CA IdentityMinder™

Installation Guide (WebSphere)

12.6.4

CA Technologies Product References

This document references the following CA Technologies products:

- CA CloudMinder™ Identity Management
- CA Directory
- CA IdentityMinder ™
- CA GovernanceMinder (formerly CA Role & Compliance Manager)
- CA SiteMinder®
- CA User Activity Reporting
- CA AuthMinder ™

Contact CA Technologies

Contact CA Support

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

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

Providing Feedback About Product Documentation

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

To provide feedback about CA Technologies product documentation, complete our short customer survey which is available on the CA Support website at http://ca.com/docs.

Contents

Chapter 1: Installation Overview

This guide provides instructions for installing CA IdentityMinder and also includes information about optional components for installation such as Provisioning and CA SiteMinder.

This section contains the following topics:

Sample CA IdentityMinder Installations

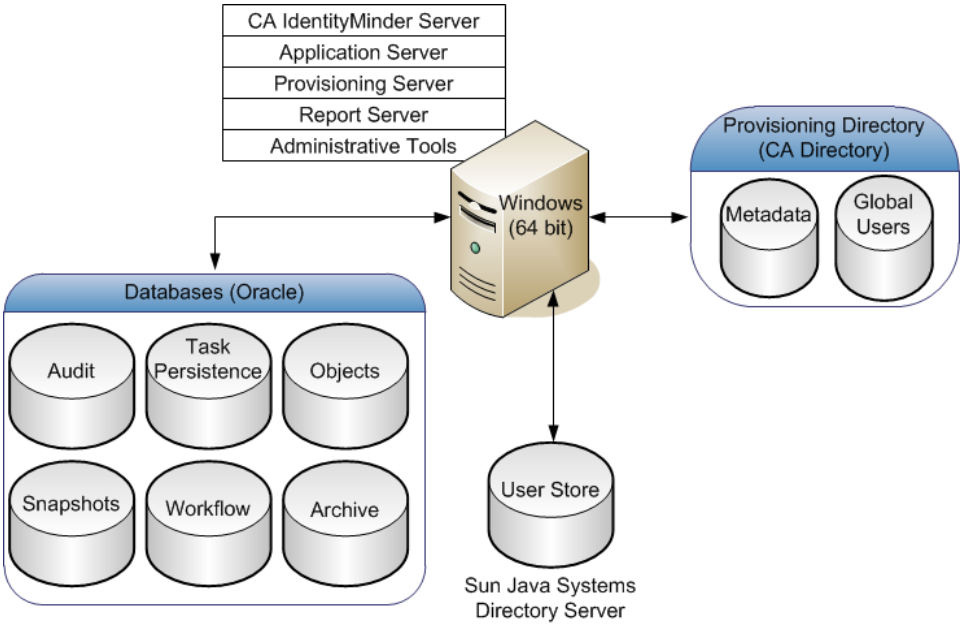
With CA IdentityMinder, you can control user identities and their access to applications and accounts on endpoint systems. Based on the functionality you need, you select which CA IdentityMinder components to install.

In all CA IdentityMinder installations, the CA IdentityMinder Server is installed on an application server. You use the CA IdentityMinder Installer to install the other components you need.

The following sections illustrate some examples of CA IdentityMinder implementations at a high level.

Example: Single Node Installation

In a single node installation, the CA IdentityMinder Server is installed on one application server node. Also, one copy of each provisioning component is installed, but components can be on different systems. The following figure is an example of a single node CA IdentityMinder installation with a Provisioning Server on the same system and a Provisioning Directory on another system:



This example also illustrates choices for platforms. In this case:

- The CA IdentityMinder server is installed on Windows.
- The user store is on the Sun Java Systems Directory server.
- The databases are on Oracle

These platforms are only examples. You can select other platforms instead.

CA IdentityMinder Server

Executes tasks within CA IdentityMinder. The J2EE CA IdentityMinder application includes the Management Console (for configuring environments), and the User Console (for managing an environment).

CA IdentityMinder Administrative Tools

Provides tools and samples for configuring and using CA IdentityMinder. The tools include Connector Xpress, the Java Connector Server SDK, configuration files, scripts, utilities, and JAR files that you use to compile custom objects with CA IdentityMinder APIs and API samples. The Provisioning Manager and WorkPoint Designer are also included with the Administrative Tools.

The default installation location for most Administrative Tools follows:

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

However, the default location for Provisioning Manager, which is only installed on Windows, follows:

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

Note: The Tools\db directory also includes a document that describes the database schema.

