CA Identity Manager

Installation Guide (WebLogic)

r12

CA Product References

This document references the following CA products:

- CA Identity Manager
- CA SiteMinder® Web Access Manager
- CA Security Command Center (SCC)
- CA Audit
- eTrust® Directory, also known as CA Directory

Contact Technical Support

For online technical assistance and a complete list of locations, primary service hours, and telephone numbers, contact Technical Support at http://ca.com/support.

Contents

Chapter 1: Installation Overview

This guide provides instructions for installing Identity Manager and also includes information on optional components for installation such as provisioning and SiteMinder.

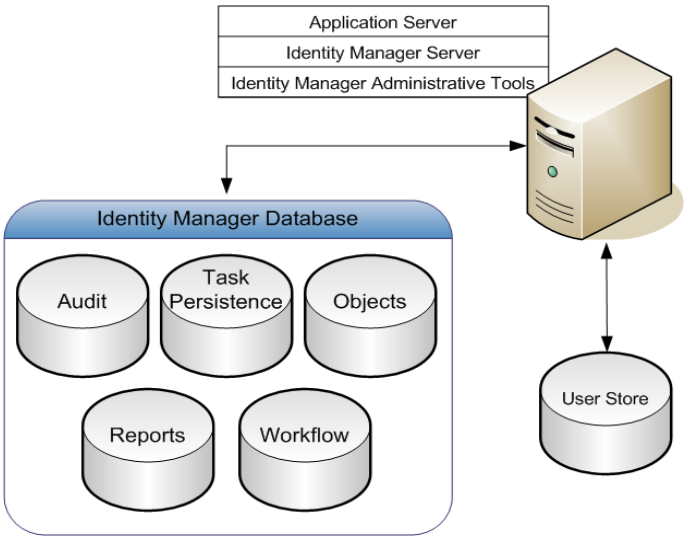
This section contains the following topics:

Sample Identity Manager Installations

Based on the functionality you want to implement, you can choose which components of Identity Manager you want to install in your environment. The following section illustrates some examples of Identity Manager implementations at a high level.

Basic Installation

In all Identity Manager installations, the Identity Manager Server is installed on an application server. After you install the application server, you use the Identity Manager Installer to install all the software on the same system. The following figure is an example of a basic Identity Manager installation:



Identity Manager Server

Executes tasks within Identity Manager. The J2EE Identity Manager application includes the Management Console (configuring environments), and the User Console (managing an environment). With the Identity Manager Server, you can also install Identity Manager iRecorder, which you use for auditing tasks.

Identity Manager Administrative Tools

Provides tools and samples for configuring and using Identity Manager. The tools include configuration files, scripts, utilities, and jar files that you use to compile custom objects with Identity Manager APIs and API samples. The Provisioning Manager and WorkPoint Designer are also included with the Administrative Tools. Administrative Tools are placed in the following locations:

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

Identity Manager Database

Stores data for Identity Manager. This database stores information for auditing, task persistence, reporting, workflow, and Identity Manager objects. This must be a relational database.

Note: For a complete list of supported relational databases, see the Identity Manager Support Matrix on the Identity Manager support site http://ca.com/support.

Identity Manager User Store

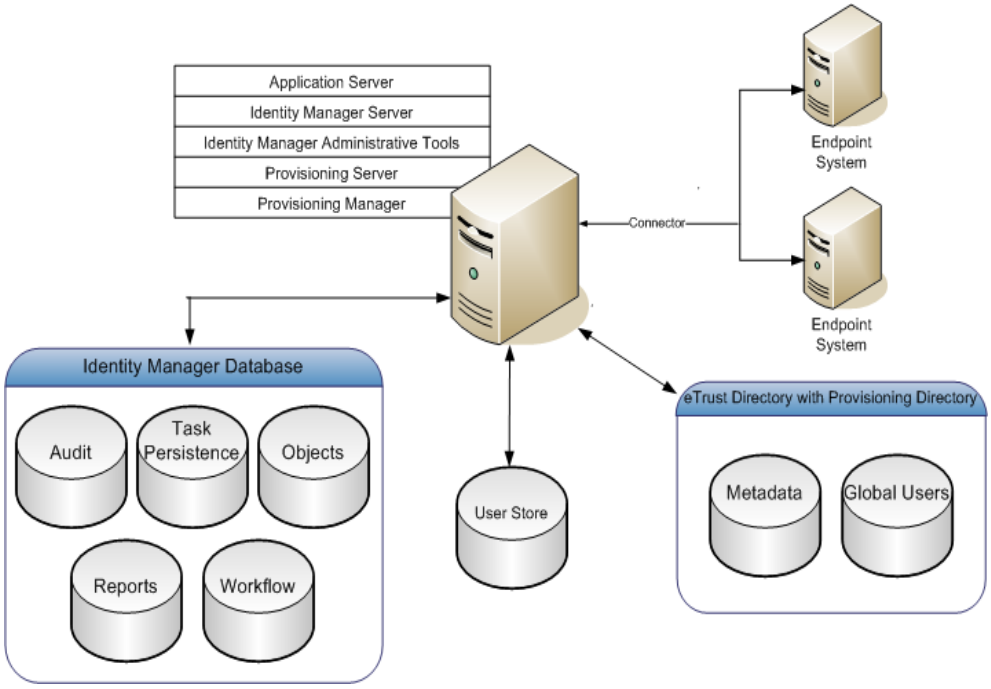
Contains users and their information. This store can be a pre-existing user store already in use by the company. This can be LDAP or a relational database.

Note: For more information on setting up a user store for Identity Manager, see the *Configuration Guide*.

Installation with Provisioning Components

Identity Manager provisioning allows you to create an Environment that connects to a Provisioning Server for provisioning accounts to various endpoint systems. You can assign provisioning roles to users you create through Identity Manager. Provisioning roles are roles with account templates that define accounts that users can receive on endpoint systems. Accounts provide users with access to additional resources, such as an email account.

When you assign a provisioning role to a user, that user receives the accounts defined by the account templates in the role. The account templates also define how user attributes are mapped to accounts. The accounts exist in managed endpoints defined by the account templates. The following figure is an example of an Identity Manager installation with provisioning:



Identity Manager Server

Executes tasks within Identity Manager. The J2EE Identity Manager application includes the Management Console (configuring environments), and the User Console (managing an environment). With the Identity Manager Server, you can also install Identity Manager iRecorder, which you use for auditing tasks.

Identity Manager Administrative Tools

Provides tools and samples for configuring and using Identity Manager. The tools include configuration files, scripts, utilities, and jar files that you use to compile custom objects with Identity Manager APIs and API samples. The Provisioning Manager and WorkPoint Designer are also included with the Administrative Tools. Administrative Tools are placed in the following locations:

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

Identity Manager Database

Stores data for Identity Manager. This database stores information for auditing, task persistence, reporting, workflow, and Identity Manager objects. This must be a relational database.

Note: For a complete list of supported relational databases, see the Identity Manager Support Matrix on the Identity Manager support site http://ca.com/support.

Identity Manager User Store

Contains users and their information. This store can be a pre-existing user store already in use by the company. This can be LDAP or a relational database.

Note: For more information on setting up a user store for Identity Manager, see the *Configuration Guide*.

Identity Manager Provisioning Server

Manages accounts on endpoint systems.

Note: Before installing the Provisioning Server, install eTrust Directory on a separate system and run the Provisioning Directory Initialization on the eTrust Directory system.

Identity Manager Provisioning Directory Initialization

Specifies the directory schema to eTrust Directory. This schema sets up the Directory System Agents (DSAs) within eTrust Directory.

Note: eTrust Directory is a prerequisite to running the Provisioning Directory Initialization.

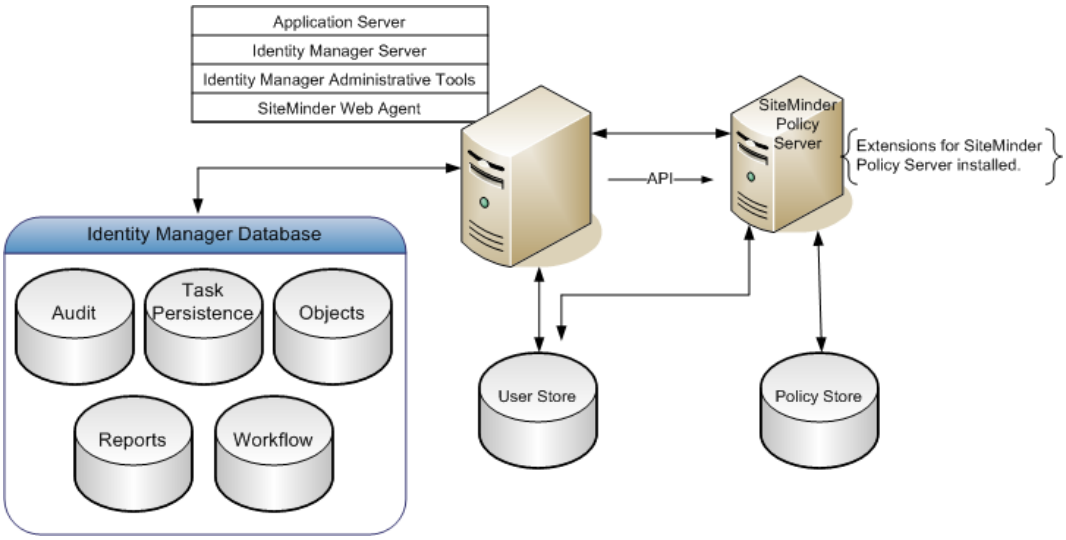
Identity Manager Provisioning Manager

Manages the Provisioning Server through a graphical interface. This is used for administrative tasks such as acquiring endpoints, installing endpoint types, and managing provisioning server options. The Provisioning Manager is installed as part of the Identity Manager Administrative Tools.

Note: This application runs on Windows only.

Installation with SiteMinder Policy Server

A SiteMinder Policy Server provides advanced authentication and protection for your Environment. The following figure is an example of an Identity Manager installation with a SiteMinder Policy Server:



Identity Manager Server

Executes tasks within Identity Manager. The J2EE Identity Manager application includes the Management Console (configuring environments), and the User Console (managing an environment). With the Identity Manager Server, you can also install Identity Manager iRecorder, which you use for auditing tasks.

Identity Manager Administrative Tools

Provides tools and samples for configuring and using Identity Manager. The tools include configuration files, scripts, utilities, and jar files that you use to compile custom objects with Identity Manager APIs and API samples. The Provisioning Manager and WorkPoint Designer are also included with the Administrative Tools. Administrative Tools are placed in the following locations:

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

Identity Manager Database

Stores data for Identity Manager. This database stores information for auditing, task persistence, reporting, workflow, and Identity Manager objects. This must be a relational database.

Note: For a complete list of supported relational databases, see the Identity Manager Support Matrix on the Identity Manager support site http://ca.com/support.

Identity Manager User Store

Contains users and their information. This store can be a pre-existing user store already in use by the company. This can be LDAP or a relational database.

Note: For more information on setting up a user store for Identity Manager, see the *Configuration Guide*.

SiteMinder Web Agent

Works with the SiteMinder Policy Server to protect the User Console. Installed on the system with the Identity Manager Server.

SiteMinder Policy Server

Provides advanced authentication and authorization for Identity Manager, as well as other facilities such as Password Services, Single Sign-On, and so forth.

Extensions for SiteMinder Policy Server

Enables a SiteMinder Policy Server to support Identity Manager. Install the extensions on each SiteMinder Policy Server system in your Identity Manager implementation.

Installation Process

To install Identity Manager, perform the following steps:

1. Install the prerequisite hardware and software.
2. Install the Identity Manager components.
3. Starting Identity Manager.
4. (Optional) Protect Identity Manager with SiteMinder.
5. (Optional) Configure provisioning.
6. (Optional) Configure email notification.
7. (Optional) Configure workflow.
8. (Optional) Install reporting.
9. (Optional) Configure internationalization.

Note: In this document, each chapter includes a checklist of the steps to install or configure an Identity Manager feature or component. It is the section that begins with a How To title in each chapter. The appendix **Installation Checklists** includes all checklists. You may want to print this appendix before you begin the installation.

Installation Worksheet

During Identity Manager installation, you are prompted for the location of software, administrator account names, and other information. To simplify the installation process, see the appendix **Installation Worksheet** to have answers ready for these questions.

Chapter 2: Identity Manager Prerequisites

This section contains the following topics:

Installation Status

The following table shows you where you are in the installation process:

You Are Here	Step in Installation Process
X	**1. Install prerequisite hardware and software.**
	2. Install Identity Manager components.
	3. Start Identity Manager.
	4. (Optional) Protect Identity Manager with SiteMinder.
	5. (Optional) Configure provisioning.
	6. (Optional) Configure email notification.
	7. (Optional) Configure workflow.
	8. (Optional) Install reporting.
	9. (Optional) Configure internationalization.

Prerequisite Knowledge

This guide is intended for users who are familiar with Java, J2EE standards, or application server technology. It assumes that you have the following technical knowledge:

- An understanding of J2EE application servers and multi-tier architecture
- Experience with managing the application server, including tasks such as starting the application server
- Experience with managing a relational database
- (Optional) Familiarity with SiteMinder concepts, terms, and Policy Server configuration tasks

How to Install Prerequisite Components

To install the prerequisite hardware and software for Identity Manager:

✓	Step
	1. Confirm that the system that will host Identity Manager satisfies the hardware requirements.
	2. Review the software prerequisites for Identity Manager.
	3. Create a database for Identity Manager.
	4. Confirm that the application server that will host Identity Manager is installed and configured correctly.

Hardware Requirements

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

- CPU: Single or dual-processor, Intel Pentium III (or compatible) 700-900 MHz, or Sparc Workstation 440MHz
- Memory: 2 GB
- Available disk space: 1 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.

Software Requirements

Before you install Identity Manager, do the following:

1. Install the application server on the system where you plan to install the Identity Manager Server.
2. Install a supported Java Development Kit (JDK) or Java Runtime Environment (JRE) for Identity Manager on the application server system.

   Note: For a complete list of supported platforms and versions, see the Identity Manager Support Matrix on the Identity Manager support site http://ca.com/support.
3. If you plan to enable provisioning, run the Provisioning Directory Initialization on the system with eTrust Directory installed. eTrust Directory is a prerequisite to running the Provisioning Directory Initialization.

   Important! For a production environment, install eTrust Directory on a separate system from the Identity Manager Server.
4. If you plan to use SiteMinder to protect Identity Manager, install the SiteMinder Policy Server and download the SiteMinder bookshelf.
5. Install Security Command Center if you have purchased it and plan to install Identity Manager iRecorder.

Access the Identity Manager Support Matrix

For a complete list of supported software versions, see the Identity Manager support matrix.

To locate the support matrix

1. Log into support.ca.com.
2. Click Support By Product or Solution.
3. Select CA Identity Manager in the Products section under Select a Product or Solution page.

   The CA Identity Manager page opens.
4. Scroll to Recommend Readings.
5. Click CA Identity Manager Informational Documentation Index.

A page displays platform support matrices for supported versions of Identity Manager.

Create a Database

Create a database for Identity Manager. This database will be used to store objects and data for auditing, reports, workflow, and task persistence. For more information, see the appendix on **Creating a New Database**.

Create a user account for the database. This user must have administrative rights to the database.

When you run the Identity Manager installer, provide the database information when prompted, and all the database schemas will be created automatically.

WebLogic Application Server

The following sections provide information to aid users with a WebLogic application server. If you are comfortable using WebLogic, you may alter the instructions in the following sections. However, note the following:

- Identity Manager is a J2EE application. You may use WebLogic's features to tune Identity Manager according to your preferences.
- The Identity Manager Server must be the only application deployed on the application server.
- Identity Manager takes advantage of the auto-deployment feature of WebLogic. When creating your WebLogic domain, be sure to select a domain type that supports auto-deployment.

Deployment Differences in WebLogic 8.1 and WebLogic 9.2

Identity Manager r12 supports WebLogic 8.1 and WebLogic 9.2. Due to changes in the WebLogic 9.2 application server, there is a difference in how Identity Manager is deployed on each version of the application server.

The following table describes the differences in deploying Identity Manager on WebLogic 8.1 and WebLogic 9.2.

Feature	WebLogic 8.1	WebLogic 9.2
Supported Java Environment	JRE 1.4.2_13	JDK 1.5.0_09

Location of the WebLogic start scripts	*wl domain directory/wl_domain* For example, the Windows default is: c:\bea\user_projects\domains*wl_domain*	*wl domain directory/wl_domain*/bin For example, the Windows default is: c:\bea\user_projects\domains*wl_domain*\bin

Note: For a complete list of supported platforms and versions, see the Identity Manager Support Matrix on the Identity Manager support site http://ca.com/support.

Install a WebLogic Application Server

Install the WebLogic server as described in BEA's documentation:

- WebLogic 8.1:
  http://edocs.bea.com/platform/docs81/install/index.html
- WebLogic 9.2:
  http://edocs.bea.com/wls/docs92/index.html

Note: For a complete list of supported platforms and versions, see the Identity Manager Support Matrix on the Identity Manager support site http://ca.com/support.

