexport\ReportDefinitions\IM Standard Reports\Ms-SQL_Reports\ms-sql_r12_to_r12.5_reports.biar`
  - `admin_tools\imlexport\ReportDefinitions\IM Standard Reports\Oracle Reports\oracle_r12_to_r12.5_reports.biar`

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

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

## Upgrade SiteMinder

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

In CA Identity Manager r12, the Servlet Filter Agent was deprecated. If you are using SiteMinder to protect CA Identity Manager, and you do not have a Web Agent installed, configure a Web Agent for CA Identity Manager r12.5.

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*.



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

---

This section contains the following topics:

[How to Perform Post-Upgrade Configuration](#) (see page 41)

[\(WebSphere only\) Enable XA Transactions](#) (see page 41)

[\(RDB Only\) Modify the User Store](#) (see page 42)

[\(RDB Only\) Recreate Directories and Environments](#) (see page 42)

[Upgrade Custom Workflow Scripts](#) (see page 42)

[Update the Proxy Forwarder](#) (see page 43)

[Upgrade TEWS](#) (see page 43)

[Specify an Inbound Administrator](#) (see page 44)

## How to Perform Post-Upgrade Configuration

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

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

## (WebSphere only) Enable XA Transactions

When using WebSphere with MS SQL 2005, enable XA transactions. CA Identity Manager needs an XA data source for the database transactions to work properly. For more information on enabling XA transactions on Microsoft SQL Server, go to <http://msdn.microsoft.com/en-us/library/aa342335.aspx>

## (RDB Only) Modify the User Store

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

### To modify an RDB user store

1. Edit the `directory.xml` and add the following element:  
`<JDBC datasource=" userstore_jndi"/>`
2. Remove the `maxrows` attribute from the `DirectorySearch` element.
3. If your RDB user store supports Organizations, run the following script located in the `admin_tools\samples\NeteAutoRdb\Organization\` directory:
  - **SQL:** `mssql-orgpath-addon-upgrade-8-to-r12.sql`
  - **ORACLE:** `oracle-orgpath-addon-upgrade-8-to-r12.sql`

## (RDB Only) Recreate Directories and Environments

If you are using an RDB user store, the [Directories](#) (see page 59) and [Environments](#) (see page 62) were automatically exported during the upgrade. However, you need to manually recreate the Directories and Environments after the upgrade. To do this, see the Manual Upgrades section of this guide.

## Upgrade Custom Workflow Scripts

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

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

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

change it as follows:

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

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

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

change it as follows:

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

## Update the Proxy Forwarder

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

## Upgrade TEWS

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

### To recreate the WSDL files

1. Generate the WSDL file in CA Identity Manager r12.5.
2. Keep the following code segments unchanged:
  - `_PND__PND_objectType`
  - `_PND__PND_friendlyName` (when it is used as password policy friendly name)
  - `_PND__PND_regExValue`
  - `_PND__PND_bNoMatch`
  - `_PND__PND_passwordPolicyOid`

3. Remove any other “\_PND\_\_PND\_” from the customized web service code. Capitalize the first character after “\_PND\_\_PND\_”. For example, ViewAccessRoleSearchResultResultItem\_PND\_\_PND\_friendlyName should be changed to ViewAccessRoleSearchResultResultItemFriendlyName.
4. Six method names in six WSDL classes have changed. Modify the customized web service code appropriately if these classes are referenced. The method list is as follows:

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

The six WSDL classes are as follows:

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

5. Save the WSDL file.

## Specify an Inbound Administrator

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

### To specify an Inbound Administrator

1. In the Management Console, click on the Environment.
2. Under the Provisioning Server property, click configure (green arrow) to configure the Provisioning Directory.

3. Under Provisioning Properties, check that the Inbound Administrator field is populated.
4. If there is no Inbound Administrator, specify one before continuing the upgrade.