Report Server

Uses CA Business Intelligence. You use this server to include data from the Snapshot Database, which contains information from the CA IdentityMinder Object Store and the CA IdentityMinder user store. An example of a Snapshot Report is the User Profile report. You can also create reports with a disabled snapshot applied, which include data from other data sources, such as the Audit Database.

CA IdentityMinder Databases

Store data for CA IdentityMinder. The databases store information for auditing, task persistence, snapshots (reporting), workflow, and CA IdentityMinder objects. Each database must be a relational database.

Note: For a complete list of supported relational databases, see the CA IdentityMinder support matrix on the CA Support Site.

CA IdentityMinder User Store

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

Note: For more information about setting up a user store for CA IdentityMinder, see the *Configuration Guide*.

CA IdentityMinder Provisioning Server

Manages accounts on endpoint systems. On the same system or another system, you can also install Connector Servers, which manage Java or C++ based connectors to endpoints.

CA IdentityMinder Provisioning Directory

Specifies the Provisioning Directory schema to CA Directory. This schema sets up the Directory System Agents (DSAs) within CA Directory. The CA IdentityMinder user store can also be the Provisioning Directory.

CA IdentityMinder Provisioning Manager

Manages the Provisioning Server through a graphical interface. This tool is used for administrative tasks such as synchronizing accounts with account templates. The Provisioning Manager is installed as part of the CA IdentityMinder Administrative Tools or can be installed separately from those tools.

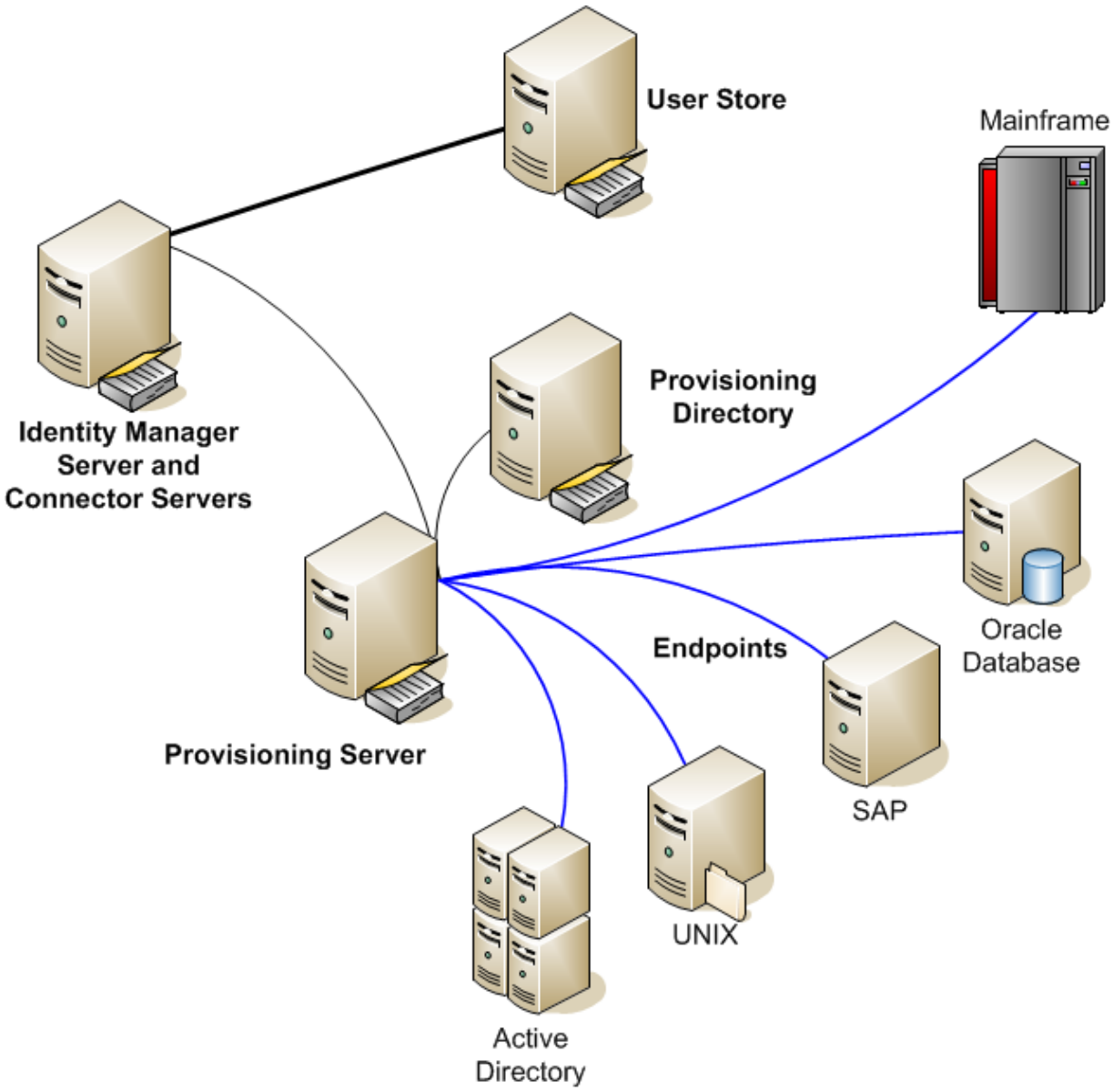
Note: This application runs on Windows only.