Create a WebLogic Application Server Instance

Before installing Identity Manager Server, create a WebLogic domain using the Configuration Wizard that is part of the WebLogic installation and do the following:

- Note the name of the domain. You will need the domain name when you install Identity Manager.
- Select the Basic WebLogic Server Domain template.
- Verify that the JAVA_HOME variable is set to the path for the required Java environment in one of the following files:
  - WebLogic 8.1: the StartWebLogic.cmd/.sh file, which is located in *weblogic_home*\user_projects\domains*weblogic_domain*
  - WebLogic 9.2: the setDomainEnv.cmd/.sh file, which is located in *weblogic_home*\user_projects\domains*weblogic_domain*\bin

Verify the WebLogic Domain

Confirm the following:

- The WebLogic server is running.
- You can access the WebLogic console at the following URL:
  http://*hostname*:*port*/console

  For example:
  http://myserver.mycompany.com:7001/console
- In the WebLogic console, under Domain Configurations, select the Domains link.

  The newly created domain should appear in the list of existing domains.

Note: Once you have completed the verification, shut down the application server to prepare for Identity Manager installation.

Chapter 3: Installing Identity Manager Components

This section contains the following topics:

Installation Status

The following table shows you where you are in the installation process:

You Are Here	Step in Installation Process
	1. Install prerequisite hardware and software.
X	**2. Install Identity Manager components.**
	3. Start Identity Manager.
	4. (Optional) Protect Identity Manager with SiteMinder.
	5. (Optional) Configure provisioning.
	6. (Optional) Configure email notification.
	7. (Optional) Configure workflow.
	8. (Optional) Install reporting.
	9. (Optional) Configure internationalization.

Identity Manager Components

The Identity Manager installation components include the following:

- Identity Manager Server
- Identity Manager Administrative Tools
- Identity Manager Provisioning Server
- Identity Manager Provisioning Directory Initialization
- Identity Manager Extensions for SiteMinder

How to Install Identity Manager Components

Use the following checklist to install the components of Identity Manager:

✓	Step
	1. Gather information needed for the installation program.
	2. Check if any Identity Manager Cumulative Releases exist.
	3. Review important notes prior to the Identity Manager installation.
	4. Install the Identity Manager components.
	5. Install the Identity Manager Bookshelf.

Important! If you are going to use SiteMinder, see the chapter on Protecting Identity Manager with SiteMinder and follow the steps to configure SiteMinder to work with Identity Manager.

Gather Information for the Installation

The Identity Manager installation program asks you for information about previously installed software and the software that you are installing.

Note: Use the **Installation Worksheet** to record this information. We recommend that you complete the worksheet before starting the installation.

WebLogic Information

Record the following WebLogic information you need during the Identity Manager installation:

Field Name	Description	Your Response
WebLogic Binary Folder	The location of the application server home directory.	
Domain Folder	The name of the WebLogic domain you created for Identity Manager. **Default:** mydomain	
Server Name	The name of the WebLogic server on which the domain is configured. **Default:** myserver	
Cluster Name	The cluster name for high-availability implementations. This is only needed if you plan on installing Identity Manager in a clustered environment. **Note:** For more information on clustering, see the *High-Availability Guide*.	
App Server URL and port	The application URL and port number of the system that will host the Identity Manager Server (system that will host the application server).	

Provisioning Information

Record the following Provisioning Directory information you need during the Identity Manager installation:

Field Name	Description	Your Response
Host	The hostname of the remote Provisioning Directory system.	

Field Name	Description	Your Response
Port	The port number of a remote Provisioning Directory system.	
User Password	The remote Provisioning Directory user password.	
Domain Name	The domain name for the Provisioning Directory. This is required for both local and remote Provisioning Directory installations. **Default:** IDENTITY_MANAGER **Note:** You should not change the domain unless you are connecting to an existing domain.	

Database Information

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

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

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

iRecorder Information

Record the following iRecorder information you need during the Identity Manager installation:

Field Name	Description	Your Response
Host name or IP of Audit Client or iRouter	The hostname or IP address of the iRouter used by CA Security Command Center or CA Audit.	

SiteMinder Information

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

Field Name	Description	Your Response
Policy Server Host Name	The hostname of the SiteMinder Policy Server.	
SiteMinder Administrator Name	The administrator username for the SiteMinder Policy Server.	
SiteMinder Administrator Password	The administrator user password for the SiteMinder Policy Server.	
SiteMinder Folder (Solaris Only)	The location of SiteMinder on the system with a SiteMinder Policy Server installed.	

Important! When installing Identity Manager with SiteMinder, the installation does not prompt the user for the Web Agent name. Instead, the installer refers to the generic username as the agent name and the generic password as the agent shared secret. To connect to an existing SiteMinder deployment with set agent credentials, edit the ra.xml file under the "IdentityMinder.ear\policyserver.rar\META-INF" folder and set the AgentName and AgentSecret properties to the correct values.

Check for Identity Manager Cumulative Releases

Check for the latest Identity Manager Cumulative Release (CR) at the Identity Manager support site. If you find a CR release for Identity Manager r12, use the Identity Manager CR installer to install or to upgrade an existing r12 installation with the latest fixes and enhancements.

To check for Identity Manager Cumulative Releases

1. In a web browser, go to the Identity Manager support site http://ca.com/support.
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 Identity Manager components on one system or several systems.

Important Notes for Installation

Before installing an Identity Manager component, note the following:

- Install the Identity Manager Server on the system where you installed the application server.
- If you are installing on a Solaris system, all the installer executables must have the appropriate permissions. To do this, execute the following command:
  chmod -R a+x *install_directory*
- If you are installing the Provisioning Server on a Windows system, log in as a Local Administrator.
- If you are installing the Provisioning Server on a Solaris system, run the installer as root.
- If you are installing the iRecorder with the Identity Manager Server on a Solaris system, run the installer as root.

- If you want to use a SiteMinder Policy Server to protect Identity Manager, install the Identity Manager Extensions for Policy Server on each Policy Server in your Identity Manager deployment. Also, ensure that you configure the policy store for Identity Manager.

  Note: For more information on how to configure SiteMinder to work with Identity Manager, see the section on Protecting Identity Manager with SiteMinder.

- If you need the Provisioning Manager to be installed, install the Administrative Tools on a Windows system.

- If you want to enable provisioning in Identity Manager, run the Provisioning Directory Initialization on the system where eTrust Directory is installed. eTrust Directory is a prerequisite for enabling provisioning in Identity Manager.

  Important! For a production environment, install eTrust Directory on a separate system from the Identity Manager Server. This can be done by running the Identity Manager installer on the remote machine.

- If you want to use the Identity Manager workflow feature or the Identity Manager export utility, ensure that JDK 1.4.2_13 or higher is installed on the system where you are installing the Administrative Tools.

- If you are running the Identity Manager installer on an IPv6 system, ensure that you provide hostnames (and not IP addresses) in the installer screens.

Install Identity Manager Components

Run the Identity Manager installation program on each server in your deployment to install the appropriate component. Choose the option to install one or more of the following components:

- Identity Manager Server
- Identity Manager Administrative Tools—These tools include the Provisioning Manager which can only run in a Windows environment.
- Identity Manager Provisioning Server—If you want to enable provisioning within Identity Manager, install the Provisioning Server. Install the Provisioning Server on the same system as the Identity Manager Server or a separate system.
- Identity Manager Provisioning Directory Initialization—This should be run on the system where eTrust Directory is installed. eTrust Directory is a prerequisite for enabling provisioning in Identity Manager.

- Identity Manager extensions to the Policy Server—If you are using SiteMinder Policy Server to protect Identity Manager, install these extensions. Install these extensions on the same system as the Policy Server.

The Identity Manager installer also allows you to configure the following options during installation:

iRecorder

The iRecorder sends Identity Manager events to CA Audit. Once in CA Audit, the events can be monitored by CA Audit or CA Security Command Center (SCC). For more information about the iRecorder, see the iRecorder Reference Guide for CA Identity Manager, which is available in the Identity Manager Bookshelf.

Connection to a remote Provisioning Directory

If you have already installed a Provisioning Directory on another system, as recommended, this option allows you to connect the Identity Manager Server to that system.

FIPS 140-2

All components in an Identity Manager environment need to be FIPS 140-2 enabled in order for Identity Manager to support FIPS 140-2. You will need a FIPS encryption key to enable FIPS 140-2 during installation. A Password Tool for providing a FIPS key is located in the following directory:

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

Important! Use the same FIPS 140-2 encryption key in all installations and ensure that you safeguard the key file once generated by the Password Tool.

Production Environments

Important! For a production environment, keep all data systems and server systems separate. For example, eTrust Directory and a database (SQL or Oracle) should be on a separate system than the Identity Manager Server and the Provisioning Server.

To install Identity Manager components in a production environment

1. Complete the steps that apply to your installation:
   - If you are installing the Identity Manager Server, stop the application server.
   - If you are installing only the Administrative Tools and you want to use Identity Manager's WorkPoint workflow feature, skip to Step 2.
   - If you are installing Identity Manager Extensions for the Policy Server, stop the SiteMinder services.
   - If you are running the Provisioning Directory Initialization, ensure that eTrust Directory is already installed on the system.
2. Do one of the following:
   - **Windows:** From your installation media, run the following program: \win32\ca-im-12.0-win32.exe
   - **UNIX:** From your installation media, run the following program: /solaris/ca-im-12.0-sol.bin

   The Identity Manager installer opens.
3. Complete the instructions in the Identity Manager installation dialog boxes.

   When prompted, select the components to install.
4. Check that you can ping the systems that host the Policy Server and other Identity Manager components from the system with the Identity Manager Server.
5. To continue with the installation, proceed to Install the Identity Manager Bookshelf.

Demonstration Environments

You may decide to install all the components of your Identity Manager deployment on a single system. If so, use the Identity Manager installation program to quickly install all software components of Identity Manager on the same system.

Important! Installing *all* Identity Manager components on one system is recommended for demonstration environments *only*.

To install all Identity Manager software on a single system

1. Stop the application server.
2. Run the Identity Manager installer:
   - **Windows:** From your installation media, run the following program: \win32\ca-im-12.0-win32.exe
   - **UNIX:** From your installation media, run the following program: /solaris/ca-im-12.0-sol.bin

   The Identity Manager installer opens.
3. Check all of the following components to install on a single system:
   - Identity Manager Server
   - Identity Manager Administrative Tools

     Note: Provisioning Manager will only be installed if the system is Windows.
   - Identity Manager Provisioning Server
   - Identity Manager Provisioning Directory Initialization

     Note: eTrust Directory must already be installed on the system.
   - Identity Manager Extensions to the Policy Server
4. Complete the instructions in the Identity Manager installer dialog boxes.

To continue with the installation, proceed to Install the Identity Manager Bookshelf.

Install Additional Components

If you installed a subset of the Identity Manager components, you may want to install additional components at a later date.

To install additional components

1. Stop the application server.
2. Do one of the following:
   - **Windows:** From your installation media, run the following program: \win32\ca-im-12.0-win32.exe
   - **UNIX:** From your installation media, run the following program: /solaris/ca-im-12.0-sol.bin

   The Identity Manager installer opens.

3. To install one or more of the following components, select it and continue with the installation:
   - Identity Manager Server
   - Identity Manager Administrative Tools
   - Identity Manager Provisioning Server
   - Identity Manager Provisioning Directory Initialization
   - Identity Manager Extensions for SiteMinder Policy Server

   Note: If a component is already installed, Identity Manager will update that component if it is selected. To prevent Identity Manager from updating the component, clear it before continuing.
4. Complete the instructions in the Identity Manager installation dialog boxes.
5. To install or configure a connection to the Provisioning Directory or the iRecorder, complete one of the following steps:
   - If the Identity Manager Server is not installed, select the Identity Manager Server component and the additional components to install, and continue with the installation.
   - If the Identity Manager Server is installed, select just the additional components to install, and continue with the installation.

Install the Identity Manager Bookshelf

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

- Use a single console to view documents published for Identity Manager (including Provisioning).
- 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 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.

Chapter 4: Starting Identity Manager

This section contains the following topics:

Installation Status

The following table shows you where you are in the installation process:

You Are Here	Step in Installation Process
	1. Install prerequisite hardware and software.
	2. Install Identity Manager components.
X	**3. Start Identity Manager.**
	4. (Optional) Protect Identity Manager with SiteMinder.
	5. (Optional) Configure provisioning.
	6. (Optional) Configure email notification.
	7. (Optional) Configure workflow.
	8. (Optional) Install reporting.
	9. (Optional) Configure internationalization.

How to Start Identity Manager

After you install the Identity Manager software components, perform the following steps to start the Identity Manager Server for the first time:

	Step
	1. Start the Identity Manager Server.

Step
2. Confirm that Identity Manager started correctly.

Start the Identity Manager Server

To start Identity Manager on WebLogic, you use the startWebLogic.cmd file for Windows, or the startWebLogic.sh file on UNIX. This file is located in the directory that was created for your Identity Manager domain.

To start Identity Manager Server on WebLogic

1. Navigate to *one* of the following from a command line:
   - WebLogic 8.1: *weblogic_home*/*weblogic_domain*

     For example, the Windows default is:
     c:\bea\user_projects\domains*weblogic_domain*
   - WebLogic 9.2: *weblogic_home*/*weblogic_domain*/bin

     For example, the Windows default is:
     c:\bea\user_projects\domains*weblogic_domain*\bin
2. Enter the following:
   - **Windows:** startWebLogic
   - **UNIX:** ./startWebLogic.sh

   You may be prompted for the WebLogic administrator name and password for the application server to start up.
3. If prompted, enter the WebLogic administrator name and password that you provided when you created the domain.

   To automate this step, see the WebLogic documentation:
   http://e-docs.bea.com/wls/docs81/ConsoleHelp/startstop.html#1203247

   Note: The first time you start the Identity Manager Server, Identity Manager's JSP files are precompiled. This can cause the initial start up to take some time.

   When you see the following message, the server has completed its startup process:
   <Server started in RUNNING mode>

Verify that Identity Manager Started

To verify that the Identity Manager Server has started successfully, you can access the Management Console.

Confirm the following:

- You can access the following URL from a browser:
  http://*im_fqdn*:*port*/idmmanage

  For example:
  http://MyServer.MyCompany.com:*port-number*/idmmanage
- The Management Console opens.
- No errors are displayed in the application server log.
- You do not receive an error message when you click the Directories link.

  Note: For details about the Management Console, see the *Configuration Guide*.

Advanced Configuration

You can now use the Management Console to do the following post-installation configurations:

- Deploy an Identity Manager Directory
- Configure an Identity Manager Environment

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

The remainder of this guide discusses optional features including the following:

- Protecting Identity Manager using a SiteMinder Policy Server
- Configuring provisioning
- Configuring email notification
- Configuring workflow
- Installing reporting
- Installing support for internationalization
- Reinstalling or removing Identity Manager
- Upgrading to Identity Manager r12 from previous versions of Identity Manager
- Creating unattended Identity Manager installations

Chapter 5: Protecting Identity Manager with SiteMinder

This section contains the following topics:

Installation Status

The following table shows you where you are in the installation process:

You Are Here	Step in Installation Process
	1. Install prerequisite hardware and software.
	2. Install Identity Manager components.
	3. Start Identity Manager.
X	**4. (Optional) Protect Identity Manager with SiteMinder.**
	5. (Optional) Configure provisioning.
	6. (Optional) Configure email notification.
	7. (Optional) Configure workflow.
	8. (Optional) Install reporting.
	9. (Optional) Configure internationalization.

How Resources are Protected

Advanced authentication requires you to use a SiteMinder Policy Server in your implementation.

In many situations, the application server hosting the Identity Manager Server is on a separate system from the one with the Web Server that proxies requests to the application server. To provide forwarding services, the Web Server needs the following:

- A plug-in that is provided by the application server vendor
- A SiteMinder agent to protect the Identity Manager resources, such as the User Console, Self Registration, and the Forgotten Password feature

The Web Agent controls the access of users who request Identity Manager resources. After authenticating and authorizing users, the Web Agent allows the Web Server to process the requests.

When the Web Server receives the request, the application server plug-in forwards it to the application server hosting the Identity Manager Server.

The Web Agent facilitates communication between the Identity Manager Server and the Policy Server and protects Identity Manager resources that are exposed to users and administrators.

How to Protect Identity Manager with SiteMinder

The following table describes the steps involved in protecting Identity Manager resources:

✓	Step
	1. Install and configure a SiteMinder Agent to protect Identity Manager resources.
	2. Install the plug-in the Web Server uses to forward requests to the application server.
	3. Verify that the plug-in is successfully forwarding requests to the application server.
	4. Configure the SiteMinder Policy Store for use with Identity Manager.

Install the SiteMinder Web Agent

You can use a SiteMinder Web Agent or a Web Agent Group to protect Identity Manager resources. For supported Web Agent versions, see the Identity Manager Platform Support Matrix on the Identity Manager support site http://ca.com/support.

Note: For more information about Web Agent groups, see the *CA SiteMinder Web Access Manager Policy Server Configuration Guide*.