# Chapter 5: New Feature Configuration

---

This section contains the following topics:

[Add New Roles and Tasks](#) (see page 47)

[Add New Account Screens](#) (see page 48)

[Add Sample Workflow Processes](#) (see page 48)

[Add Workflow Support for AccumulatedProvisioningRolesEvent](#) (see page 49)

[Add Delegation](#) (see page 50)

[Configure IPv6 Support](#) (see page 50)

## Add New Roles and Tasks

In order to add new tasks and roles to a CA Identity Manager r12.5 environment after the upgrade, use the Management Console to import one of the following new role definitions files:

- Upgrade-8.1-to-12.5-RoleDefinitions.xml
- Upgrade-12-to-12.5-RoleDefinitions.xml

### To add new roles and tasks

1. In the Management Console, click Environments.
2. Select the environment.
3. Go to Role and Task Settings.
4. Click Import.  
Multiple role definitions files are listed for import.
5. Select the appropriate role definitions file to add the new roles and tasks.
6. Click Finish.
7. To view and access any new tasks, assign them to the appropriate admin role.

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

## Add New Account Screens

New endpoints are supported in CA Identity Manager r12.5. In order to manage these new endpoints, you must add the the new account management screens to the User Console.

### To add new account management screens

1. In the Management Console, click Environments.
2. Select the environment.
3. Go to Role and Task Settings.
4. Click Import.  
Multiple role definitions files are listed for import.
5. Select the role definitions file for the account screens you want to add.
6. Click Finish.

## Add Sample Workflow Processes

### Template Method Workflow and Task-Level Workflow

To support template method workflow and task-level workflow, use the Workpoint archive tool to import the sample workflow processes as follows:

1. In Workpoint Designer, click Import.  
Workpoint Designer location: *admin\_tools\Workpoint\bin*
2. Navigate to *admin\_tools\workflowScripts* and select *81to12UpgradeWFScripts.zip*.
3. Select one work item.
4. Click Import.
5. Answer the prompts as follows:
  - Are you importing in to empty DB tables: No
  - This import will: treat all objects as new objects
  - If Duplicate Name or reference is encountered: Rename the imported Name or Reference to be unique
6. Repeat Steps 3 through 5 for all work items.
7. Click Finish.

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

## Add Workflow Support for AccumulatedProvisioningRolesEvent

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

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

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

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

This procedure includes references to *admin\_tools*, which represents the folder for the CA Identity Manager Administrative Tools.

The Administrative Tools are placed in the following default locations:

- **Windows:** C:\Program Files\CA\IAM Suite\Identity Manager\tools\tools
- **UNIX:** [set the alternate Installation Path variable]/tools

To enable workflow for the AccumulatedProvisioningRolesEvent

1. For an existing environment, import the appropriate upgrade Role Definitions file (Upgrade-8.1-to-12.5-RoleDefinitions.xml or Upgrade-12-to-12.5-RoleDefinitions.xml) in the Management Console, Role and Task Settings.

See the *Upgrade Guide* for more information.

**Note:** For new environments created with CA Identity Manager r12.0 CR1 or later, the AccumulatedProvisioningRolesUpdate.xml import is not necessary as the approval task is available with new environments.

2. Restart the application server.
3. Verify that the Approve Accumulated Provisioning Roles task exists by using View Admin Task.
4. Run the Archive.bat program, which is located in the *admin\_tools\Workpoint\bin* folder.

5. Import the AccumulatedProvisioningRolesApproveProcess.zip, which is located in the `admin_tools\Workpoint\bin` folder.
6. Open Designer.bat to verify that this process definition now exists.  
Workflow now supports the AccumulatedProvisioningRolesEvent.