Example: Installation with Multiple Endpoints

Installing a Provisioning Server allows administrators to provision accounts on endpoints such as email servers, databases, and other applications to end users. To communicate with the endpoint systems, you install connector servers for endpoint-specific connectors, such as an SAP connector.

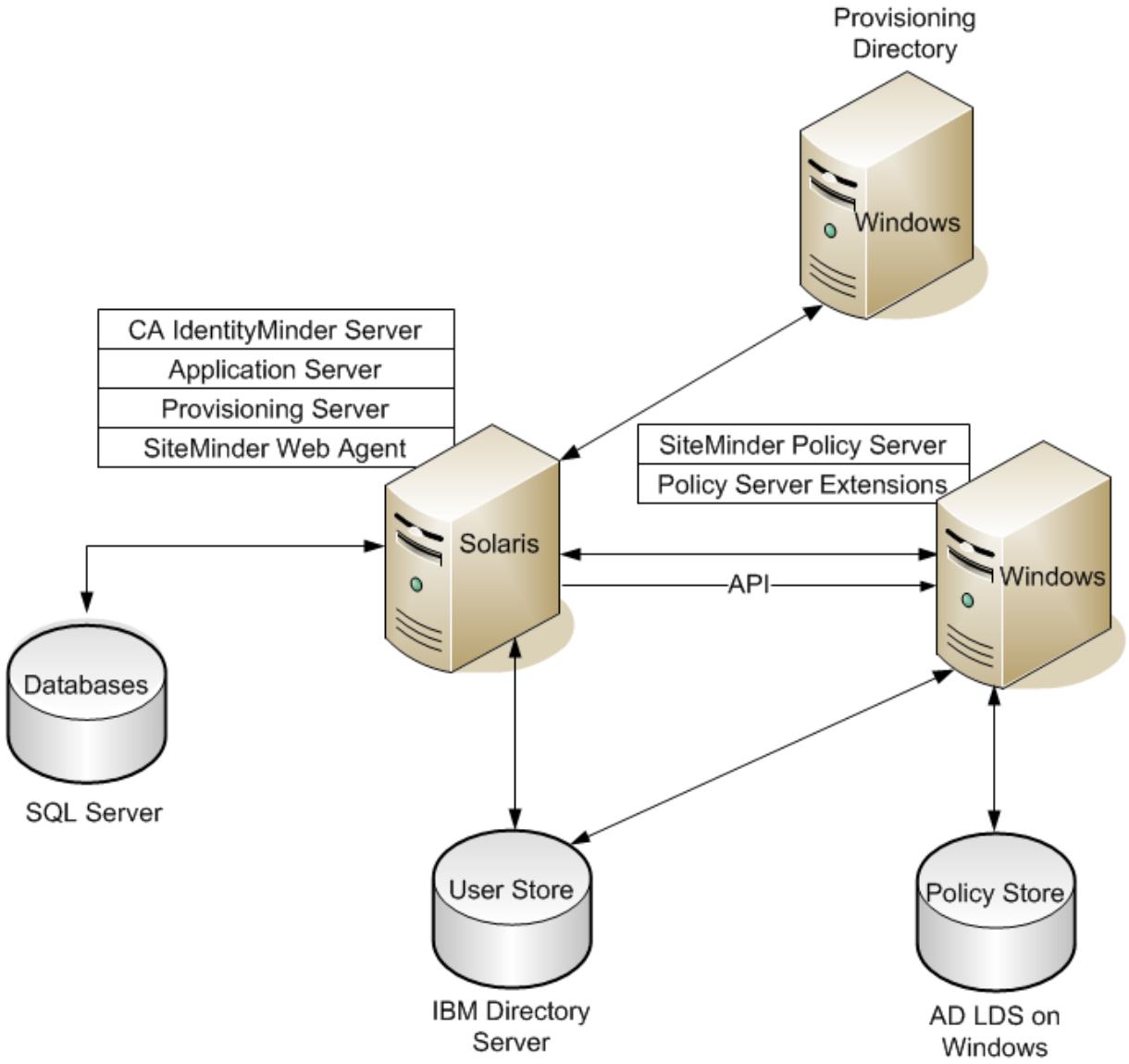
A typical installation scenario involves separate systems for the user store and the Provisioning Directory, which remained synchronized.