Before installing the Web Agent, ensure the following requirements have been met:

- The SiteMinder Policy Server is installed and configured.
- The system that will host the Web Agent has network access to the Policy Server.
- The Web Server that will host the Web Agent is running.

The following table lists the steps to install and configure a SiteMinder Web Agent:

✓	Step	Refer to...
	1. Install and configure the Web Agent.	*CA SiteMinder Web Access Manager Web Agent Installation Guide*
	2. If you installed the Web Agent on an IIS Web Server, be sure to set the DefaultAgentName and DefaultPassword parameters of your Agent Configuration Object.	*CA SiteMinder Web Access Manager Web Agent Installation Guide*
	3. Enable the Web Agent.	*CA SiteMinder Web Access Manager Web Agent Installation Guide*
	4. If you are using an IIS web server, ensure the SiteMinder web agent ISAPI filter appears before any other filter, including the SePlugin filter, in the IIS console.	IIS documentation

To use the SiteMinder Web Agent to protect Identity Manager, select the Web Agent when you create an Environment. For instructions, see the *Configuration Guide*.

Note: You do not need to create any additional objects in SiteMinder to use the SiteMinder Web Agent.

To verify the Web Agent, confirm the following:

- The SiteMinder Policy Server Authentication and Authorization logs verify that the Web Agent starts properly.
- The Agent log for the Web Agent verifies that the Web Agent starts properly.

Install the Proxy Plug-In

Once the Web Agent authenticates and authorizes a request for an Identity Manager resource, the Web Server on which you installed the Web Agent must forward the request to the application server that hosts the Identity Manager Server. This is accomplished through a Web Server proxy plug-in provided by the application server vendor.

1. Install the WebLogic proxy plug-in for your Web Server as described in the WebLogic documentation. The documentation can be found at the following location:
   http://e-docs.bea.com/wls/docs81/plugins/index.html

   Note: For IIS users, when you install the proxy plug-in, be sure to configure proxying by file extension and by path. When you configure proxying by file extension, add an application mapping in the App Mapping tab with the following properties:
   Executable: IISProxy.dll
   Extension: .wlforward
2. Configure the proxy plug-in for Identity Manager as described in one of the following sections:
   - Configure the IIS Proxy Plug-in (see page 45)
   - Configure the iPlanet Proxy Plug-in (see page 45)
   - Configure the Apache Proxy Plug-in (see page 48)

Configure the IIS Proxy Plug-in

The proxy plug-in for IIS Web Servers requires an iisproxy.ini file. This file contains the specific parameters used by the plug-in to determine proxy behavior.

To use the WebLogic plug-in, edit the WlForwardPath parameter in the iisproxy.ini file that you created when you installed the proxy plug-in for IIS as follows:

```
WlForwardPath=/idm,/castylesr5.1.1
```

For example:

```
WebLogicHost=MyServer.MyCompany.com
WebLogicPort=7001
ConnectTimeoutSecs=20
ConnectRetrySecs=2
WlForwardPath=/idm,/castylesr5.1.1
WLLogFile=c:\temp\proxy.log
DebugConfigInfo=ON
```

For more information about the iisproxy.ini file, see BEA's documentation at the following location:

http://e-docs.bea.com/wls/docs81/plugins/isapi.html#112307

Configure the iPlanet Proxy Plug-in

To configure the plug-in, modify the following iPlanet configuration files:

- magnus.conf
- obj.conf

The iPlanet configuration files have strict rules about the placement of text. To avoid problems, note the following:

- Eliminate extraneous leading and trailing white space. Extra white space can cause your iPlanet server to fail.
- If you must enter more characters than you can fit on one line, place a backslash (\) at the end of that line and continue typing on the following line. The backslash directly appends the end of the first line to the beginning of the following line. If a space is necessary between the words that end the first line and begin the second line, be certain to use one space, either at the end of the first line (before the backslash), or at the beginning of the second line.
- Do not split attributes across multiple lines.

The iPlanet configuration files for your iPlanet instance are found in the following location:

iplanet_home/https-*instance_name*/config/

where *iplanet_home* is the root directory of the iPlanet installation, and *instance_name* is the particular server configuration that you are using.

To install the proxy plug-in on an iPlanet Web Server

1. From the *weblogic_home*/server/lib directory, copy the libproxy.so file that corresponds to your version of your iPlanet Web Server to the file system where you installed iPlanet.
2. In a text editor, modify the iPlanet magnus.conf file.

   To instruct iPlanet to load the libproxy.so file as an iPlanet module, add the following lines to the beginning of the magnus.conf file:

   ```
   Init fn="load-modules" funcs="wl_proxy,wl_init"\
   shlib=path in file system from step 1/libproxy.so
   Init fn="wl_init"
   ```

   For example:

   ```
   Init fn="load-modules" funcs="wl_proxy,wl_init"\
   shlib=/usr/local/netscape/plugins/libproxy.so
   Init fn="wl_init"
   ```

   The function load-modules tags the shared library for loading when iPlanet starts up. The values wl_proxy and wl_init identify the functions that the plug-in executes.

3. In a text editor, modify the iPlanet obj.conf file as follows:

   a. After the last line that begins with the following:

      NameTrans fn=....

      Add the following Service directive to the Object name="default" section:

      ```
      Service method="(GET|HEAD|POST|PUT)" type=text/jsp fn="wl-proxy"
      ```

      Note: You may add this directive in a line following existing Service directives.

   b. Add the following to the end of the file:

   ```
   <Object name="idm" ppath="*/idm*">
   Service fn="wl-proxy" WebLogicHost="hostname" WebLogicPort="portnumber" PathTrim="/weblogic"
   </Object>
   <Object name="weblogic1" ppath="*/console*">
   Service fn="wl-proxy" WebLogicHost="hostname" WebLogicPort="portnumber" PathTrim="/weblogic"
   </Object>
   ```

      where *hostname* is the server name and domain of the system where you installed WebLogic, and *portnumber* is the WebLogic port (default is 7001).

      You may have more than one Object entry.

   For example:

   ```
   <Object name="idm" ppath="*/idm*">
   Service fn="wl-proxy" WebLogicHost="MyServer.MyCompany.com" WebLogicPort="7001"
   PathTrim="/weblogic"
   <Object name="weblogic1" ppath="*/console*">
   Service fn="wl-proxy" WebLogicHost="MyServer.MyCompany.com" WebLogicPort="7001"
   PathTrim="/weblogic"
   </Object>
   ```

4. Save your iPlanet configuration file.

5. Restart your Web Server instance.

Configure the Apache Proxy Plug-in

1. After installing a Web Agent on Solaris, stop the Apache web server and copy the mod_wl_20.so file from the following location:
   weblogic_home/server/lib/solaris

   to
   apache_home/modules
2. Edit the http.conf file (located in *apache_home*/conf) and make the following changes:
   a. Under the load module section, add the following:
      LoadModule weblogic_module modules/mod_wl_20.so
   b. Edit the server name with the name of the Apache server system.
   c. Add an If block at the end of the file as follows:
      <IfModule mod_weblogic.c>
      WebLogicHost *my_weblogic_server*.com
      WebLogicPort 7001
      MatchExpression /idm
      MatchExpression /castylesr5.1
      </IfModule>
3. Save the http.conf file.
4. Restart the Apache web server.

For more information about the http.conf file, see BEA's documentation at the following locations:

WebLogic 8:
http://e-docs.bea.com/wls/docs81/plugins/apache.html

WebLogic 9:
http://e-docs.bea.com/wls/docs90/plugins/apache.html

Verify the Web Agent and Connector

The Identity Manager Server installation contains a JSP page that you can use to verify that the application server connector is successfully forwarding requests to the application server.

In a browser, enter the following URL:
http://*web_server_hostname*/idm/ui/ping.jsp

For example:
http://MyServer.MyCompany.com/idm/ui/ping.jsp

If your application server connector is functioning, you will receive a JSP page with an initial heading of Request Information. This page provides details about the processing of the request for the JSP page.

If the Web Agent you created is functioning correctly, information similar to the following will appear under Request Headers in the page displayed in your browser:

SM_AUTHTYPE = Not Protected
SM_DOMAIN = *your_domain*
SMTRANSACTIONID = *some_system-generated_id*

For example:

SM_AUTHTYPE = Not Protected
SM_DOMAIN = *.MyCompany.com*
SMTRANSACTIONID = *41041aac-04ec-3edbc669-0a70-012d19d9*

Configure the Policy Store for Identity Manager

Once you install the Identity Manager Extensions for SiteMinder on the system with the Policy Store, extend the policy store schema for Identity Manager.

To extend the schema to the policy store, use the Identity Manager Administrative Tools. Install the tools using the Identity Manager installation program, without installing the Identity Manager server.

Configure a Relational Database

To configure a relational database policy store

1. Configure the directory as a supported SiteMinder Policy Store.

   Note: Be sure that SiteMinder is pointing to this policy store. For configuration instructions, see the *CA SiteMinder Web Access Manager Policy Server Installation Guide.*

2. Run one of the following scripts for Identity Manager on the Policy Store database:

   - **SQL:** C:\Program Files\CA\IAM Suite\Identity Manager\tools\policystore-schemas\MicrosoftSQLServer\ims8_mssql_ps.sql
   - **Oracle:** HOME/CA/IAM_Suite/Identity_Manager/tools\policystore-schemas/OracleRDBMS/ims8_oracle_ps.sql

Configure Sun Java Systems Directory Server or IBM Directory Server

To configure a Sun Java Systems Directory or IBM Directory policy store

1. Configure the directory as a supported SiteMinder Policy Store.

   Note: Be sure that SiteMinder is pointing to this policy store. For configuration instructions, see the *CA SiteMinder Web Access Manager Policy Server Installation Guide.*

2. Add the appropriate LDIF schema file from the following table to the directory. The LDIF files are located in C:\Program Files\CA\IAM Suite\Identity Manager\tools\policystore-schemas.

   For information on adding schema files, see the following documentation for your directory:

   - **IBM Directory Server:**
     IBMDirectoryServer\V3.identityminder8
   - **Sun Java Systems Directory Server (iPlanet):**
     SunJavaSystemDirectoryServer\sundirectory_ims8.ldif

Configure Microsoft Active Directory

To configure a Microsoft Active Directory policy store, you apply the activedirectory_ims8.ldif script.

To configure an Active Directory policy store

1. Configure the directory as a supported SiteMinder Policy Store.

   Note: Be sure that SiteMinder is pointing to this policy store. For configuration instructions, see the *CA SiteMinder Web Access Manager Policy Server Installation Guide.*

2. Modify the activedirectory_ims8.ldif schema file as follows:

   a. In a text editor, open the following file:

      C:\Program Files\CA\IAM Suite\Identity Manager\tools\policystore-schemas\MicrosoftActiveDirectory\
      activedirectory_ims8.ldif

   b. Replace all instances of {root} with the root organization for the directory.

      The root organization must match the root organization that you specified when you configured the policy store in the Policy Server Management Console.

      For example, if the root is dc=myorg,dc=com, replace
      dn: CN=imdomainid6,CN=Schema,CN=Configuration,{root} with dn: CN=imdomainid6,CN=Schema,CN=Configuration,dc=myorg,dc=com

   c. Save the file.

3. Add the schema file as described in the documentation for your directory.

Configure Microsoft ADAM

To configure a Microsoft ADAM policy store, you apply the adam_ims8.ldif script.

To configure a Microsoft ADAM policy store

1. Configure the directory as a supported SiteMinder Policy Store.

   Note: Be sure that SiteMinder is pointing to this policy store. For configuration instructions, see the *CA SiteMinder Web Access Manager Policy Server Installation Guide.*

2. Modify the adam_ims8.ldif schema file as follows:

   a. In a text editor, open this file:

      C:\Program Files\CA\IAM Suite\Identity Manager\tools\policystore-schemas\MicrosoftADAM\
      adam_ims8.ldif\

   b. Replace every cn={guid} reference with the string you found when you configured the SiteMinder policy store in Step 1 of this procedure.

      For example, if the guid string is CN={39BC711D-7F27-4311-B6C0-68FDEE2917B8}, then replace every cn={guid} reference with CN={39BC711D-7F27-4311-B6C0-68FDEE2917B8}.

   c. Save the file.

3. Add the schema file as described in the documentation for your directory.

Configure eTrust Directory Server

To configure an eTrust Directory policy store

1. Configure the directory as a supported SiteMinder Policy Store.

   Note: Be sure that SiteMinder is pointing to this policy store. For configuration instructions, see the *CA SiteMinder Web Access Manager Policy Server Installation Guide.*

2. Copy etrust_ims8.dxc from C:\Program Files\CA\IAM Suite\Identity Manager\tools\policystore-schemas\eTrustDirectory to *dxserver_install*\config\schema

   where *dxserver_install* is the directory where eTrust Directory is installed.

3. Create a custom schema configuration file as follows:

   a. Copy the *dxserver_install*\config\schema\default.dxg to *dxserver_install*\config\schema*company_name*-schema.dxg.

   b. Edit the *dxserver_install*\config\schema*company_name*-schema.dxg file by adding the following lines to the bottom of the file:

   ```
   # Identity Manager Schema
   source "etrust_ims8.dxc";
   ```

4. Edit the *dxserver_install*\bin\schema.txt file by adding the contents of C:\Program Files\CA\IAM Suite\Identity Manager\tools\policystore-schemas\eTrustDirectory\
   etrust_ims_schema.txt to the end of the file.

5. Create a custom limits configuration file as follows:

   a. Copy the *dxserver_install*\config\limits\default.dxc to *dxserver_install*\config\limits*company_name*-limits.dxc.

   b. Increase the default size limit to 5000 in the *dxserver_install*\config\limits*company_name*-limits.dxc file as follows:

   ```
   set max-op-size=5000
   ```

6. Edit the *dxserver_install*\config\servers*dsa_name*.dxi as follows:

   ```
   # schema
   source "company_name-schema.dxg";

   #service limits
   source "company_name-limits.dxc";
   ```

   where *dsa_name* is the name of the DSA using the customized configuration files.

7. Run the dxsyntax command.

   This utility will report any errors with the directory configuration. If this utility runs with no errors, continue to Step 8.

8. Stop and restart the eTrust DSA as the dsa user to make the schema changes take effect, as follows:

   ```
   dxserver stop dsa_name
   dxserver start dsa_name
   ```

Configure Novell eDirectory Server

To configure an Novell eDirectory Server policy store, you apply the novell_ims8.ldif script.

To configure an Novell eDirectory policy store

1. Configure the directory as a supported SiteMinder Policy Store.

   Note: Be sure that SiteMinder is pointing to this policy store. For configuration instructions, see the *CA SiteMinder Web Access Manager Policy Server Installation Guide.*

2. Find the DN of the NCPServer for your Novell eDirectory Server by entering the following information in a command window on the system where the Policy Server is installed:
   ldapsearch -h *host* -p *port_number* -b *container* -s sub
   -D *admin_login* -w *password* objectClass=ncpServer dn

   For example:
   ldapsearch -h 192.168.1.47 -p 389 -b "o=nwqa47container" -s sub -D "cn=admin,o=nwqa47container" -w password objectclass=ncpServer dn

3. Open the novell_ims8.ldif file.

4. Replace every NCPServer variable with the value you found in Step 2.

   The novell_ims8.ldif is located in:
   C:\Program Files\CA\IAM Suite\Identity Manager\tools\policystore-schemas\NovelleDirectory\

   For example, if the DN value is cn=servername,o=servercontainer, you would replace every instance of *NCPServer* with cn=servername,o=servercontainer.

5. Update the eDirectory Server with the novell_ims8.ldif file.

   See the Novell eDirectory documentation for instructions.

Configure Oracle Internet Directory (OID)

To configure an Oracle Internet Directory policy store

1. Configure the directory as a supported SiteMinder Policy Store.

   Note: Be sure that SiteMinder is pointing to this policy store. For configuration instructions, see the *CA SiteMinder Web Access Manager Policy Server Installation Guide.*

2. Update the Oracle Internet Directory Server with the oracleoid_ims8.ldif file, which is located in the following directory:
   C:\Program Files\CA\IAM Suite\Identity Manager\tools\policystore-schemas\OracleOID\

   See the Oracle Internet Directory documentation for instructions.

3. Start the Policy Server services as follows:
   a. Open the Policy Server Management Console.
   b. Click the Update button in the console and verify that the services started successfully.

Note: If you experience a timeout when searching for Admin roles using the wildcard (*) character, create a SearchTimeout string value in the LdapPolicy key in the registry. Set the value to a number greater than 20 seconds, which is the default search timeout, then restart the Policy Server services.

To access the registry on Windows, open Start, Run. Enter REGEDT32 in the Run window. On Solaris, open *siteminder_installation*/registry/sm.registry.

The LdapPolicy key is located in:
HKEY_LOCAL_MACHINE\SOFTWARE\Netegrity\SiteMinder\CurrentVersion\Ds\

Verify the Policy Store

To verify the policy store, confirm the following:

- Your Policy Server log does not contain a section of warnings that begins with the following:
  *** IMS NO SCHEMA BEGIN

  Note: For SiteMinder r6.x, check smps.log.