## Add Delegation

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

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

These scripts can be found in the following locations:

`admin_tools\samples\NeteAutoRdb\Organization`

`admin_tools\samples\NeteAutoRdb\NoOrganization`

## Configure IPv6 Support

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

### To configure IPv6 on a JBoss application server

1. Open the `run_idm.bat/sh` file located in `jboss_installation\bin`.
2. Modify *one* of the the following properties in the JAVA\_OPTS entry:
  - For IPv6 only systems, uncomment the following entry:  
`#DM_OPTS="$IDM_OPTS -Djava.net.preferIPv6Addresses=true"`
  - For IPv6/IPv4 systems, uncomment the following entry:  
`#DM_OPTS="$IDM_OPTS -Djava.net.preferIPv4Stack=true"`
3. Save the file.

# Appendix A: Manual Upgrades

---

This section contains the following topics:

- [How to Manually Upgrade to CA Identity Manager r12.5](#) (see page 51)
- [Manually Upgrade the Provisioning Directory](#) (see page 52)
- [Manually Upgrade the Provisioning Server](#) (see page 53)
- [Manually Upgrade the Java Connector Server](#) (see page 54)
- [Manually Upgrade the Provisioning Manager](#) (see page 54)
- [Manually Upgrade the Identity Manager Server](#) (see page 55)
- [Manually Deploy CA Identity Manager on WebSphere](#) (see page 63)

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

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

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. In CA Directory r12 SP1, a new memory-mapped file technology named DXgrid is used. For Provisioning to work with CA Identity Manager r12.5, upgrade the Provisioning Directory schema and CA Directory.

**Note:** If you want to install your Provisioning Directory on a new system, [migrate the Provisioning Directory](#) (see page 27) instead of performing an upgrade.

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

### To manually upgrade the Provisioning Directory

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

9. Run the upgrade.bat file.

The Provisioning Directory upgrade wizard starts.

Note the following:

- Part of the Provisioning Directory upgrade is the upgrade of CA Directory to r12 SP1. Due to architectural changes in CA Directory r12 SP1, 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*.

After the upgrade completes, you can find CA Directory r12 SP1 documentation in the following locations:

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

## Manually Upgrade the Provisioning Server

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

### To manually upgrade the Provisioning Server

1. (Windows only) Be sure the Local Service account has read/write permissions to the folder where the Provisioning Server will be installed.
2. Navigate to the Provisioning/ProvisioningServer folder on the CA Identity Manager installer media.

3. Run the setup file.
4. Go through the wizard and enter the information you collected for the upgrade.

Your Provisioning Server is upgraded.

## Manually Upgrade the Java Connector Server

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

### **To manually upgrade the Java Connector Server**

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

Your Java Connector Server is upgraded.

## Manually Upgrade the Provisioning Manager

Perform the following process to manually upgrade the Provisioning Manager.

### **To manually upgrade the Provisioning Manager**

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

Your Provisioning Manager is upgraded.

## Manually Upgrade the Identity Manager Server

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

1. Upgrade the Workflow database.
2. Migrate task persistence data.
3. If upgrading from CA Identity Manager r8.1. SP2, do the following:
  - a. Manually export the Directories and Environments.
  - b. Perform the [configuration after an upgrade from CA Identity Manager r8.1 SP2](#) (see page 41).
  - c. Recreate the Directories and Environments.

### Manually Upgrade the Workflow Database

In Identity Manager r12.5, an updated version of WorkPoint Workflow was added to the installation. Update the workflow database to work with WorkPoint 3.4.2 after upgrading to Identity Manager r12.5.

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

#### **To upgrade to WorkPoint 3.4.2**

1. Run the `wp331_to_wp34_cnv_step1.sql` script to create the new tables for Workpoint 3.4 and to add the new columns to the end of old tables.  
This script also inserts rows into the `WP_*_TYPE` tables as needed.
2. Run the `wp331_to_wp34_cnv_step2.sql` script to create the stored procedures required to convert the data.
3. Run the `wp331_to_wp34_cnv_step3.sql` script to convert the text data to the new columns.  
This script also populates the new `WP_BULK_DATA` table from the old `WP_BULK_STORAGE` table.
4. Run the `wp34_20060927_add.sql` script to create the new tables for Workpoint 3.4.20060927.  
This script also inserts rows into the `WP_INI` and `WP_*_TYPE` tables as needed.
5. Run the `wp34_20070625_add.sql` script to create the new tables for Workpoint 3.4.2.20070625. This also inserts rows into the `WP_INI` and `WP_*_TYPE` tables as needed.