This example illustrates the use of CA IdentityMinder to provide access to accounts on Active Directory, UNIX, SAP, Oracle, and mainframe systems.



Example: SiteMinder and CA IdentityMinder Installation

CA IdentityMinder can be integrated with a SiteMinder Policy Server, which provides advanced authentication and protection for your environments. The following figure is an example of a CA IdentityMinder installation that uses a CA SiteMinder Policy Server for authentication and authorization:



The SiteMinder elements are defined as follows:

SiteMinder Web Agent

Works with the SiteMinder Policy Server to protect the User Console. Installed on the system with the CA IdentityMinder Server.

SiteMinder Policy Server

Provides advanced authentication and authorization for CA IdentityMinder and facilities such as Password Services, and Single Sign-On.

SiteMinder Policy Server Extensions

Enable a SiteMinder Policy Server to support CA IdentityMinder. Install the extensions on each SiteMinder Policy Server system in your CA IdentityMinder implementation.

The CA IdentityMinder components are defined in the previous example on a single node installation; however, in this example, the components are installed on different platforms. The CA IdentityMinder databases are on Microsoft SQL Server and the user store is on the IBM directory Server. The SiteMinder Policy Store is on AD LDS on Windows, which is one of several supported platforms for a policy store.

High Availability Installation

Before you install CA IdentityMinder, consider the goals for your implementation. For example, one goal could be a resilient implementation that consistently provides good performance. Another goal could be scalability.

A high-availability implementation provides the following features:

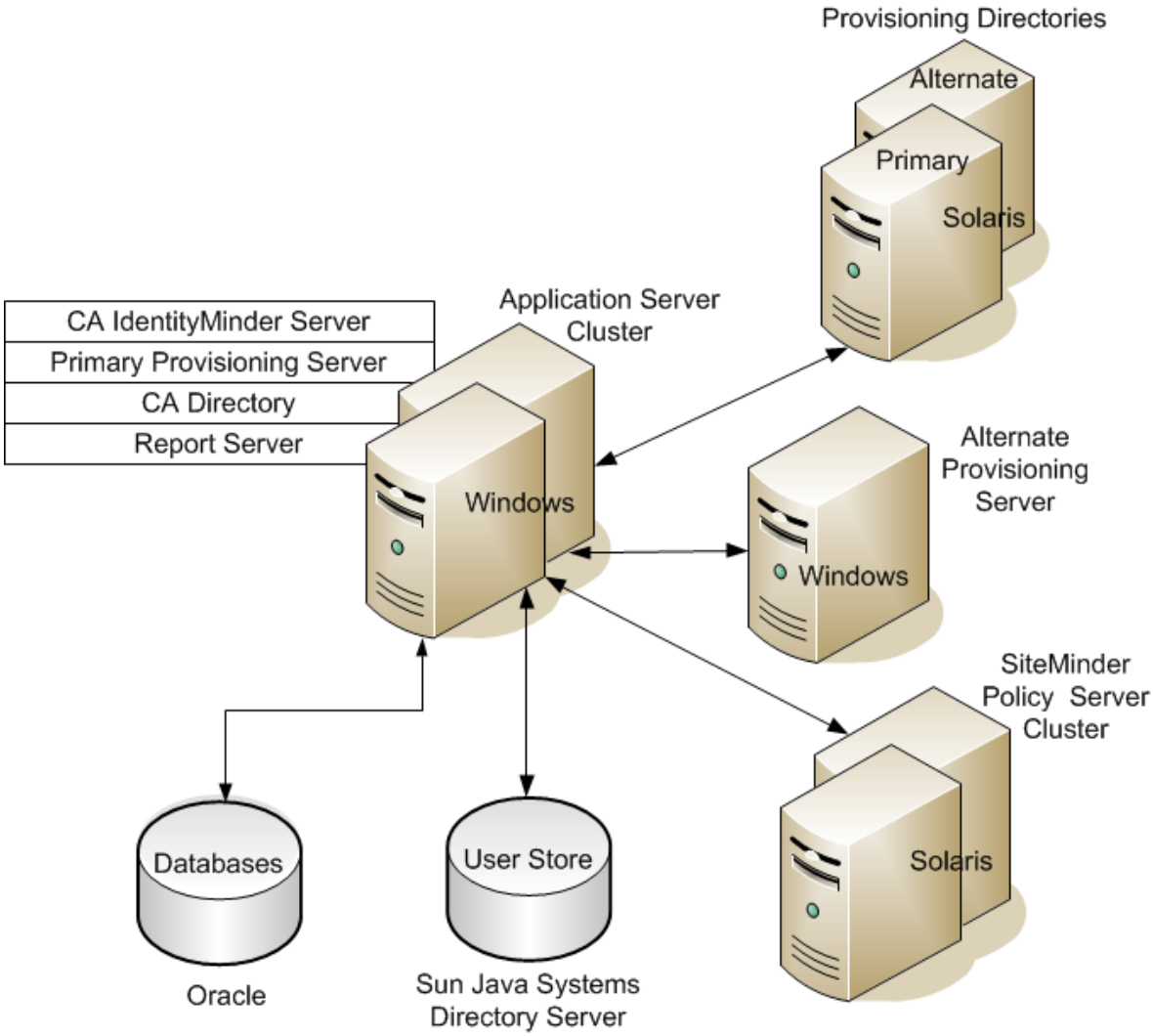
- Failover—Switches to another system automatically if the primary system fails or is temporarily offline for any reason.
- Load balancing—Distributes processing and communications activity evenly across a computer network so that performance remains good and no single device is overwhelmed.
- Various deployment tiers that provide the flexibility to serve dynamic business requirements.