  This warning appears only if you have installed the Identity Manager Extensions for the SiteMinder Policy Server, but you have not extended the Policy Store schema.
- The Identity Manager objects exist in the policy store database or directory. The Identity Manager objects begin with an ims prefix.

Chapter 6: Configuring Provisioning

This section contains the following topics:

Installation Status

The following table shows you where you are in the installation process:

You Are Here	Step in Installation Process
	1. Install prerequisite hardware and software.
	2. Install Identity Manager components.
	3. Start Identity Manager.
	4. (Optional) Protect Identity Manager with SiteMinder.
X	**5. (Optional) Configure provisioning.**
	6. (Optional) Configure email notification.
	7. (Optional) Configure workflow.
	8. (Optional) Install reporting.
	9. (Optional) Configure internationalization.

Important Notes for Provisioning Installation

If you want to implement provisioning within your Environment, review the following process for the high-level steps:

1. Install eTrust Directory on a different system from the one where you plan to install the Identity Manager Server and the Provisioning Server. For a list of supported versions of eTrust Directory, see the Identity Manager Support Matrix on the Identity Manager support site http://ca.com/support. You can also download eTrust Directory from this site (a license for eTrust Directory is included with Identity Manager).
2. Run the Identity Manager installer to run the Provisioning Directory Initialization on the system where eTrust Directory is installed.

   This will set up your directory for provisioning.
3. Run the Identity Manager installer to install the Identity Manager Server and the Provisioning Server on the system where a supported application server is installed.

   Important! You must be logged in as a Local Administrator for the Provisioning Server installation.
4. Access the Management Console and configure it for provisioning.

   Note: For more information about configuring the Management Console for provisioning, see the *Provisioning Guide*.
5. Configure the Provisioning Manager.
6. Consider optional provisioning components for installation.

How to Configure Provisioning

Perform the following steps to configure Identity Manager provisioning:

	Step
	1. If your Provisioning Server is remote (not on the same system as the Provisioning Manager), run the Provisioning Manager setup.
	2. Configure the Identity Manager Server and notifications within the Provisioning Manager.
	3. Consider optional Provisioning Components to install.

Provisioning Manager Setup

If your Provisioning Server is remote (not on the same system as the Provisioning Manager), run the Provisioning Manager setup.

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

To run the Provisioning Manager setup

1. Go to Start, Programs, CA, Identity Manager, Provisioning Manager Setup
2. Enter the hostname of the Provisioning Server.

   Note: You must use the hostname, entering localhost or an IP will not work.
3. Click Configure.
4. Click Ok.

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

Configure the Provisioning Manager

Set up the Identity Manager Server and enable inbound synchronization in the Provisioning Manager.

To configure the Provisioning Manager

1. Go to Start, Programs, CA, Identity Manager, Provisioning Manager
2. Log in to the Provisioning Manager using the global username and password you provided while installing the Identity Manager Administrative Tools.
3. Click System.
4. Click Identity Manager Setup on the left.
5. Enter the hostname, port number and environment alias for the Identity Manager server.
6. Click Add.
7. Click Apply.

   Note: If you get a shared secret error, re-enter the password under Shared Secret and Confirm Shared Secret and click Apply again.
8. Click Domain Configuration on the left.
9. Expand the Identity Manager Server folder and click Enable Notification.

10. Click Edit.
11. Change the value to Yes.
12. Click Apply.
13. Restart the Provisioning Server.

Optional Provisioning Components

Once you've installed Identity Manager with Provisioning, you can do the following post-installation configurations:

- Configure Endpoint Types
- Acquire Endpoints

Optional components for Identity Manager provisioning include the following:

- GINA
- Password Synchronization Agent
- Credential Provider
- Connector Server Framework

Note: For more information on advanced provisioning topics, see the *Provisioning Guide*.

Java Connector Server

The *Java Connector Server (Java CS)* is a server component which handles hosting, routing to, and management of Java connectors. The Java CS provides a Java alternative to the C++ Connector Server. It is architecturally and functionally similar to the C++ Connector Server, except that it has a Java API instead of a C++ API, which allows your connectors to be implemented in Java. In addition, the Java CS is data-driven rather than code-driven, which allows more functionality to be addressed by the container (or Java CS) instead of by connectors themselves.

The Provisioning Server handles provisioning of users, and then delegates to connectors (using the C++ Connector Server or Java Connector Server) to manage endpoint accounts, and groups.

Note: For more information on the Java Connector Server, see the *Java Server Connector (JCS) Implementation Guide*.

Connectors

Before you can acquire any endpoint, first install the endpoint connector that manages that kind of endpoint. In some cases, you must install an agent on each system you manage.

Provisioning connectors run on the Provisioning Server and communicate with the systems managed by an endpoint in a domain. For example, machines running Advanced Directory Services (ADS) can be managed only if the ADS Connector is installed on the Provisioning Server.

Some of the connectors have prerequisites that you must meet before you can successfully install them. See the connector guides to review the prerequisites for connectors you want to install.

By default, Identity Manager configures the following connectors during installation:

- Active Directory Services
- Unix ETC
- Generic LDAP
- Universal Provisioning
- Windows NT
- MS-SQL Server

Note: For more information about each connector, see the corresponding Connector Guide.

High Availability

Note: For more information on implementing a high-availability environment, see the *High Availability Guide*.

Chapter 7: Configuring Email Notification

This section contains the following topics:

Installation Status

The following table shows you where you are in the installation process:

You Are Here	Step in Installation Process
	1. Install prerequisite hardware and software.
	2. Install Identity Manager components.
	3. Start Identity Manager.
	4. (Optional) Protect Identity Manager with SiteMinder.
	5. (Optional) Configure provisioning.
X	**6. (Optional) Configure email notification.**
	7. (Optional) Configure workflow.
	8. (Optional) Installing reporting.
	9. (Optional) Configure internationalization.

How to Configure Email Notification

The following checklist describes the steps to configure Identity Manager's email notification feature:

✓	Step
	1. Configure SMTP for the application server.
	2. Enable email notification through the Management Console

WebLogic 8.1: Configure SMTP Settings

You configure email settings in the WebLogic Console and in an email.properties file.

To configure email settings for WebLogic 8.1

1. In the WebLogic Console, set the mail.smtp.host property to your SMTP server by replacing @SMTP with your SMTP server name.

   For example:
   mail.smtp.host=mymailserver.company.com

2. In a text editor, open the following email properties file for Identity Manager:
   weblogic_domain\applications\IdentityMinder.ear\config\com\netegrity\config\email.properties

3. Set the email return address used by workflow generated email by locating the admin.email.address property and setting the value to the appropriate email address. For example:
   admin.email.address=admin@company.com

4. Enable email notification in the Management Console.

WebLogic 9.2: Configure SMTP Settings

You configure email settings in the WebLogic Console and in an email.properties file.

To configure email settings for WebLogic 9.2

1. In the WebLogic Console, create a new mail session with the following properties:
   - **mail.smtp.host** property: Set this value to your SMTP server. For example, mail.smtp.host=mymailserver.company.com
   - **mail.transport.protocol** property: Set this value to SMTP. For example, mail.transport.protocol=smtp
   - **JNDI Name**: nete/Mail
   - **Target**: the WebLogic server name
2. In a text editor, open the following email properties file for Identity Manager:
   weblogic_domain\applications\IdentityMinder.ear\config\com\netegrity\config\email.properties
3. Set the email return address used by workflow generated emails by locating the admin.email.address property and setting the value to the appropriate email address. For example:
   admin.email.address=admin@company.com
4. Enable email notification in the Management Console.

Enable Email Notification

Perform the following procedure to configure email notification.

To enable email notification for an Identity Manager environment

1. In the Environments screen, click the name of the appropriate Environment.

   The Identity Manager environment Properties screen opens.
2. Click Advanced Settings, Email.

   The Email Properties screen opens.

3. To enable email notification for the Identity Manager environment, select the Enable check boxes that apply:

   - Events E-mail Enabled

     Enables email notification for Identity Manager events

   - Tasks Email Enabled

     Enables email notification for Identity Manager tasks

   Note: For more information on event and task level email notifications, see the *Administration Guide*.

4. Enter the location of the email templates that Identity Manager uses to create the email messages.

   The email templates are located in a subdirectory in the following location:
   IdentityMinder.ear\custom\emailTemplates

   Note: When you create an email template file with a file name using a different language, the operating system session should be operating in a language that supports the character set. For more information on deploying custom email templates, see the *Administration Guide*.

5. Specify the events for which email notifications are sent as follows:

   - To add an event, select the event in the Event list box, and click Add.

     Identity Manager adds the event you selected to the list of events for which email notifications are sent.

     Note: If you select an event that is not associated with a workflow process, Identity Manager sends an email notification when the event completes.

   - To delete an event, select the event's check box, then click Delete.

6. Specify the tasks for which email notifications are sent as follows:

   - To add a task, search for the task by selecting a condition in the first field, and entering a task name in the second field. Click Search.

     You can enter a partial task name by using the wildcard (*) character. For example, to search for a Create task, enter Create*.

     Select one or more tasks from the search results. Click Add.

     Note: Task-level email notifications are not available for tasks that have the action type View or Self View. To see the action type of a task, go to Modify Admin Task, Select a Task, and check the action field in the task profile.

   - To delete a task, select the task's check box, then click Delete.

     Deleting a task removes the task from the Task table. It does not delete the task.

Chapter 8: Configuring Workflow

This section contains the following topics:

Installation Status

The following table shows you where you are in the installation process:

You Are Here	Step in Installation Process
	1. Install prerequisite hardware and software.
	2. Install Identity Manager components.
	3. Start Identity Manager.
	4. (Optional) Protect Identity Manager with SiteMinder.
	5. (Optional) Configure provisioning.
	6. (Optional) Configure email notification.
X	**7. (Optional) Configure workflow.**
	8. (Optional) Installing reporting.
	9. (Optional) Configure internationalization.

How to Configure Workflow

The following checklist describes the steps to configure Identity Manager's workflow feature:

✓	Step
	1. Enable workflow in the Management Console
	2. (Optional) Configure WorkPoint Administrative Tools if you plan to use WorkPoint Designer.

Enable Workflow

To enable workflow, use the Management Console.

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

To enable workflow in the Management Console

1. Run the Management Console.
   http://*im_fqdn*:*port*/idmmanage
2. Select an Environment.
3. Select Advanced Settings.
4. Select Workflow.
5. Check Enable.
6. Click Save.
7. Restart the application server.

After you enable workflow, you can find information about how to use Identity Manager's workflow features in the *Administration Guide*.

Configure WorkPoint Administrative Tools

WorkPoint Designer is software from Insession Technologies that is integrated with Identity Manager. WorkPoint Designer lets you manage workflow processes and workflow jobs.WorkPoint Administrative Tools include WorkPoint Designer and WorkPoint Archive. In order to configure WorkPoint Administrative Tools, install the Identity Manager Administrative Tools. If you have not installed the Identity Manager Administrative Tools, you can run the installer and select the Identity Manager Administrative Tools option.

Note: To use the Administrative Tools for workflow, a supported JDK must be installed on the system where the Administrative Tools are installed. For a complete list of supported platforms and versions, see the Identity Manager Support Matrix on the Identity Manager support site http://ca.com/support.

The workflow client tools are located in:

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

The tools in this directory allow you to do the following:

- Create the workflow database schema
- Load the default workflow scripts
- Design and monitor Workflow processes and jobs

Edit init.bat/init.sh

To edit init.bat/init.sh

1. In a text editor, edit one of the following files:
   - **Windows:**
     C:\Program Files\CA\IAM Suite\Identity Manager\tools\Workpoint\bin\init.bat
   - **UNIX:**
     HOME/CA/IAM_Suite/Identity_Manager/tools/Workpoint/bin/init.sh
2. Uncomment the following line in the section for WebLogic application servers.
   - **Windows:**
     SET EJB_CLASSPATH=..\lib\wlclient.jar
   - **UNIX:**
     EJB_CLASSPATH=../lib/wlclient.jar

   Note: Make sure that all sections for other application servers are commented.
3. Copy the wlclient.jar file from *wl_home*\server\lib to the following location:
   C:\Program Files\CA\IAM Suite\Identity Manager\tools\Workpoint\lib\

Edit workpoint-client.properties

You must edit the workpoint-client.properties file based on the type of application server you selected during the Identity Manager installation.

To configure the workpoint-client.properties file

1. Open C:\Program Files\CA\IAM Suite\Identity Manager\tools\Workpoint\conf\ workpoint-client.properties in a text editor.
2. Locate the section titled BEA WEBLOGIC.
3. Uncomment all of the property values in that section.

   For example:
   java.naming.factory.initial=weblogic.jndi.WLInitialContextFactory
   java.naming.provider.url=t3://*im_fqdn*:*port*
   java.naming.security.principal=IDM
   java.naming.security.credentials=password
4. Save the file.

   Note: The java.naming.provider.url property must point to the fully-qualified domain name and WebLogic port number of the system on which you installed the Identity Manager Server.

Chapter 9: Installing Reporting

This section contains the following topics:

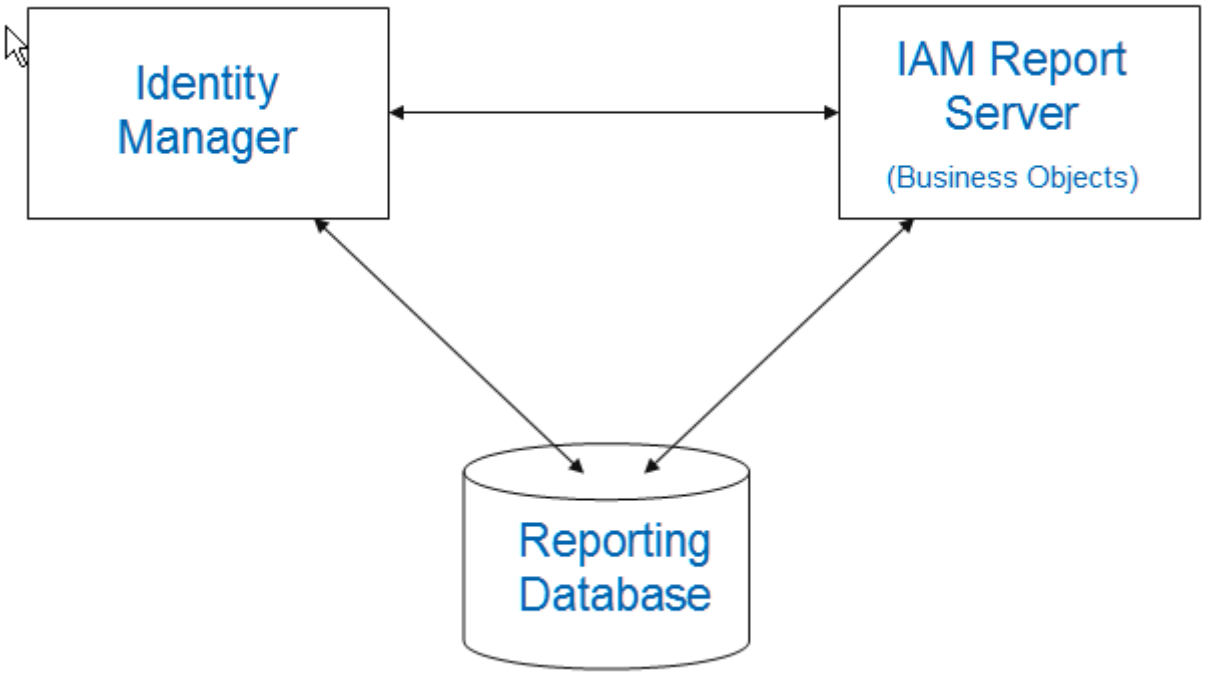
Installation Status

The following table shows you where you are in the installation process:

You Are Here	Step in Installation Process
	1. Install prerequisite hardware and software.
	2. Install Identity Manager components.
	3. Start Identity Manager.
	4. (Optional) Protect Identity Manager with SiteMinder.
	5. (Optional) Configure provisioning.
	6. (Optional) Configure email notification.
	7. (Optional) Configure workflow.
X	**8. (Optional) Install reporting.**
	9. (Optional) Configure internationalization.

Reporting Architecture

In Identity Manager, the reporting setup requires the three major components in the following diagram:



IAM Report Server

Also known as the Business Objects Server. This is the engine behind the generation ofreports for Identity Manager. It communicates directly with Identity Manager and the Reporting Database.

Identity Manager

Identity Manager allows you to export Identity Manager object data to the Reporting Database.

Reporting Database

A separate database containing the snapshot data of objects in Identity Manager

Important! The IAM Report Server is powered by Business Objects Enterprise XI. If you already have an IAM Report Server in your environment and want to use it with Identity Manager, the minimum version required by Identity Manager is Business Objects XI r2 sp2.

Reporting Considerations

Consider the following before installing the report server:

- Installing the report server requires approximately 4 GB of free disk space.
- Installing the report server can take up to two hours.

Hardware Requirements

The following requirements must be met for the IAM Report Server to install and run correctly in the following environments:

Important! Business Objects Enterprise XI software is supported on Windows only for the 32-bit AMD and Intel chipsets.