6. Run the wp342\_20071218\_add.sql script to create the new tables for Workpoint 3.4.2.20071218.

This script also inserts rows into the WP\_INI and WP\_\*\_TYPE tables as needed.

7. Enter 'Commit;' to save all changes.

**Note:** The WorkPoint scripts are located in Administrative Tools folder\Workpoint\database. The Administrative Tools are placed in the following default locations:

- **Windows:** C:\Program Files\CA\IAM Suite\Identity Manager\tools\tools
- **UNIX:** [set the alternate Installation Path variable]/tools

## Manually Migrate Task Persistence Data

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

### To manually migrate task persistence data

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

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

2. Be sure that the environment variable `JAVA_HOME` is set.
3. From a command line, navigate to `admin_tools/tpmigration` and run the task persistence migration tool as follows:
  - For Windows:  
`runmigration.bat`
  - For UNIX:  
`runmigration.sh`
4. Enter the following information:
  - Environment protected Alias ('all' for all environments).  
**Note:** If you do not specify all, only one environment can be entered.
  - Task state.  
**Note:** If you do not specify all, only one task state can be entered.
  - CA Identity Manager version to migrate from (1-8.x, 2-12.0).
  - Date range for the tasks to be migrated (y/n).  
**Note:** If you choose 'y', you must enter a Start Date (mm/dd/yy) and End Date (mm/dd/yy).

The migration starts.

After the migration completes, the status indicates how many tasks were migrated.

## Manually Export the Directories and Environments

In CA Identity Manager r12.5, objects previously stored in the SiteMinder Policy Store need to be moved to a relational database object store. SiteMinder objects that are no longer used are not deleted after the migration, but you can manually delete them after the upgrade.

Use the Migration Tool (`imsconfig.bat/imsconfig.sh`) to export your Directory and Environment configurations. Then, use the Management Console to re-import the configurations into r12.5.

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

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

### To export a Directory and Environment

1. Navigate to the following directory:

```
admin_tools\81to12Migration-tool\
```

2. Export a Directory by running the following command:

```
imsconfig -h policy_server_hostname -a agent_name -s agent_shared_secret -u  
siteminder_super_user_name -p siteminder_super_user_password -d im_directory -x folder_name
```

***policy\_server\_hostname***

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

***agent\_name***

Defines the agent.

***agent\_shared\_secret***

Defines the agent's shared secret.

***siteminder\_super\_user\_name***

Defines the SiteMinder administrator.

***siteminder\_super\_user\_password***

Defines the SiteMinder administrator password.

***im\_directory***

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

***folder\_name***

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

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

3. Export an Environment by running the following command:

```
imsconfig -h policy_server_hostname -a agent_name -s agent_shared_secret -u  
siteminder_super_user_name -p siteminder_super_user_password -e im_environment -m folder_name
```

***policy\_server\_hostname***

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

***agent\_name***

Defines the agent.

***agent\_shared\_secret***

Defines the agent's shared secret.

***siteminder\_super\_user\_name***

Defines the SiteMinder administrator.

***siteminder\_super\_user\_password***

Defines the SiteMinder administrator password.

***im\_environment***

The name of the CA Identity Manager environment to export.