To provide these high-availability features, the following implementation options exist:

- The CA IdentityMinder Server can be installed on an application server cluster to allow the failover to any of the node in the cluster, providing uninterrupted access to users. The application server can be a 64-bit format, which provides better performance than a 32-bit application server.
- The Provisioning Server uses a CA Directory router to route traffic to a Provisioning Directory.
- CA IdentityMinder includes connector servers that you configure per-directory or per-managed systems. Installing multiple connector servers increases resilience. Each connector server is also an LDAP server, similar to the Provisioning Server.

Example: High Availability Installation

The following diagram is an example that provides high availability for the CA IdentityMinder Server, Provisioning Server, Provisioning Directory, and SiteMinder Policy Server. The use of alternate components and clusters provide the high availability features.



In addition to illustrating high availability, this figure shows the different platforms that are used for the components comparing to the SiteMinder illustration. For example, the database uses Oracle instead of Microsoft SQL Server, which appeared in the previous illustration.

CA IdentityMinder Server Architecture

A CA IdentityMinder implementation may span a multi-tiered environment that includes a combination of hardware and software, including three tiers:

- Web Server tier
- Application Server tier
- Policy Server tier (optional)

Each tier may contain a cluster of servers that perform the same function to share the workload for that tier. You configure each cluster separately, so that you can add servers only where they are needed. For example, in a clustered CA IdentityMinder implementation, a group of several systems may all have a CA IdentityMinder Server installed. These systems share the work that CA IdentityMinder Server has performed.

Note: Nodes from different clusters may exist on the same system. For example, an application server node can be installed on the same system as a Policy Server node.

Provisioning Components Architecture

Provisioning provides high availability solutions in the following three tiers:

- Client tier

  The clients are the CA IdentityMinder User Console, CA IdentityMinder Management Console and the Provisioning Manager. You can group clients that are together based on their geographic locations, organizational units, business functions, security requirements, provisioning workload, or other administration needs. Generally, we recommend keeping clients close to the endpoints they manage.

- Provisioning Server tier

  Clients use primary and alternate Provisioning Servers, in order of their failover preference. Client requests continue to be submitted to the first server until that server fails. In other words, the connection stays active until the server fails. If a failure occurs, the client reviews the list of configured servers in order of preference to find the next available server.