Windows

- Processor: P3, 700 MHz
- Physical Memory: 2 GB is recommended
- Disk Space: 5 GB for Business Objects and 1.5 GB for Performance Management
- Drives: CDROM

Solaris 8, 9

- Processor: SPARC v8plus
- Physical Memory: 2 GB is recommended
- Disk Space: 4 GB for Business Objects full install

Note: For information regarding supported OS versions and databases, see the Business Objects web site http://support.businessobjects.com/documentation/.

How to Install Reporting

The following checklist describes the steps to install Identity Manager's reporting feature:

✓	Step
	1. Ensure you have reviewed the reports pre-installation checklist.

✓	Step
	2. Gather reporting information.
	3. Install the IAM Report Server (Business Objects)
	4. Copy the jdbc JAR files.
	5. Run the command line to deploy the default reports.

Note: For more information on configuring reporting after the installation, see the *Administration Guide*.

Reports Pre-Installation Checklist

You may want to print the following to use as a checklist to help ensure you meet the minimum system and database requirements before installing the report server:

- ☐ Ensure that the Windows or UNIX system to which you are installing the report server meets the minimum system requirements.
- ☐ Ensure that you are using a supported version of MS SQL Server or Oracle database for the report database.
- ☐ If you are using MS SQL Server as a report database, create a data source name (DSN) that the report server is to use to communicate with the report database.
- ☐ If you are using Oracle as a report database, create a transparent network substrate (TNS) that report server is to use to communicate with the report database.
- ☐ (UNIX) Set the following parameters:
  - Oracle_Home=*oracle_root*

  oracle_root

  Specifies the path to the Oracle root.
  - LD_LIBRARY_PATH=$ORACLE_HOME/lib32:$ORACLE_HOME/lib
  - ORACLE_SID=*SID_name*

  SID_name

  Specifies the SID name used in the tnsnames.ora file.

- JAVA_HOME=*JAVA_root*

JAVA_root

Specifies the path to the Java Root. Business Objects installs a JDK in the following location:
IAM_Report_Server_Root_Folder/j2sdk1.4.2_08

- PATH=$LD_LIBRARY_PATH:$JAVA_HOME:$JAVA_HOME/bin:$ORACLE_HOME/bin:$PATH
- LC_ALL=en_US.UTF-8

☐ (UNIX) Ensure that you have access to a non-root user account. You cannot use a root-user account to install the report server.

Reporting Information

Record the following information you need during the IAM Report Server installation:

Field Name	Description	Your Response
Report Server Administrator Password	The installer automatically creates an administrator account for the IAM Report Server. Determine the password for this account.	
Database Host Name and Port	Identify the server where the Reporting Database is installed.	
DSN Name	Identify the name of the DSN that the report server is to use to communicate with the Reporting Database.	
Database Name	Identify the Reporting Database name.	
Database Username	Identify the username for the Reporting Database.	
Database Password	Identify the administrative password credentials for the Reporting Database.	

Field Name	Description	Your Response
TNS Name	The name of the TNS that the IAM Report Server is to use to communicate with the Reporting Database. **Note:** This information is needed only if you are using Oracle.	
Pre-Installed Tomcat Information	Identify the path and port numbers for any previous installation of Tomcat. If you do not want to use a previous installation of Tomcat, IAM Report Server installer can install Tomcat.	
Tomcat Port Number	The Tomcat connection, redirect, and shutdown ports. **Note:** If you are installing the IAM Report Server on the same system as the Identity Manager, ensure that the Tomcat connection port does not conflict with the port number you specified for the application server URL when installing the Identity Manager.	

Install the IAM Report Server

You can install the report server on a supported Windows or UNIX system. The following sections detail how to install the report server using a Windows and UNIX installation wizard, as well as a UNIX console.

Important! For a production environment, install the the IAM Report Server on a separate system from the Identity Manager Server. If you want to install the IAM Report Server on the same system as the Identity Manager Server for demonstration purposes, choose non-default ports for 8080 and 1099.

The IAM Report Server is powered by Business Objects Enterprise XI.

Run the Windows Installer

Install the IAM Report Server using the Windows installation wizard (ca-wamui-12.0-win32.exe) found on the Identity Manager media.

To install the IAM Report Server

1. Exit all applications.
2. Open the win32 folder.
3. If the installer does not automatically start, double-click ca-iamreportserver-12.0-win32.exe.

   The installation wizard starts.
4. Use the gathered reporting information to install the report server.

   Note: If you are installing the IAM Report Server on the same system as Identity Manager, ensure that the Tomcat connection port does not conflict with the port number you specified for the application server URL when installing Identity Manager.
5. Review the installation settings and click Install.

   The IAM Report Server is installed.

Run the UNIX Installer

You install the IAM Report Server using the UNIX installation wizard (ca-iamreportserver-12.0-sol.bin) found on the Identity Manager media.

Note: You may need to add executable permissions to the install file by running the following command:

```
chmod+x ca-iamreportserver-12.0-sol.bin
```

Important! The installer may crash if you execute it across different subnets. To avoid this problem, install the IAM Report Server directly on the host machine.

To install the IAM Report Server

1. Exit all applications.
2. Open a command window and navigate to where the install program is located.
3. Enter the following command:

   ```
   sh./ca-iamreportserver-12.0-sol.bin
   ```

   The installation wizard starts.
4. Use the gathered reporting information to install the report server.

Note the following:

- The installer installs the report server to /opt/CA/SharedComponents/CommonReporting. Specifying another location will not change the installation location. The /opt/CA directory must have non-root user permissions or the installation fails.
- If you are installing the IAM Report Server on the same system as Identity Manager, ensure that the Tomcat connection port does not conflict with the port number you specified for the application server URL when installing Identity Manager.

5. Review the installation settings and click Install.

   The IAM Report Server is installed.

6. Click Done and reboot the system.

Copy the JDBC JAR Files

To copy the jdbc JAR files

1. Navigate to the C:\Program Files\CA\IAM Suite\Identity Manager\tools\lib\jdbcdrivers folder on the Identity Manager Installer media.
2. Copy one of the following JAR files to *report_server_home*/common/3.5/java/lib:
   - **SQL:** sqljdbc.jar
   - **Oracle:** ojdbc14.jar
3. In *report_server_home/*common/3.5/java, open the CRConfig.xml file.
4. Add the location of the jdbc JAR files to the Classpath. For example, if you are using an MS SQL database, your Classpath would look like the following:
   <Classpath>C:*report_server_home*\common\3.5\java\lib\sqljdbc.jar;…</Classpath>
5. Save the file.
6. Restart the IAM Report Server as follows:
   a. Go to Start, CA, IAM Report Server, Central Configuration Manager.

      The Central Configuration Manager opens.

   b. Select all services and click Restart.

Deploy Default Reports

Identity Manager comes with default reports you can use for reporting.

To deploy the default reports

1. Unzip the importbiarfilestool.zip file on the machine where the IAM Report Server is installed. This tool can be found in the following location:
   C:\Program Files\CA\IAM Suite\Identity Manager\tools\BIARTool

   Note: Unzip from the root drive.

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

   Provide the following information needed to import the default reports:

   - IAM Report Server Root Folder—root of the business objects install folder, for example, c:/Program Files/CA/IAM Report Server
   - Reporting Database Type—1=MSSQL, 2=Oracle

     Note: This is *not* the Identity Manager database.
   - IAM Report Server Administrator Name—The default is Administrator. If you have a different administrator name, provide it here.
   - Reporting Database User—user created for the Reporting Database
   - Reporting Database Password—password for the user created in Reporting Database
   - Reporting Database DSN Name—the ODBC DSN name created
   - Reporting Database Name—the Reporting Database name
   - Reporting System Password—reporting administrator's password entered during the installation

- BIAR File Location—use one of the following:
  - C:\Program Files\CA\IAM Suite\Identity Manager\tools\imrexport\ReportDefinitions\IM Standard Reports\Ms-SQL_Reports\ms-sql_reports.biar
  - C:\Program Files\CA\IAM Suite\Identity Manager\tools\imrexport\ReportDefinitions\IM Standard Reports\Oracle Reports\oracle_reports.biar
- Platform—1=Windows, 2=Solaris

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

Note: After the import completes, you will be 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.

Verify the Reporting Installation

To ensure that reporting has been installed correctly, do the following:

- In the Central Configuration Manager, ensure that all services are running.
- Ensure that your reporting database is running.

Note: For more information on configuring reporting after the installation, see the *Administration Guide*.

How to Uninstall the Report Server

Complete the following procedures to uninstall the report server:

1. Uninstall the report server.
2. Remove leftover items.

Uninstall the Report Server from Windows

You uninstall the report server when it is no longer required on the system.

To uninstall the report server

1. Click Start, Settings, Control Panel.

   The Control Panel opens.

2. Double-click Add/Remove Programs.

   A list of currently installed programs appears.

3. Select IAM Report Server, and click Change/Remove

   A wizard to uninstall the report server starts.

4. Follow the instructions and prompts in the wizard.

   Note: If the system displays a remove shared file message, click No to All.

5. If requested, reboot the system.

   The report server is uninstalled.

Uninstall the Report Server from UNIX

You uninstall the report server when it is no longer necessary on the system.

To uninstall the report server on UNIX

1. Change to the following directory in a console window:

   report_server_install

   report_server_install

   Specifies the report server installation path.

2. Run the following command:

   ./iam-report-server-uninstall.sh

   The uninstallation program appears.

3. Press Enter.

   A status indicator shows the report server is being uninstalled and prompts successful completion.

Remove Leftover Items

The following sections detail the items you must manually remove after uninstalling the report server to keep the system as clean as possible and to prevent a reinstallation of the report server to the same machine from failing.

Remove Windows Items

To remove leftover report server items after uninstalling a report server from a Windows system

1. Navigate to *report_server_home*\CA\IAM Report Server

   report_server_home

   Specifies the report server installation path.

2. Open the BusinessObjects Enterprise 11.5 folder, and delete the following folders:
   - Data
   - Developer_Help
   - java
   - Logging
   - Samples
   - Web Content
   - Web Services
   - win32x86
3. Return to the IAM Report Server folder.
4. Open the common folder.
5. Open the 3.5 folder, and delete the following folders:
   - crystalreportviewers115
   - java
6. Return to the IAM Report Server folder, and delete the following folders:
   - log
   - OLAP Intelligence 11.5
   - stylesheets

   You have completed removing leftover items.

Remove UNIX Items

To remove leftover report server items after uninstalling a report server from a UNIX system

1. Navigate to the following location from a command prompt:

   /opt/CA/SharedComponents

2. Delete the following folders:

   - CommonReporting
   - iamreportserver

   You have completed removing leftover items.

Chapter 10: Configuring Internationalization

This section contains the following topics:

Installation Status

The following table shows you where you are in the installation process:

You Are Here	Step in Installation Process
	1. Install prerequisite hardware and software.
	2. Install Identity Manager components.
	3. Start Identity Manager.
	4. (Optional) Protect Identity Manager with SiteMinder.
	5. (Optional) Configure provisioning.
	6. (Optional) Configure email notification.
	7. (Optional) Configure workflow.
	8. (Optional) Install reporting.
X	**9. (Optional) Configure internationalization.**

How to Configure Internationalization

To configure Identity Manager for internationalization, complete the following steps:

✓	Step
	1. Confirm that the system hosting Identity Manager satisfies the prerequisites.
	2. (Optional) Configure the SiteMinder Web Agent for Internationalization.

Internationalization Prerequisites

Before installing support for internationalization, note the following:

- If you are using SiteMinder, ensure that a supported version of the SiteMinder Policy Server is installed and configured.
- Ensure that the LDAP directory is not enforcing a 7-bit check for the user ID, password, and email attribute. See the documentation for the LDAP directory you are using.
- Ensure the user directory is configured to support localization. For more information, see the relevant user directory documentation.
- Identity Manager must be installed and configured, and at least one Environment exists.

  Note: If you are using SiteMinder and your Environment manages users with multi-byte user IDs, those users must authenticate with a SiteMinder authentication scheme that supports multi-byte characters. For example, HTML Forms Based authentication. The basic authentication scheme does not support multi-byte authentication. For information on configuring an authentication scheme for Identity Manager, see the chapter on configuring SiteMinder Features for Identity Manager in the *Configuration Guide*.

Configure the SiteMinder Web Agent

Configure the encoding for HTTP header values that the SiteMinder Web Agent passes to Identity Manager by setting the HTTPheaderEncodingSpec parameter as follows:

HTTPHeaderEncodingSpec=*encoding_spec, wrapping_spec*

where *encoding_spec* is a text string that represents one of the following encoding types: UTF-8 or Shift-JIS, and *wrapping_spec* is the wrapping specification, which must be RFC-2047.

For example:

HTTPHeaderEncodingSpec="Shift-JIS,RFC-2047"

Note: If no value is specified in the HTTPHeaderEncodingSpec parameter, the encoding is UTF-8 with no wrapping.

You can configure the HTTPHeaderEncodingSpec parameter centrally in the Agent Configuration Object or locally for each Web Agent, in the WebAgent.conf file.

Note: For more information, see the *CA SiteMinder Web Access Manager Web Agent Configuration Guide.*

Create Language-Specific Tasks and Roles

Identity Manager includes sample role definition files, which you can use to create French, Korean, Japanese, or German versions of the Identity Manager roles and tasks that appear in the User Console. You can use these samples as defined to create the default roles and tasks, or use the samples as templates for creating a custom set of roles and tasks.

These files are installed in the following location:
C:\Program Files\CA\IAM Suite\Identity Manager\tools\samples\Localization*language*

where *language* is the language that you want to use.

To import a role definitions file

1. In the Management Console, click Environments.

   A list of Environments appears.

2. Click the name of the appropriate Environment.

   The Properties screen for that environment opens.

3. Click Roles.
4. Enter the path and file name for one of the role definitions files, or browse for the file.
5. Click Finish.

   The status is displayed in the Role Configuration Output window.
6. Click Continue to exit.

Restrictions on the Use of International Character Sets

The following input must contain ASCII characters only:

- Environment names and aliases
- Directory names
- Class names used in the following APIs:
  - Event Listener API
  - Notification Rule API
  - Logical Attribute API
  - Workflow Organization Resolver API
- Logical attribute names and physical attribute names used by the Logical Attribute
- The URL for the end-user license agreement that appears when users self-register

  Note: The end-user license agreement can contain internationalized character sets.

Chapter 11: Reinstalling and Uninstalling Identity Manager

This section contains the following topics:

Reinstall Identity Manager

You can reinstall any of the Identity Manager software components by rerunning the installer. When you run the installer, it detects any Identity Manager components installed on the system. You may reinstall the same components that you originally installed on the system or other components that were not originally on the system.

Note: Reinstalling the Identity Manager Administrative Tools replaces all of the files in the Administrative Tools directory. To prevent overwriting custom files, back up the directory where the Administrative Tools are installed.

Uninstall Identity Manager

To fully uninstall Identity Manager, remove Identity Manager software components and clean up the Identity Manager-specific configuration in your application server.

If you were using SiteMinder, you may also want to remove the SiteMinder Policy Server. For information about removing the Policy Server, see the *CA SiteMinder Web Access Manager Policy Server Installation Guide*.

How to Uninstall Identity Manager

The following checklist describes the steps to uninstall Identity Manager:

✓	Step
	1. Delete Identity Manager objects from the policy store.
	2. (Optional) Remove the Identity Manager schema from the policy store.
	3. Uninstall the Identity Manager components.
	4. Remove Identity Manager configuration information from the application server.

Remove Identity Manager Objects with the Management Console

In order to remove objects created automatically by Identity Manager when you configure Environments and Directories, use the Management Console.

1. Open the Management Console:
   http://*im_fqdn*:*port*/idmmanage
2. Click Environments.
3. Select all of the check boxes for the existing Environments.
4. Click Delete.
5. Click Directories.
6. Select all of the check boxes for the existing Directories.
7. Click Delete.

Remove the Identity Manager Schema from the Policy Store

If you were using a SiteMinder Policy Server, remove the Identity Manager schema from the policy store as follows:

- Remove the Identity Manager schema from a SQL Policy Store
- Remove the Identity Manager schema from a LDAP Policy Store

Remove the Identity Manager schema from a SQL Policy Store

On systems where you installed the SiteMinder Policy Server Extensions for Identity Manager, remove the Identity Manager schema by executing the following command:

- SQL Server:
  C:\Program Files\CA\IAM Suite\Identity Manager\tools\policystore-schemas\mssql\ims8_mssql_ps_delete.sql
- Oracle:
  HOME/CA/IAM_Suite/Identity_Manager/tools/policystore-schemas/oracle/ims8_oracle_ps_delete.sql

Remove the Identity Manager schema from a LDAP Policy Store

Note: If you are using Microsoft Active Directory or Microsoft ADAM as a policy store, you do not need to complete this procedure. You cannot remove schema objects from these policy stores. However, you can disable them. See the documentation for your directory for more information.

To remove the Identity Manager schema from a LDAP policy store

1. Complete one of the following:
   - If you are using IBM Directory Server as a policy store, in the IBM Directory Server Web Administration user interface, remove the schema file V3.imsschema60 from the Files section of the schema configuration. Then, restart the directory server.