***folder\_name***

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

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

- *alias\_environment\_roles.xml*—environment role definitions
- *alias\_environment\_settings.xml*—environment settings not included with the role definitions
- *alias\_environment.xml*—general environment information

## Manually Recreate the Identity Manager Directory

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

## Recreate the Directory on JBoss

### To recreate the Directory on JBoss

1. Create the data source as follows:
  - a. Using the task persistence data source as a template (imtaskpersistencedb-ds.xml), create a userstore-ds.xml data source descriptor file and put it in the *jboss\_home/server/default/deploy* directory.
  - b. Change the JndiName in the data source descriptor file to jdbc/userstore.
  - c. Change the DatabaseName, User, and Password in the data source descriptor to the appropriate values for the userstore database.
2. In the Management Console, click Directories.
3. Click New.
4. Import the previously exported directory.xml to create a new Identity Manager Directory.
5. Specify the JNDI name of the data source you created in Step 1.
6. Click Next.
7. Verify the directory settings and click Finish.

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

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

## Recreate the Directory on WebLogic

### To recreate the Directory on WebLogic

1. Create the data source as follows:
  - a. Within the WebLogic administrative console, create a new userstore data source descriptor.
  - b. Change the JndiName in the data source descriptor according to jdbc/userstore.
  - c. Change the DatabaseName, User, and Password in the data source descriptor to the appropriate values for the userstore database.
  - d. Disable Support Global Transactions on the data source.
2. In the Management Console, click Directories.
3. Click New.
4. Import the previously exported directory.xml to create a new Identity Manager Directory.

5. Specify the JNDI name of the data source you created in Step 1.
6. Click Next.
7. Verify the directory settings and click Finish.

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

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

## Recreate the Directory on WebSphere

### To recreate the Directory on WebSphere

1. Create the data source as follows:
  - a. Within the WebSphere administrative console, create a new userstore data source descriptor.
  - b. Change the JndiName in the data source descriptor to jdbc/userstore.
  - c. Change the DatabaseName, User, and Password in the data source descriptor to the appropriate values for the userstore database.
  - d. Depending on your database, do one of the following:
    - **SQL:** Ensure that the data source is XA, and create a new property for the data source called *enable2phase* and set it to true.
    - **Oracle:** Ensure that the data source is XA.
2. In the Management Console, click Directories.
3. Click New.
4. Import the previously exported directory.xml to create a new Identity Manager Directory.
5. Specify the JNDI name of the data source you created in Step 1.
6. Click Next.
7. Verify the directory settings and click Finish.

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

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

## Manually Recreate the Environment

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

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

### To recreate the environment

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

CA Identity Manager recreates the environment.

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

## Manually Deploy CA Identity Manager on WebSphere

If you want to upgrade CA Identity Manager by manually deploying the EAR on WebSphere, perform the following steps.

**Note:** There is a check box option in the installer that creates a WebSphere EAR for manual deployment.

1. Back up your custom files inside the WebSphere EAR, for example, files under the IdentityMinder.ear/custom/ directory.

You will need to reapply these files after you upgrade to CA Identity Manager r12.5.

2. Extract the EAR from the CA Identity Manager installation as follows:

### Windows:

- a. Copy the following files from *websphere\_home*\WebSphere-tools\ to *websphere\_home*\bin:

- imsExport.bat
- imsExport.jacl

- b. From the command line, navigate to *websphere\_home*\bin and ensure the WebSphere application server is running.

- c. Run the imsExport.bat script as follows:

```
imsExport.bat path_to_exported_ear
```

where *path\_to\_exported\_ear* is the full path and file name that the imsExport utility creates.

### UNIX:

- d. Copy *websphere\_home*\WebSphere-tools\imsExport.jacl to *websphere\_home*\bin.

- e. From the command line, navigate to *websphere\_home*\bin and ensure the WebSphere application server is running.

- f. Run the imsExport.jacl script as follows:

```
./wsadmin.sh -f imsExport.jacl -conntype RMI -port 2809 path_to_exported_ear
```

where *path\_to\_exported\_ear* is the full path including the file name of the exported EAR file.

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

3. Install the extracted CA Identity Manager EAR to a supported version of WebSphere.
4. (Optional) To successfully connect to SiteMinder, do the following:
  - a. Log in to the WebSphere Administrative Console.
  - b. Go to Application Servers, server1, Process Definition, Environment Entries.
  - c. Delete the PATH and LD\_LIBRARY\_PATH entries that point to the agentframework\bin.
5. Re-add the custom files that you backed up in Step 1. Put these files in *websphere\_home/profiles/profile\_name/installedApps/cell\_name/IdentityMinder.ear/custom/*.

**Important!** We recommend that you disable security at profile creation. For example, create a WebSphere profile with the Security Enabled option unchecked. If you do enable security, CA Identity Manager deploys, but with security exceptions at startup. To address this problem, set up WebSphere security using your WebSphere documentation.

# Appendix B: Unattended Upgrades

---

This section contains the following topics:

[How to Perform Unattended Upgrades](#) (see page 65)

[Identity Manager Server Unattended Upgrade](#) (see page 65)

[Provisioning Components Unattended Upgrade](#) (see page 66)

## 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-r12.5-win32.exe -f im-installer.properties -i silent
```

- **UNIX:**

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

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

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

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

## Provisioning Components Unattended Upgrade

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

**-options-template *response\_file\_name***

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

**-options-record *response\_file\_name***

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

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

**Provisioning Directory**

`setup.exe -silent -options response_file_name`

**Provisioning Server**

`setup.exe -silent -options response_file_name`

**Provisioning Manager**

`setup.exe -silent -options response_file_name`

# Appendix C: Successful Upgrade Verification

---

This section contains the following topics:

- [How to Verify the Upgrade](#) (see page 67)
- [CA Directory and Provisioning Directory](#) (see page 68)
- [Provisioning Server and Connector Server](#) (see page 68)
- [Identity Manager Application](#) (see page 69)
- [Runtime Database Schema Upgrades](#) (see page 69)
- [Object Store](#) (see page 70)
- [Pending Tasks](#) (see page 70)
- [Adapters](#) (see page 71)
- [SiteMinder Integration](#) (see page 71)
- [Report Server](#) (see page 72)

## How to Verify the Upgrade

Verify the following CA Identity Manager components to be sure your upgrade to CA Identity Manager r12.5 completed successfully:

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

## CA Directory and Provisioning Directory

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

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

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

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

If one or all of the above dsa services will not start, check the corresponding log file under `dxserver/logs`. To start a dsa service in debug mode, run the following command for the dsa that will not start: "dxserver -d start `system_name-impd-main`"

4. Verify that Ingres is not running, and that it has been completely uninstalled from the system.

## Provisioning Server and Connector Server

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

1. Check the `imps_server_install.log` and the `im_connector_server_install.log` for errors, located in the temp directory for the user who installed the product.
2. Verify that both the CA Identity Manager Provisioning Service and Connector Service have started from the services window.

If they fail to start, check the corresponding logs located in Provisioning Server Install Location/logs folder.

3. If all of the services have started, log into the Provisioning Manager, pointing to the Provisioning Server installed. Acquire and Explore/Correlate a few different endpoints to make sure the Connector Server is working properly.

## Identity Manager Application

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