     Note: There are no other steps required to remove the schema from an IBM Directory Server. Continue with Uninstall Identity Manager Software Components.
   - If you are using eTrust Directory as a policy store, remove the etrust_ims.dxc file from *dxserver_install*\config\schema.

     dxserver_install is the directory where eTrust is installed.

     Note: There are no other steps required to remove the schema from an eTrust Directory Server. Continue with Uninstall Identity Manager Software Components.
   - If you are using another LDAP directory as a policy store, skip to Step 2.
2. Navigate to the following location:
   - **Windows:** C:\Program Files\CA\IAM Suite\Identity Manager\tools\policystore-schemas\
   - **UNIX:** HOME/CA/IAM_Suite/Identity_Manager/tools/policystore-schemas

3. Use the appropriate LDIF schema file from the following table to remove the schema from the directory.

   For information on removing schema files, see the documentation for your directory.

Directory Type	LDIF File
Novell eDirectory	novell\novell-delete-ims8.ldif
Oracle Internet Directory (OID)	oracle-internet-directory\oracle-internet-directory-delete-ims8.ldif
Sun Java Systems (Sun One, iPlanet)	sunone\sunone-delete-ims8.ldif

Uninstall Identity Manager Software Components

Use the instructions in this section to uninstall Identity Manager components from each system on which you installed a component. For example, if you installed the Identity Manager Server and the Identity Manager Administrative Tools on separate systems, uninstall components from both systems.

Note: To uninstall Identity Manager components, a JVM should be running on the host.

To uninstall Identity Manager software components on Windows

1. Go to Start, Control Panel, Add/Remove Programs and select CA Identity Manager.
2. Select specific components to uninstall. This removes only the Identity Manager components that you select. You can uninstall the following components:
   - Identity Manager Server
   - Identity Manager Administrative Tools
   - Identity Manager Provisioning Server
   - Identity Manager Provisioning Directory Initialization
   - Identity Manager Extensions for SiteMinder
3. Click Change/Remove.

Note: If you want to uninstall Identity Manager completely, uninstall CA Identity Manager *and* CA IAM Suite from Add/Remove Programs.

To uninstall Identity Manager software components on UNIX

1. Navigate to:

   /CA_Identity_Manager/install_config_info/im-uninstall/uninstall

2. Run the following script:
   sh im-uninstall.sh

3. Follow the on-screen instructions.

WebLogic 8.1: Remove Identity Manager

After uninstalling the Identity Manager software, you can remove the Identity Manager configuration from your WebLogic application server.

You should remove the WebLogic domain you defined for the Identity Manager Server in your WebLogic environment after you uninstall Identity Manager.

If you created a separate domain as instructed in WebLogic Application Server (see page 22), you can simply delete the directory that was created for the domain <*wl_domain*>.You can also delete the IdentityMinder_ear, SiteMinder_ear, and Agent_ear by doing the following:

1. Open the WebLogic Console:
   http://*hostname*:*port*/console

   For example:
   http://MyServer.MyCompany.com:7001/console

2. Navigate to *WebLogic domain*, Deployments, Applications

3. Delete the appropriate EAR.

WebLogic 9.2: Remove Identity Manager

After uninstalling the Identity Manager software, you can remove the Identity Manager configuration from your WebLogic application server.

To remove the Identity Manager application from WebLogic 9.2

1. Make sure the WebLogic application server is running.

2. Run the setWLSEnv.cmd (for Windows) or setWLSEnv.sh (for Solaris) command from the following location:
   weblogic_home\weblogic92\server\bin

3. Navigate to *weblogic_home*\user_projects\domains*im_domain*\bin and execute the following command:

   ```
   java weblogic.wlst imCleanup.wlst
   ```

   This command removes the JMS resources for Identity Manager and workflow.

Chapter 12: Upgrading to Identity Manager r12

This section contains the following topics:

How to Upgrade to Identity Manager r12

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

- Identity Manager r8.1 or later without provisioning (Web Edition).
- Identity Manager r8.1 or later with provisioning.
- eTrust Admin r8.1 SP2

Important! If you are using SiteMinder, Identity Manager r12 requires a SiteMinder Policy Server r6.0.5 CR15 or later.

Perform the following steps to upgrade to Identity Manager r12:

If you currently have...	Perform these upgrade steps...
eTrust Admin r8.1 SP2	1. Upgrade the Provisioning Server Components with the Provisioning Installers. 2. Upgrade the Connectors using the Provisioning Server installer. 3. Perform a new Installation of the Identity Manager Server with the Identity Manager Installer.
Identity Manager r8.1 or later without Provisioning (Web Edition)	1. Upgrade the Identity Manager Server with the Identity Manager Installer. 2. Perform a new Installation of the Provisioning Server Components with the Identity Manager Installer. 3. Install Connectors using the Product Explorer.

If you currently have...	Perform these upgrade steps...
Identity Manager r8.1 or later with Provisioning	1. Upgrade the Provisioning Server Components with the Provisioning Installers. 2. Upgrade the Connectors using the Provisioning Server installer. 3. Upgrade the Identity Manager Server with the Identity Manager Installer.

Upgrade Provisioning Server Components

Important! Only upgrades from eTrust Admin r8.1 SP2 are supported. If you have a previous version of eTrust Admin, first upgrade to eTrust Admin r8.1 SP2 and then continue with the Identity Manager r12 upgrade.

Perform the following steps to upgrade Provisioning (eTrust Admin r8.1 SP2) to Identity Manager r12:

Step
1. Review Important Notes for Provisioning Upgrades
2. Update the Provisioning Directory Schema
3. Gather information for the Provisioning Server upgrade
4. Upgrade the primary Provisioning Server
5. Upgrade other Provisioning components (alternate servers, connector servers, SDK, agents)

Update the Provisioning Directory Schema

In order for Provisioning to work with Identity Manager r12, first upgrade the Provisioning Directory schema on the system running eTrust Directory.

Important! We recommend backing up your eTrust Directory databases before upgrading.

To upgrade the Provisioning Directory schema

1. Navigate to the Provisioning/Provisioning_Directory folder on the Identity Manager installer media.

2. Run the setup file on the system with eTrust Directory.

   The upgrade wizard will start.

3. Go through the wizard and enter the required information.
4. On the Custom Location Setup screen, choose the Provisioning Directory installation path.
5. Click Next.

   The Provisioning Directory schema will be updated.

Gather Information for Provisioning Server Upgrade

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 Provisioning Directory installed.	
Directory Port	The port number of the system with the Provisioning Directory installed.	
Directory DN	The DN of the Provisioning Directory.	
Directory Password	The password for the Provisioning Directory.	
Username	The Provisioning domain administrator's username.	
Password	The Provisioning domain administrator's password.	
Description	Provide a description for the Provisioning administrator.	

Upgrade the Provisioning Server

Note: For more information on how to address Provisioning Server upgrades in a high-availability environment, see the *High Availability Guide*.

To upgrade the Provisioning Server

1. Navigate to the Provisioning/Provisioning_Server folder on the Identity Manager installer media.
2. Run the setup file.
3. Accept the terms of the license agreement and click Next.
4. Choose Custom setup type and click Next.
5. Click Browse if you want to search for another install location, or click Next to install the Provisioning Server in the default location.
6. Choose Provisioning Server and Connector Server (C++) and click Next.
7. Provide the following Provisioning Directory details:
   - Directory Host
   - Directory Port
   - Directory DN
   - Directory Password

   Click Next.
8. All the connectors detected in your environment will be checked for upgrade. Click Next.
9. Choose if the Provisioning Server you are upgrading is the primary server or an alternate server and click Next.
10. Provide the domain name for your Provisioning domain configuration and click Next.
11. Provide the following Provisioning domain administrator details:
    - Username
    - Password
    - Description

    Click Next.
12. Provide passwords for all Provisioning components and click Next.

    The Provisioning Server is upgraded.

Upgrade Other Provisioning Components

Java Connector Server

Run the Java Connector Server installer from the Provisioning Components installation media, and register the Java Connector Server with the Provisioning Server on the final install screen.

Note: For more information on upgrading to the Java Connector Server, see the *Java Connector Server Implementation Guide*.

SuperAgent

Upgrade each SuperAgent by running the Provisioning Server installer on the Identity Manager installation media. Select C++ Connector Server.

eTrust Admin Manager

Run the Provisioning Manager installer on the Identity Manager installation media to upgrade eTrust Admin Manager.

Upgrade Connectors

To upgrade connectors, use the Identity Manager installation media and run the Provisioning Server installer.

Note: For more information on upgrading a specific connector, see the *Connector Guide*.

Custom Java Connectors

The Identity Manager r12 Java Connector Server is compatible with the Identity Manager r8.1 SP2 SDK connector code.

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

Custom Options

If you are currently using a SuperAgent with custom options, your custom options will be compatible with the Identity Manager r12 version of the SuperAgent, now called the C++ Connector Server. No upgrade of these options is required.

Upgrade the Identity Manager Server

Perform the following steps to upgrade Identity Manager to Identity Manager r12:

Step
1. Configure a Web Agent.
2. Upgrade the Identity Manager Server
3. Export the Directories and Environments
4. Modify the Configuration
5. Recreate the Identity Manager Directory
6. Recreate the Environments
7. Additional New Feature Configuration
8. Install the Identity Manager r12 Bookshelf

Configure a Web Agent

As SiteMinder is used to protect Identity Manager, you must configure a Web Agent (see page 43).

Note: The Servlet Filter Agent is being deprecated in Identity Manager r12. If you are using a Servlet Filter Agent, Identity Manager will work properly after the upgrade, but we strongly recommend configuring a Web Agent for Identity Manager r12.

Upgrade the Identity Manager Server

To upgrade the Identity Manager Server, run the Identity Manager Installer. The installer will auto-detect the previous version of Identity Manager and ask you if you want to continue with an upgrade.

Important! Ensure that you shut down the application server before upgrade.

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

All unused files will be deleted.

The following custom configuration files will be preserved:

- Policy Server connection
- Data store definitions
- Custom JSPs

Export the Directories and Environments

In Identity Manager r12, objects previously stored in the SiteMinder Policy Store need to be moved to a relational database object store. After you upgrade to Identity Manager r12, objects will be stored in *both* the Identity Manager object store and the SiteMinder policy server.

Use the r12 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.

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

Note: Ensure 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:
   C:\Program Files\CA\IAM Suite\Identity Manager\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 *SM_admin_user* -p *SM_admin_pw* -d *ims_dir_name* -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.

   SM_admin_user

   Defines the SiteMinder administrator.

   SM_admin_pw

   Defines the SiteMinder administrator password.

   ims_dir_name

   Defines the name of the Identity Manager directory to export.

   folder_name

   Defines the name of the folder where you'd like the r12 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 *SM_admin_user* -p *SM_admin_pw* -e *ims_env_name* -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.

   SM_admin_user

   Defines the SiteMinder administrator.

   SM_admin_pw

   Defines the SiteMinder administrator password.

   ims_env_name

   The name of the 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 the following ZIP file:
   ims_env_name.zip

Modify the Configuration

After upgrade Identity Manager to r12, modify the configuration to support the new architecture. Perform the following steps to modify the Identity Manager configuration.

1. Upgrade TEWS
2. Copy the JDBC driver files
3. Add new JDBC data sources
4. Modify the RDB user store
5. Update existing data sources.
6. Update the application server proxyforwarder
7. Upgrade workflow
8. Upgrade reporting
9. Configure the Provisioning Manager

Upgrade TEWS

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

To recreate the WSDL files

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

If you had this method in Identity Manager r8.1...	Use this method in Identity Manager r12...
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.

Upgrade from r8.1 TEWS Changes

If you are upgrading from Identity Manager r8.1, consider the following TEWS changes:

Namespace and Package Name Changes

With this release of Identity Manager, WSDL generation is invoked using a specific URL that generates a single WSDL file with a single namespace. By producing a single WSDL file without references to other files, any existing client code that needs to interact with Identity Manager TEWS may have to be modified.

The single namespace necessitates removing all the namespaces that previously had to be defined to import a WSDL file for each task. This results in a major change when generating the proxies and reduces multiple generated package names to one package name. Your client code will need to be modified to reflect changed package names.

Attribute Name Changes

An Axis-related change involves the transition from Axis 1.2 beta. This change results in a performance boost, but it also affects client code in that the generated proxies vary with the different Axis versions. For example, a lot of underscores used in attribute names have been eliminated, resulting in more readable code.

Result and Status Proxy Values

In previous releases of Identity Manager, if a service returned both a result and a status, special holder classes were generated for proxies so the result and status could be returned by reference from the method call. This exposed a parsing problem with Axis, and required a special patched version of Axis to be shipped with Identity Manager.

In the current release of Identity Manager, the result and status are returned as a single value rather than as two values by reference. This eliminates the requirement to use the patched version of Axis to generate proxies.

Result and Status Code

Result and status information are now contained within a single return value which simplifies client code. The following example demonstrates the holder classes used in previous Identity Manager releases:

```
/* output parameter for status part of the message */
_ImsStatusHolder statusHolder = new _ImsStatusHolder();
/* output parameter for the return message part */
_ViewMyRolesQueryResultHolder resultHolder =
new _ViewMyRolesQueryResultHolder();
/* this forms the SOAP request, and processes the return document */
port.viewMyRolesQuery(admin_id,vmrq,statusHolder,resultHolder);
```

With the new release, the same code returns a value without the need for a holder class. The status can now be queried directly:

```
ViewMyRolesQueryResult result = port.viewMyRolesQuery(admin_id,vmrq);
ImsStatus imsStatus = result.getImsStatus();
```

Public and Protected Context Tasks

All context information for TEWS tasks have been encapsulated into public and protected context types. These types are defined in the WSDL and are the first parameter for all tasks.

In previous releases, all tasks required the admin_id as part of the request message, regardless of whether they were public or protected. In this release, the WSDL does not define an admin_id attribute in request messages for public tasks. Therefore, admin_id is not required for public tasks, although it is still required for protected tasks. This may impact migrating customer code that currently sets the admin_id for public tasks.

In addition, each context type lists a number of optional attributes that apply to particular tasks. For example, the protected context includes workitem_id and action attributes which are expected for approval tasks.

Context Code Changes

The execution of a task in TEWS includes code that evaluates the information supplied in the context. Values that are required for a given task are checked, and any appropriate SOAP fault is generated.

If attributes that are not required are specified anyway, warnings are logged on the console and the values are ignored. This change allows for the future addition of context attributes without impacting the proxies that are generated.

Therefore, context changes require existing client code to be refactored to account for the context type that is now included in rebuilt proxies.

The following code example does not consider context:

```
EnableDisableUserSearchResult result =
searchPort.enableDisableUserSearch(strAdminDN, es);
Whereas migrated code must take the context into account:
TaskContext ctx = new TaskContext();
ctx.setAdmin_id(strAdminDN);
EnableDisableUserSearchResult result =
searchPort.enableDisableUserSearch(ctx, es);
```

Locators and Ports

In this release, the number of ports changes in the generated WSDL. In previous releases, a separate port was defined for each task. With the single WSDL, there is one port defined for the protected alias and one port defined for the public alias. Tasks are sorted into these two ports based on whether the task is public or protected. This means that with most proxies, the location of the web service can be changed with a single method call.

In general, to call an operation you now use code similar to the following example:

```
Tews6Locator locator = new Tews6Locator();
Tews6PortType port = locator.getPort();
/* access operations on port */
The same port can be used for multiple operations. Previous releases required code similar to the
following example, in which each task had its own port:
Tews6Locator locator = new Tews6Locator();
```

ChangeMyPasswordPortType port = locator.getChangeMyPasswordPortType();

Copy the JDBC Drivers

After upgrading from Identity Manager r8.1 to r12, copy the jdbc drivers to the application server.

WebLogic 9

Copy the jar files to: c:\bea\weblogic92\server\lib

WebLogic 8

Copy the jar files to: c:\bea\weblogic81\server\lib

Note: The JDBC driver jars are located in the following location:
C:\Program Files\CA\IAM Suite\Identity Manager\tools\lib\jdbcdrivers

Add New Data Sources

Identity Manager r12 requires two new data sources for the Identity Manager Server. One data source is for the new object store database and the other is for the report snapshot database.

To add the new data sources

1. Using the WebLogic administrative console, create the following two new data sources:
   - jdbc/reportsnapshot
   - jdbc/objectstore.
2. Edit both data sources created in Step 1 as follows:
   a. Provide the new database name in the data source.
   b. Depending on your database, add the following to Custom Properties:
      - **SQL:** user=<username>, password=<password>, selectMethod=cursor
      - Oracle: user=<username>, password=<password>
   c. Ensure the JDBC class names are as follows:
      - **SQL:** com.microsoft.sqlserver.jdbc.SQLServerDriver
      - **Oracle:** oracle.jdbc.driver.OracleDriver
   d. Disable Support Global Transactions on the data source.
3. Restart the application server.

Modify the RDB User Store

To modify an RDB user store for upgrade

1. If you are using a relational database user store, edit the generated directory.xml as follows:
   a. Add the following element:
   <JDBC datasource=" userstore_jndi"/>
   b. Remove the maxrows attribute from the DirectorySearch element.
2. If you are using a relational database user store that supports Organizations, run the following script located in the C:\Program Files\CA\IAM Suite\Identity Manager\tools\samples\NeteAutoRdb\Organization\ directory:
   - **SQL:** mssql-orgpath-addon-upgrade-8-to-r12.sql
   - **ORACLE:** oracle-orgpath-addon-upgrade-8-to-r12.sql

Update Existing Data Sources

Disable Support Global Transactions in all existing data sources for Identity Manager r12.

Update the Proxy Forwarder

Identity Manager r12 introduces 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 the /idm in the http proxy forwarder.

Upgrade Workflow

In Identity Manager r8.1 SP1, an updated version of WorkPoint Workflow was added to the installation. If you are upgrading from a version of Identity Manager prior to 8.1 SP1, you update the workflow database to work with WorkPoint 3.3 after upgrading to Identity Manager r12.

After updating the workflow database, you can continue to use the workflow processes that you developed in WorkPoint 3.2.

To upgrade workflow

1. Convert the workflow database to the WorkPoint 3.3.2 schema:
   a. Log into the workflow database as the workpoint db user.
   b. Run wp32_to_wp33_cnv.sql.

      This script is located in the following location:

      C:\Program Files\CA\IAM Suite\Identity Manager\tools\Workpoint\database*db_type*

      Note: If errors occur, use the wp32_to_wp33_cnv_undo.sql script to revert to the WorkPoint 3.2 database schema.
   c. Run the wp32_to_wp33_cnv_cleanup.sql script to clean up the database if no errors occurred when you ran wp32_to_wp33_cnv.sql.

      After you run the cleanup script, you can no longer revert to the WorkPoint 3.2 database schema.
2. Run the wp330_to_wp331_cnv.sql script.

3. If you developed custom workflow scripts using the Workflow API in previous versions of Identity Manager, change all occurrences of ClientContextEJB to ClientContext.

   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
```

4. If you developed custom workflow scripts using the Workflow API in previous versions of Identity Manager, the method signature to generate the workflow context has changed.

   If you have custom code that resmbles the following:

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

   change it as follows:

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

To verify that WorkPoint Workflow is configured correctly, log in into Identity Manager and execute tasks that are configured for workflow. You should see work items and be able to approve them .

Upgrade Reporting

If you used reporting with an earlier version of Identity Manager, run the one of the following upgrade scripts on the Reporting Database:

- **MS SQL:**

  C:\Program Files\CA\IAM Suite\Identity Manager\tools\imrexport\db\sqlserver\ims_mssql_upgrade_6x_to_8.sql
  C:\Program Files\CA\IAM Suite\Identity Manager\tools\imrexport\db\sqlserver\ims_mssql_upgrade_8_to_r12.sql

- **Oracle:**

  C:\Program Files\CA\IAM Suite\Identity Manager\tools\imrexport\db\oracleims_oracle_upgrade_6x_to_8.sql
  C:\Program Files\CA\IAM Suite\Identity Manager\tools\imrexport\db\oracleims_oracle_upgrade_8_to_r12.sql

Note: If you have custom identifier files, put them in the following location:

IdentityMinder.ear\config\com\netegrity\config\imrexport\sample

Configure the Provisioning Manager

Set up the Identity Manager Server and enable inbound synchronization in the Provisioning Manager.

To configure the Provisioning Manager

1. Go to Start, Programs, CA, Identity Manager, Provisioning Manager
2. Log in to the Provisioning Manager using the global username and password you provided while installing the Identity Manager Administrative Tools.
3. Click System.
4. Click Identity Manager Setup on the left.
5. Enter the hostname, port number and environment alias for the Identity Manager server.
6. Click Add.
7. Click Apply.

   Note: If you get a shared secret error, re-enter the password under Shared Secret and Confirm Shared Secret and click Apply again.
8. Click Domain Configuration on the left.
9. Expand the Identity Manager Server folder and click Enable Notification.
10. Click Edit.
11. Change the value to Yes.
12. Click Apply.
13. Restart the Provisioning Server.

Recreate the Identity Manager Directory

In previous versions of Identity Manager, communication to the user stores was done through SiteMinder. In Identity Manager r12, user store communication is done through the application server. Also, the directory configuration information needs to be re-imported into the new object store.

LDAP User Stores

To recreate the directory configuration to an LDAP user store

1. In the Management Console, click Directories.
2. Click New.
3. Import the previously exported directory.xml to create a new Identity Manager Directory.
4. Click Next.
5. Verify the directory settings and click Finish.

   The old directory is recreated for Identity Manager r12. Identity Manager uses standard JNDI to talk to all LDAP users stores, so no additional configuration is needed in the application server.

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

RDB User Stores

To recreate the directory configuration to an RDB user store

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 Identity Manager r12.

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

Recreate the Environment

Previously, Identity Manager objects, such as roles, tasks, and so on, were stored in the SiteMinder Policy Store. In r12, Identity Manager objects are stored in the object store. During the upgrade, this information needs to be imported to the object store using the Management Console.

To recreate the environment

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

   At this point, Identity Manager will recreate the environment and migrate task persistence data. Only *pending* tasks will be migrated.

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 Identity Manager r12, you can use the Migrate Task Persistence Data from Identity Manager 8.1 button on the Environment page in the Management Console to restart the migration process. Restarting this process will not duplicate tasks that have already been migrated.

Additional New Feature Configuration

The following new features are optional and can be configured in Identity Manager r12.

Delegation

If you are upgrading from a previous version of Identity Manager, do the following:

- If you are upgrading from an earlier version of Identity Manager than r8.1 SP2, add the %DELEGATORS% wellknown 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:
  C:\Program Files\CA\IAM Suite\Identity Manager\tools\samples\NeteAutoRdb\Organization
  C:\Program Files\CA\IAM Suite\Identity Manager\tools\samples\NeteAutoRdb\NoOrganization

Template Method Workflow and Task-Level Workflow

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

1. In Workpoint Designer, click Import.

   Workpoint Designer location: C:\Program Files\CA\IAM Suite\Identity Manager\tools\Workpoint\bin

2. Navigate to C:\Program Files\CA\IAM Suite\Identity Manager\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: Ensure 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 section on configuring workflow.

Roles and Tasks

In order to support new features in Identity Manager r12, such as reporting, scheduler, bulk loader, non-standard accounts, and so on, use the Management Console to import one of the following new role definitions files:

- C:\Program Files\CA\IAM Suite\Identity Manager\tools\RoleDefinitionUpdates\Upgrade-8.1-to-12-RoleDefinitions-NoOrganization.xml
- C:\Program Files\CA\IAM Suite\Identity Manager\tools\RoleDefinitionUpdates\Upgrade-8.1-to-12-RoleDefinitions-Organization.xml

- C:\Program Files\CA\IAM Suite\Identity Manager\tools\RoleDefinitionUpdates\Upgrade-8.1-to-12-RoleDefinitions-ProvisioningNoOrganization.xml
- C:\Program Files\CA\IAM Suite\Identity Manager\tools\RoleDefinitionUpdates\Upgrade-8.1-to-12-RoleDefinitions-ProvisioningOrganization.xml

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

Install the Identity Manager r12 Bookshelf

For complete information about this product, install the Identity Manager r12 Bookshelf, so that you can do the following:

- Use a single console to view documents published for Identity Manager (including Provisioning).
- 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 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.

Unattended Upgrades

To enable an unattended 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.

Note: For more information on the im-installer.properties configuration file, see the Unattended Installation section of this guide.

For Provisioning components, you can generate a response file with each of the 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 Identity Manager installer against the im-installer.properties file with one of the following commands:

- **Windows:**
  ca-im-12.0-sp02-win32.exe -f im-installer.properties -i silent
- **UNIX:**
  ./ca-im-12.0-sp02-sol.bin -f im-installer.properties -i silent

Note: For more information on the im-installer.properties configuration file, see the Unattended Installation section of this guide.

The following properties are needed in the configuration file for running the Identity Manager Server upgrade:

Weblogic 8 or 9

No input required.

JBoss

DEFAULT_JBOSS_FOLDER=location of JBOSS 4.0.5

WebSphere

If the Identity Manager r8.1 installer was run on the same system as the WebSphere application server the following properties are needed:

- DEFAULT_WEBSPHERE_FOLDER=location of WebSphere on the system
- DEFAULT_WAS_NODE=WebSphere node
- DEFAULT_WAS_SERVER=hostname of WebSphere server
- DEFAULT_WAS_CELL=WebSphere cell

- WAS_PROFILE=WebSphere profile
- DEFAULT_WAS_CLUSTER=WebSphere cluster name

Currently we do not support unattended upgrade when Identity Manager has been deployed manually to the WebSphere application server.

Note: 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 Identity Manager 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 A: Unattended Installation

This section contains the following topics:

Modify the Configuration File

To enable an unattended Identity Manager installation, you modify the settings in the im-installer.properties configuration file using a text editor. The default parameters in the file reflect the information you entered during the initial Identity Manager installation. Change the default values as needed.

The file is located in the CA Identity Manager installation directory. The following is an example of the im-installer.properties file created during the initial Identity Manager installation.

Guidelines for File Modification

Follow these guidelines when modifying the configuration file:

- Make a back-up copy of the installer properties file before modifying the original, since the file holds all of the values you entered during the initial installation or configuration.
- Do not add extra spaces between the parameter name, the equals sign (=), and the attribute value.
- All directory names on Windows must contain either double back slashes or forward slashes, not single back slashes.

Configuration File Format

Below is an example of the im-installer.properties configuration file:

```
################################################################
### Silent input properties file for the IMR12 installer ##
################################################################

#INSTANCE DISPLAY NAME
#   For fresh installation it will always be 'New Installation'
#   For Upgrade NEW_INSTANCE_DISPLAY_NAME will be equal to INSTANCE_NAME
DEFAULT_NEW_INSTANCE_DISPLAY_NAME=New Installation

#INSTANCE NAME
#   Instance name for IAM Suite provided in the Main product installer
#DEFAULT_INSTANCE_NAME=Identity Manager

# Complete install
#   If this is true, component selection (below) is ignored.
#DEFAULT_COMPLETE_INSTALL=false

# Component list
#   Valid values (comma-separated, one or more):  Server,Exten,Admin,Provision,Directory
DEFAULT_COMPONENTS=Server,Admin

# Install folder
#   All products are installed in subfolders under this folder
#   This is parent product root selected by the user
#   For e.g. C:\\\\Program Files\\\\CA
DEFAULT_INSTALL_FOLDER=C:\\Program Files\\CA

#Generic login information
DEFAULT_GENERIC_USERNAME=imuser
#DEFAULT_GENERIC_PASSWORD=<For silent install, insert generic user password here and uncomment
line.>

# Provisioning Server and Provisioning Directory Information.
#  Configure the Provisioning Server to a remotely installed Provisioning Directory(true/false)
DEFAULT_CONFIG_REMOTE_PROVISIONING=false

DEFAULT_DOMAIN_NAME=IDENTITY_MANAGER
DEFAULT_DIRECTORY_HOST=
DEFAULT_DIRECTORY_PORT=
```

```
#DEFAULT_DIRECTORY_BINDDN=eTDSAContainerName=DSAs,eTNamespaceName=CommonObjects,dc
=etadb
#DEFAULT_DIRECTORY_PASSWORD=<For silent install, insert password to be used with Provisioning
Components here and uncomment line.>


#FIPS 140-2 Compliance mode (true/false) for Provisioning Manager and Provisioning Server
DEFAULT_FIPS_MODE=true

#Identity Manager Application Server information
#   App Server
#   Valid values:  JBoss, WebSphere, WebSphere6, WebLogic8, Weblogic9
DEFAULT_APP_SERVER=WebLogic8

#Application Server Host: This value will be derived from APP_SERVER_URL by removing the port appended to
it
#   For e.g. http://machine.domain
#DEFAULT_APP_SERVER_HOST=http://iam-fw-wl8.ca.com

#Application Server Port: This value will be derived from APP_SERVER_URL by removing the hostname from it
#DEFAULT_APP_SERVER_PORT=7001

DEFAULT_APP_SERVER_URL=http://iam-fw-wl8.ca.com:7001

#Path to JDK/JRE for the Application Server
#   For JBoss this has to be path to JDK and for WebLogic, Websphere it is path to JRE or JDK
DEFAULT_JAVA_HOME=C:\\Program Files\\Java\\jre1.5.0_11

#JBoss info
DEFAULT_JBOSS_FOLDER=C:\jboss

#Weblogic info
DEFAULT_BINARY_FOLDER=C:\\bea\\weblogic81
DEFAULT_DOMAIN_FOLDER=C:\\bea\\user_projects\\domains\\mydomain
DEFAULT_SERVER_NAME=myserver
#WEBLOGIC_DOMAIN=mydomain
#WEBLOGIC_FOLDER value will be containing the value of C:\\bea
#DEFAULT_WEBLOGIC_FOLDER=C:\bea
#For Weblogic9 only:
DEFAULT_BEA_CLUSTER=

#WebSphere info
DEFAULT_WEBSPHERE_FOLDER=C:\websphere

#WAS_NODE Location: \\installedApps\\node name
#   and directory \\config\\cells\\\\nodes\\node name
DEFAULT_WAS_NODE=node name
```

```
#WAS_SERVER Value: \\config\\cells\\cell name\\nodes\\node name\\servers\\server1
DEFAULT_WAS_SERVER=server1

#WAS_CELL: \\config\\cells\\cell name
DEFAULT_WAS_CELL=cell name


#WebSphere 6 Only:
#   WAS_PROFILE = \\profiles\\
WAS_PROFILE=

#WebSphere 6 Only:
#WAS_CLUSTER: \\config\\cells\\cell name\\clusters\\
DEFAULT_WAS_CLUSTER=

#Policy Server info
DEFAULT_PS_HOST=localhost
DEFAULT_PS_USER=SiteMinder
#DEFAULT_PS_PW=<For silent install, insert PS Admin user password here and uncomment line.>
#DEFAULT_AGENT_NAME=imuser
#DEFAULT_AGENT_PW=

#Policy Server Extensions info
#   Location of CsSmPs-<Instance name> folder
DEFAULT_PS_ROOT=
#PS_MANAGED=true
DEFAULT_USE_SITEMINDER=false

#Path to JRE or JDK for Policy Server
#DEFAULT_NETE_JRE_HOME=

#iRecorder info
#   Set to true if you want iRecorder to be installed
DEFAULT_CONFIG_IREC=true
#   iRouter is Local or Not
DEFAULT_IROUTER_NON_LOCAL=true
#   iRouter location - if not local
DEFAULT_IREC_ROUTER_LOC=testirec.com


#Admin Tools info
#DEFAULT_ADMIN_FOLDER=C:\\bea\\user_projects\\domains\\mydomain\\applications\\IdentityMinder.ear\\IA
M Suite
```