```

18:41:20,132 WARN [default] #####
18:41:20,132 WARN [default] # CA Identity Manager 12.5.x.x.x
18:41:20,132 WARN [default] #####
18:41:20,132 WARN [default] --- CA IAM FW Startup Sequence Initiated. ---
18:41:20,132 WARN [default] * Startup Step 1 : Attempting to start ServiceLocator.
18:41:20,632 WARN [default] * Startup Step 2 : Attempting to start PolicyServerService
18:41:20,835 WARN [default] * Startup Step 3 : Attempting to start ServerCommandService
18:41:21,148 WARN [default] * Startup Step 4 : Attempting to start EnvironmentService
18:41:21,163 WARN [default] * Startup Step 5 : Attempting to start CacheManagerService
18:41:21,179 WARN [default] * Startup Step 6 : Attempting to load global plugins.
18:41:30,694 WARN [default] * Startup Step 7 : Attempting to start AdaptersConfigService
18:41:30,710 WARN [default] * Startup Step 8 : Attempting to start EmailProviderService
18:41:30,741 WARN [default] * Startup Step 9 : Attempting to start AuditProviderService
18:41:30,788 WARN [default] * Startup Step 10 : Attempting to start RuntimeStatusDetailService
18:41:30,882 WARN [default] * Startup Step 11 : Attempting to start PasswordService
18:41:30,898 WARN [default] * Startup Step 12 : Attempting to start LogicalAttributeService
18:41:30,898 WARN [default] * Startup Step 13 : Attempting to start BLTHService
18:41:30,898 WARN [default] * Startup Step 14 : Attempting to start ParticipantResolverService
18:41:30,898 WARN [default] * Startup Step 15 : Attempting to start NotificationRuleService
18:41:30,898 WARN [default] * Startup Step 16 : Attempting to start EventAdapterService
18:41:30,898 WARN [default] * Startup Step 17 : Attempting to start TaskService
18:41:30,913 WARN [default] * Startup Step 18 : Attempting to start WorkflowCallbackService
18:41:30,929 WARN [default] * Startup Step 19 : Attempting to start WorkflowService
18:41:30,944 WARN [default] * Startup Step 20 : Attempting to start EventService
18:41:31,023 WARN [default] * Startup Step 21 : Attempting to start AdminService
18:41:31,038 WARN [default] * Startup Step 22 : Attempting to start GeneralMonitorAdmin
18:41:31,038 WARN [default] * Startup Step 23 : Attempting to start GlobalInitializer plug-ins
18:41:31,038 WARN [default] * Startup Step 24 : Attempting to start environments
18:42:15,960 WARN [EnvironmentService] * Starting environment: XXXX
18:42:18,116 WARN [default] * Startup Step 25 : Attempting to start SchedulerService
18:42:18,163 WARN [default] * Startup Step 26 : Attempting to recover events and runtime status details
18:42:18,257 WARN [default] --- CA IAM FW Startup Sequence Complete. ---

```

## Runtime Database Schema Upgrades

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

- Workflow
- Task Persistence
- Archive
- Audit
- Snapshot

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

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

## Object Store

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

## Pending Tasks

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

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

---

## Adapters

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

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

## SiteMinder Integration

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

- Communication with the SiteMinder Policy Server

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

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

- SiteMinder Authentication

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

- Password Management

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

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

2. Attempt to modify a user's password and be sure the password composition rules from the applicable password policy are in effect.
3. Reset a user's password using the Reset Password Task, choosing the 'Password Must Change' option.
4. Attempt to login with that user and verify that the login attempt is redirected to the Change Password task.
5. Change the password and verify that the user login is successful.

## Report Server

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

1. Check the CA\_Business\_Intelligence\_InstallLog.log and the ca-install.log for errors, located in the temp directory for the user who installed the product.
2. From Start, Programs, Business Objects, start the Central Configuration Manager. Be sure that all of the services are started, with the exception of the WinHTTP Web Proxy.

If they are not started, start them.

If any of the services fail to start, check the corresponding logs located in the Business Objects Install location/logging folder.

3. If all of the services have started, log into the Admin Launchpad, by going to the following  
URL: <http://ls3:8080/businessobjects/enterprise115/adminlaunch>.
4. Launch the Central Management console.

# Index

---

## (

- (RDB Only) Modify the User Store • 40
- (RDB Only) Recreate Directories and Environments • 40
- (WebSphere only) Enable XA Transactions • 39

## A

- Adapters • 71
- Add Delegation • 48
- Add New Account Screens • 46
- Add New Roles and Tasks • 45
- Add Sample Workflow Processes • 46
- Add Workflow Support for AccumulatedProvisioningRolesEvent • 47
- Architecture Changes • 10

## B

- Back Up Custom Code • 17

## C

- CA Directory and Provisioning Directory • 68
- CA Identity Manager Upgrade • 19
- CA Product References • iii
- Check for Cumulative Releases • 14
- Check Hardware Requirements • 12
- Check Software Requirements • 14
- Collect Information Required for the Upgrade • 20
- Configuration After Upgrade from CA Identity Manager r8.1 SP2 • 39
- Configure IPv6 Support • 49
- Configure WebSphere for the Upgrade • 16
- Contact CA • iii

## H

- How to Manually Upgrade to CA Identity Manager r12.5 • 51
- How to Meet Prerequisites for the Upgrade • 11
- How to Perform Post-Upgrade Configuration • 39
- How to Perform Unattended Upgrades • 65
- How to Upgrade CA Identity Manager • 19
- How to Verify the Upgrade • 67

## I

- Identity Manager Application • 69
- Identity Manager Server Information • 22
- Identity Manager Server Unattended Upgrade • 65
- Install the CA Identity Manager Bookshelf • 11

## J

- Java Connector Server Information • 22

## M

- Manual Upgrades • 51
- Manually Deploy CA Identity Manager on WebSphere • 63
- Manually Export the Directories and Environments • 58
- Manually Migrate Task Persistence Data • 57
- Manually Recreate the Environment • 62
- Manually Recreate the Identity Manager Directory • 59
- Manually Upgrade the Identity Manager Server • 55
- Manually Upgrade the Java Connector Server • 54
- Manually Upgrade the Provisioning Directory • 52
- Manually Upgrade the Provisioning Manager • 54
- Manually Upgrade the Provisioning Server • 53
- Manually Upgrade the Workflow Database • 55
- Migrating your Provisioning Directory • 26

## N

- New Feature Configuration • 45

## O

- Object Store • 70
- Optional Upgrade Tasks • 32

## P

- Pending Tasks • 70
- Provisioning Components Unattended Upgrade • 66
- Provisioning Directory Deployment Size • 21
- Provisioning Directory Information • 20

---

Provisioning Server and Connector Server • 68  
Provisioning Server Information • 21

## R

Recompile Custom Code • 34  
Recreate the Directory on JBoss • 60  
Recreate the Directory on WebLogic • 60  
Recreate the Directory on WebSphere • 61  
Report Server • 72  
Run the Upgrade Wizard • 24  
Runtime Database Schema Upgrades • 69

## S

SiteMinder Information • 23  
SiteMinder Integration • 71  
Specify an Inbound Administrator • 42  
SSL Configuration • 17  
Successful Upgrade Verification • 67  
Supported Upgrade Paths • 9

## U

Unattended Upgrades • 65  
Update the Default Reports • 37  
Update the Proxy Forwarder • 41  
Upgrade an Identity Manager Server on a JBoss Cluster • 29  
Upgrade an Identity Manager Server on a WebLogic Cluster • 30  
Upgrade an Identity Manager Server on a WebSphere Cluster • 30  
Upgrade Custom Workflow Scripts • 40  
Upgrade Other Provisioning Components • 33  
Upgrade Overview • 9  
Upgrade Prerequisites • 11  
Upgrade Process • 9  
Upgrade Reporting • 36  
Upgrade SiteMinder • 38  
Upgrade TEWS • 41  
Upgrade the Identity Manager Server • 29  
Upgrade the Java Connector Server • 28  
Upgrade the Provisioning Directory • 24  
Upgrade the Provisioning Manager • 29  
Upgrade the Provisioning Server • 27  
Upgrade the Report Server • 36  
Upgrade to a Supported Application Server • 15

## V

Verify the Upgraded Cluster • 31