```
#Database Info
DEFAULT_DB_HOST=localhost
DEFAULT_DB_PORT=1433
DEFAULT_DB_NAME=fwstore
DEFAULT_DB_USER=fwadmin
#DEFAULT_DB_PASSWORD=<For silent install, insert database password here and uncomment line.>
DEFAULT_DB_TYPE=mssql2005
#DEFAULT_INITIALIZEDB_SELECTED=1
```

Configure Installation for Unattended Mode

To run the installer in the unattended installation mode

1. Modify the im-installer.properties file using the instructions in the following sections:
   - Initial Choices
   - Identity Manager Server
   - Optional Component Configuration
   - Identity Manager Extensions to the Policy Server
2. Run the following command:
   - **Windows:**
     ca-im-12.0-sp02-win32.exe -f im-installer.properties -i silent
   - **UNIX:**
     ./ca-im-12.0-sp02-sol.bin -f im-installer.properties -i silent

Initial Choices

For basic installation choices, enter values for the following parameters:

Parameter	Instructions
DEFAULT_NEW_INSTANCE_DISPLAY_NAME	Enter 'New Installation' if this is a fresh install. For upgrades, this will be blank.

Parameter	Instructions
DEFAULT_COMPONENTS	Enter one or more components: ■ Server - Identity Manager Server ■ Exten - Identity Manager Extensions to the Policy Server ■ Admin - Identity Manager Administrative Tools ■ Provision - Provisioning Server ■ Directory - Provisioning Directory To install more than one component, separate components by a comma.
DEFAULT_INSTALL_FOLDER	Enter the directory in which to install the Identity Manager Server.
DEFAULT_GENERIC_USERNAME	Generic login information for Identity Manager components that are installed.
DEFAULT_GENERIC_PASSWORD	Generic password information for Identity Manager components that are installed.

The installation program ignores any parameters that do not apply to the component you are installing. For example, if you set DEFAULT_COMPONENTS to Exten, only the DEFAULT_PS_ROOT and DEFAULT_USE_SITEMINDER parameters are used.

Identity Manager Server

If you plan to install the Identity Manager server, enter values for the following parameters:

Parameter	Instructions
DEFAULT_APP_SERVER	Enter, Weblogic, WebSphere, or JBoss
DEFAULT_APP_SERVER_URL	Enter full URL of the application server hosting Identity Manager, including the port.
DEFAULT_CONFIG_IREC	Enter true to install Identity Manager iRecorder.

Parameter	Instructions
DEFAULT_IROUTER_NON_LOCAL	Enter true if the iRecorder router is installed on a remote system.
DEFAULT_IREC_ROUTER_LOC	Enter location of remote iRecorder system.
DEFAULT_FIPS_MODE	Enter true if you want to install with FIPS 140-2 Compliance.
DEFAULT_JAVA_HOME	Path to JRE or JDK for Identity Manager.
Additional Database Parameters	
DEFAULT_DB_HOST	Enter the hostname of the system hosting the Identity Manager database.
DEFAULT_DB_PORT	Enter the port of the system hosting the Identity Manager database.
DEFAULT_DB_NAME	Enter the name of the Identity Manager database.
DEFAULT_DB_USER	Enter the administrative username for the Identity Manager database.
DEFAULT_DB_PASSWORD	Enter the password for the administrative user of the Identity Manager database.
DEFAULT_DB_TYPE	Enter the type of database used for the Identity Manager database.
Additional JBoss Parameter	
DEFAULT_JBOSS_FOLDER	Enter the full pathname of the directory where you installed the JBoss application server. For example, C:\Program Files\jboss-4.0.5
Additional WebLogic Parameters	
DEFAULT_BINARY_FOLDER	Enter the full directory path of the directory where you installed WebLogic. For example: C:\bea\weblogic81\

Parameter	Instructions
DEFAULT_DOMAIN_FOLDER	Enter the full path and directory name for the WebLogic domain you created for Identity Manager.
DEFAULT_SERVER_NAME	Enter the name of the WebLogic server instance you created for use with Identity Manager.
DEFAULT_BEA_CLUSTER	(WebLogic 9) Enter the cluster name for the WebLogic cluster.

Additional WebSphere Parameter	
DEFAULT_WEBSPHERE_FOLDER	Enter the full pathname of the directory where you installed Identity Manager Tools for WebSphere.
DEFAULT_WAS_NODE	Enter the name of the node in which the application server is located.
DEFAULT_WAS_SERVER	Enter the name of the system on which the application server is running.
DEFAULT_WAS_CELL	Enter the name of the cell in which the application server is located.
WAS_PROFILE	(WebSphere 6) Enter the location of the WebSphere profile files.
DEFAULT_WAS_CLUSTER	(WebSphere 6) Enter the cluster name for the WebSphere cluster.

If you are using a SiteMinder Policy Server, enter the following:

Parameter	Instruction
DEFAULT_PS_HOST	Enter the fully-qualified domain name of the Policy Server.

Parameter	Instruction
DEFAULT_PS_USER	Enter the user name of the Policy Server administrator.
DEFAULT_PS_PW	Enter the password of the Policy Server administrator.

Optional Component Configuration

If you install the iRecorder, enter the following:

Parameter	Instructions
DEFAULT_IREC_ROUTER_LOC	If you are installing Identity Manager iRecorder, enter the hostname or IP address of the iRouter used by SCC or eTrust Audit.

If you install Provisioning, enter the following:

Parameter	Instruction
DEFAULT_CONFIG_REMOTE PROVISIONING	Enter true if you are connecting to a remote Provisioning Directory.
DEFAULT_DOMAIN_NAME	Enter IDENTITY_MANAGER unless you have an existing Provisioning domain.
DEFAULT_DIRECTORY_HOST	Enter the hostname of the system with Provisioning Directory installed.
DEFAULT_DIRECTORY_PORT	Enter the port number of the system with the Provisioning Directory installed.
DEFAULT_DIRECTORY_PASSWORD	Enter the password for the Provisioning Directory.

Identity Manager Extensions to the Policy Server

To install the Identity Manager extensions to a SiteMinder Policy Server, enter this parameter:

Parameter	Instruction
DEFAULT_PS_ROOT	(Solaris Only) Enter the directory where the Policy Server is installed.
DEFAULT_USE_SITEMINDER	Enter true if you are using a SiteMinder Policy Server in your implementation.

Appendix B: Creating a New Database

This section contains the following topics:

How to Create a New Database Instance

When installing Identity Manager, all of the database schemas are created automatically.

For scalability purposes, you may want to create a new, separate database to replace any one of the existing database schemas initially created by Identity Manager. You can create a new database instance for the following:

- Workflow
- Auditing
- Task Persistence
- Object Store
- Reporting

Perform the following steps to create a new database:

1. Create a new database instance for Identity Manager as follows:
   - MS SQL
   - Oracle
2. Edit the data source.
3. (Optional) Run the SQL scripts.

Create an MS SQL Server Database Instance

To create an MS SQL Server Database Instance

1. Create a database instance in SQL server.
2. Create a user and grant this user the necessary rights (such as public and db_owner rights) to the database by editing the properties of the user.

   Note: The user must have at least select, insert, update, and delete permissions for all of the tables created by the .sql script for creating the database, and must be able to execute all of the stored procedures (if applicable) defined in these scripts.
   For example, the user must have these permissions on the tables defined in:
   C:\Program Files\CA\IAM Suite\Identity Manager\tools\db\taskpersistence\sqlserver\idm_db_sqlserver.sql
3. While editing the user's properties, set the database you just created as the default database for the user.
4. Ensure the Authentication setting has a value of SQL Server or Windows on the Security tab of the SQL Server Properties dialog for the server where the database is installed.

Note: For complete information about MS SQL, see your MS SQL documentation.

Create an Oracle Database Instance

To create an Oracle **Database Instance**

1. Create a new tablespace.
2. Create a new user.
3. Grant the new user rights to the new database.
4. Give DBA rights to the user.

Note: For complete information about Oracle, see your Oracle documentation.

Edit the Data Source

To edit the data source

1. Within the WebLogic administrative console, open the appropriate data source descriptor.

   The JNDI names for the data source descriptors are as follows:

   - Task Persistence: jdbc/idm
   - Workflow: jdbc/WPDS
   - Auditing: auditDbDataSource
   - Reporting: jdbc/reportsnapshot
   - Object Store: jdbc/objectstore

2. Change the DatabaseName, User, and Password in the data source descriptor to the appropriate values for the new database.

   The database schema (SQL scripts) will be automatically applied when you restart Identity Manager.

3. Disable Support Global Transactions on the data source.
4. Restart the application server.

Run the SQL Scripts

SQL scripts are automatically run against the databases when Identity Manager starts, however if you want to run the SQL scripts yourself, perform the following steps before restarting the application server:

These scripts are installed with the Identity Manager Administrative Tools.

To run the SQL scripts

1. Do one of the following:
   - MS SQL Server: Open the Query Analyzer tool and select the script you need.
   - Oracle: Open the SQL prompt for the script you need.
2. Select one of the following scripts depending on what the database was created for:
   - Task Persistence:
     - MS SQL: C:\Program Files\CA\IAM Suite\Identity Manager\tools\taskpersistence\sqlserver\idm_db_sqlserver.sql
     - Oracle: C:\Program Files\CA\IAM Suite\Identity Manager\tools\taskpersistence\oracle9i\idm_db_oracle.sql
   - Workflow: Run the CreateDatabase script.
   - Auditing:
     - MS SQL: C:\Program Files\CA\IAM Suite\Identity Manager\tools\db\auditing\sqlserver\ims_mssql_logs.sql
     - Oracle: C:\Program Files\CA\IAM Suite\Identity Manager\tools\db\auditing\oracle\ims_oracle_logs.sql
3. Run the script file.

To verify that the database instance is correctly configured, check the database tables for Identity Manager objects that begin with the letters idm.

Run the CreateDatabase Script for Workflow

Identity Manager includes SQL scripts for setting up a new workflow database instance.

To run the CreateDatabase script

1. Add the path to the sqljdbc.jar to the DB_CLASSPATH attribute in the CreateDatabase.bat or .sh script before you run it.
2. From a command prompt, run the C:\Program Files\CA\IAM Suite\Identity Manager\tools\Workpoint\install\CreateDatabase.bat or sh.

   A command prompt window and the WorkPoint application open.
3. Select the database type from the drop-down.

4. Use the following guidelines to fill in fields in the configuration utility:
   - For the JDBC Class parameter, enter:

     Oracle: oracle.jdbc.driver.OracleDriver

     SQL Server: com.microsoft.jdbc.sqlserver.SQLServerDriver

     SQL Server 2005: com.microsoft.sqlserver.jdbc.SQLServerDriver
   - For the JDBC URL, enter:

     Oracle: jdbc:oracle:thin:@*wf_db_systemName*:1521:*wf_oracle_SID*

     SQL Server: jdbc:microsoft:sqlserver://*wf_db_systemName*:1433; databaseName=*wf_db_name*

     SQL Server 2005: jdbc:sqlserver://*wf_db_systemName*:1433; databaseName=*wf_db_name*
   - For the Database User ID parameter, enter the workflow user you created when creating the workflow database.
   - For the Password parameter, enter the password you created for the workflow user.
   - For the Database ID, enter WPDS
5. Accept the default check box selections.
6. Click the Initialize button.

   When the configuration is complete, a message that resembles the following appears in the Command Prompt window:

   The create database process finished with 0 errors.
7. Restart the application server.

Appendix C: Installation Worksheet

This section contains the following topics:

Collect Information for an Identity Manager Installation

Use the following worksheets to collect information about your system before installing Identity Manager.

WebLogic Information

Record the following WebLogic information you need during the Identity Manager installation:

Field Name	Description	Your Response
WebLogic Binary Folder	The location of the application server home directory.	
Domain Folder	The name of the WebLogic domain you created for Identity Manager. **Default:** mydomain	
Server Name	The name of the WebLogic server on which the domain is configured. **Default:** myserver	
Cluster Name	The cluster name for high-availability implementations. This is only needed if you plan on installing Identity Manager in a clustered environment. **Note:** For more information on clustering, see the *High-Availability Guide*.	

Field Name	Description	Your Response
App Server URL and port	The application URL and port number of the system that will host the Identity Manager Server (system that will host the application server).	

Provisioning Information

Record the following Provisioning Directory information you need during the Identity Manager installation:

Field Name	Description	Your Response
Host	The hostname of the remote Provisioning Directory system.	
Port	The port number of a remote Provisioning Directory system.	
User Password	The remote Provisioning Directory user password.	
Domain Name	The domain name for the Provisioning Directory. This is required for both local and remote Provisioning Directory installations. **Default:** IDENTITY_MANAGER **Note:** You should not change the domain unless you are connecting to an existing domain.	

Database Information

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

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

iRecorder Information

Record the following iRecorder information you need during the Identity Manager installation:

Field Name	Description	Your Response
Host name or IP of Audit Client or iRouter	The hostname or IP address of the iRouter used by CA Security Command Center or CA Audit.	

SiteMinder Information

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

Field Name	Description	Your Response
Policy Server Host Name	The hostname of the SiteMinder Policy Server.	
SiteMinder Administrator Name	The administrator username for the SiteMinder Policy Server.	
SiteMinder Administrator Password	The administrator user password for the SiteMinder Policy Server.	
SiteMinder Folder (Solaris Only)	The location of SiteMinder on the system with a SiteMinder Policy Server installed.	

Important! When installing Identity Manager with SiteMinder, the installation does not prompt the user for the Web Agent name. Instead, the installer refers to the generic username as the agent name and the generic password as the agent shared secret. To connect to an existing SiteMinder deployment with set agent credentials, edit the ra.xml file under the "IdentityMinder.ear\policyserver.rar\META-INF" folder and set the AgentName and AgentSecret properties to the correct values.

Reporting Information

Record the following information you need during the IAM Report Server installation:

Field Name	Description	Your Response
Report Server Administrator Password	The installer automatically creates an administrator account for the IAM Report Server. Determine the password for this account.	
Database Host Name and Port	Identify the server where the Reporting Database is installed.	

Field Name	Description	Your Response
DSN Name	Identify the name of the DSN that the report server is to use to communicate with the Reporting Database.	
Database Name	Identify the Reporting Database name.	
Database Username	Identify the username for the Reporting Database.	
Database Password	Identify the administrative password credentials for the Reporting Database.	
TNS Name	The name of the TNS that the IAM Report Server is to use to communicate with the Reporting Database. **Note:** This information is needed only if you are using Oracle.	
Pre-Installed Tomcat Information	Identify the path and port numbers for any previous installation of Tomcat. If you do not want to use a previous installation of Tomcat, IAM Report Server installer can install Tomcat.	
Tomcat Port Number	The Tomcat connection, redirect, and shutdown ports. **Note:** If you are installing the IAM Report Server on the same system as the Identity Manager, ensure that the Tomcat connection port does not conflict with the port number you specified for the application server URL when installing the Identity Manager.	

Appendix D: Installation Checklists

Use the following checklists in this appendix in the order they appear to help you install and configure Identity Manager. You may want to print the checklists and check off the steps as you complete them.

This section contains the following topics:

How to Install Prerequisite Components

To install the prerequisite hardware and software for Identity Manager:

✓	Step
	1. Confirm that the system that will host Identity Manager satisfies the hardware requirements.
	2. Review the software prerequisites for Identity Manager.
	3. Create a database for Identity Manager.
	4. Confirm that the application server that will host Identity Manager is installed and configured correctly.

How to Install Identity Manager Components

Use the following checklist to install the components of Identity Manager:

✓	Step
	1. Gather information needed for the installation program.
	2. Check if any Identity Manager Cumulative Releases exist.
	3. Review important notes prior to the Identity Manager installation.
	4. Install the Identity Manager components.
	5. Install the Identity Manager Bookshelf.

Important! If you are going to use SiteMinder, see the chapter on Protecting Identity Manager with SiteMinder and follow the steps to configure SiteMinder to work with Identity Manager.

How to Start Identity Manager

After you install the Identity Manager software components, perform the following steps to start the Identity Manager Server for the first time:

Step
1. Start the Identity Manager Server.
2. Confirm that Identity Manager started correctly.

How to Protect Identity Manager with SiteMinder

The following table describes the steps involved in protecting Identity Manager resources:

✓	Step
	1. Install and configure a SiteMinder Agent to protect Identity Manager resources.

✓	Step
	2. Install the plug-in the Web Server uses to forward requests to the application server.
	3. Verify that the plug-in is successfully forwarding requests to the application server.
	4. Configure the SiteMinder Policy Store for use with Identity Manager.

How to Configure Provisioning

Perform the following steps to configure Identity Manager provisioning:

	Step
	1. If your Provisioning Server is remote (not on the same system as the Provisioning Manager), run the Provisioning Manager setup.
	2. Configure the Identity Manager Server and notifications within the Provisioning Manager.
	3. Consider optional Provisioning Components to install.

How to Configure Email Notification

The following checklist describes the steps to configure Identity Manager's email notification feature:

✓	Step
	1. Configure SMTP for the application server.
	2. Enable email notification through the Management Console

How to Configure Workflow

The following checklist describes the steps to configure Identity Manager's workflow feature:

✓	Step
	1. Enable workflow in the Management Console
	2. (Optional) Configure WorkPoint Administrative Tools if you plan to use WorkPoint Designer.

How to Install Reporting

The following checklist describes the steps to install Identity Manager's reporting feature:

✓	Step
	1. Ensure you have reviewed the reports pre-installation checklist.
	2. Gather reporting information.
	3. Install the IAM Report Server (Business Objects)
	4. Copy the jdbc JAR files.
	5. Run the command line to deploy the default reports.

Note: For more information on configuring reporting after the installation, see the *Administration Guide*.

How to Configure Internationalization

To configure Identity Manager for internationalization, complete the following steps:

✓	Step
	1. Confirm that the system hosting Identity Manager satisfies the prerequisites.

✓	Step
	2. (Optional) Configure the SiteMinder Web Agent for Internationalization.

How to Uninstall Identity Manager

The following checklist describes the steps to uninstall Identity Manager:

✓	Step
	1. Delete Identity Manager objects from the policy store.
	2. (Optional) Remove the Identity Manager schema from the policy store.
	3. Uninstall the Identity Manager components.
	4. Remove Identity Manager configuration information from the application server.

Appendix E: Changing the WorkPoint RMI Port

The WorkPoint General Monitor implements certain WorkPoint features, such as delay node processing, asynchronous script processing, alert monitoring, and email generation. The port number for the General Monitor RMI connection is specified in several locations.

To change the settings, modify the following properties files:

Properties File	Location	Setting
GeneralMonitor.properties	*Identity Manager.ear* \workflow_rar	RMI_Port
LicenseServer.properties	*Identity Manager.ear* \workflow_rar	rmi.port
workpoint-client.properties	*Identity Manager.ear* \workflow_rar	license.port
workpoint-server.properties	*Identity Manager.ear*\ wpServer.jar **Note:** To modify the workpoint-server.properties, extract the file from the wpServer.jar, change the license.port setting, and add the properties file to the .jar file.	license.port

In this table, *Identity Manager.ear* is the installed location of the Identity Manager.ear directory. For example, the Windows default is:
c:\bea\user_projects\domains*im_domain*\applications\Identity Manager.ear

Index

I

J

L

M

O

P

R

S

U

V

W