The Provisioning Server can have multiple connector servers in operation. Each connector server handles operations on a distinct set of endpoints. Therefore, your organization could deploy connector servers on systems that are close in the network to the endpoints. For example, assume that you have many UNIX /etc endpoints. In such case, install one connector server on each server so that each connector server controls only the endpoints on the server where it is installed.

Installing Connector Servers close to the endpoints also reduces delays in managing accounts on endpoints.

- CA Directory tier (Provisioning Directory)

  Provisioning Servers uses a CA Directory router to send requests to primary and alternate Provisioning Directories in order of preference.

Overall Installation Process

To install CA IdentityMinder, perform the following steps:

1. Install the prerequisite hardware and software and configure your system as required.
2. Install the CA IdentityMinder Server on a single node or an application server cluster.
3. (Optional) Configure separate databases.
4. (Optional) Install the report server.
5. (Optional) Install alternate Provisioning Directories, alternate Provisioning Servers, and connector servers for high availability provisioning capabilities.

Note: In this document, each chapter includes a checklist of the steps to install or configure a CA IdentityMinder feature or component. That section begins with a How To title.

Chapter 2: Installation 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 and configure your system as required.**
	2. Perform one of these installations: ■ Single node installation ■ Installation on an application server cluster.
	3. (Optional) Create separate databases.
	4. (Optional) Install the Report Server.
	5.(Optional) Install alternate Provisioning Directories, alternate Provisioning Servers, and connector servers to support the failover and load balancing.

Prerequisite Knowledge

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

- An understanding of J2EE application servers and multi-tier architecture
- Experience with installing and managing the application server, including tasks such as the following:
  - Starting the application server
  - Installing a single node
  - Installing cluster to support high availability
- 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 CA IdentityMinder required for either a standalone or cluster installation:

✓	Step
	1. Verify that your system meets the hardware requirements.
	2. Install CA Directory.
	3. (Optional) Create a FIPS key.
	4. (Optional) Create an encryption parameters file.
	5. (Optional) Integrate with SiteMinder.
	6. Create a database.
	7. Set up the application server.
	8. Meet requirements if installing on Solaris or Linux.
	9. Meet IPv6 requirements if installing on IPv6 systems.
	10. Complete the Installation Worksheets with information you need for the CA IdentityMinder installation program.

Check Hardware Requirements

CA IdentityMinder Server

These requirements take into account the requirements of the application server that is installed on the system where you install the CA IdentityMinder Server.

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

Provisioning Server or a Standalone Connector Server

Component	Minimum	Recommended
CPU	Intel (or compatible) 2.0 GHz (Windows or Red Hat Linux) SPARC 1.5 GHz (Solaris)	Dual core Intel (or compatible) 3.0 GHz (Windows or Red Hat Linux) SPARC 2.0 GHz (Solaris)
Memory	4 GB	8 GB
Available Disk Space	4 GB	8 GB
Processor	64-bit processor and operating system for intermediate and large deployments, dual core	64-bit processor and operating system, quad core

Provisioning Directory

Component	Minimum	Recommended
CPU	Intel (or compatible) 1.5 GHz (Windows or Red Hat Linux) SPARC 1.0 GHz (Solaris)	Dual core Intel (or compatible) 2.5 GHz (Windows or Red Hat Linux) SPARC 1.5 GHz (Solaris)
Memory	4 GB	8 GB
Available Disk Space	2 to 10 GB, depending on the number of endpoint accounts ■ Compact—Up to 10,000 accounts, 0.25 GB per data file (total 1 GB) ■ Basic—Up to 400,000 accounts, 0.5 GB per data file (total 2 GB) ■ Intermediate—Up to 600,000 accounts, 1 GB per data file, total 4 GB ■ Large—Over 600,000 accounts, 2 GB per data file, total 8 GB	2 to 10 GB, depending on the number of endpoint accounts ■ Compact—Up to 10,000 accounts, 0.25 GB per data file (total 1 GB) ■ Basic—Up to 400,000 accounts, 0.5 GB per data file (total 2 GB) ■ Intermediate—Up to 600,000 accounts, 1 GB per data file, total 4 GB ■ Large—Over 600,000 accounts, 2 GB per data file, total 8 GB
Processor	64-bit processor, 64-bit operating system, and CA Directory (64-bit version) for intermediate and large deployments	64-bit processor and operating system

All Components on One System

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

Component	Minimum
CPU	Intel (or compatible) 3.1 GHz (Windows or Red Hat Linux) SPARC 2.5 GHz (Solaris)
Memory	8 GB
Available Disk Space	6 to 14 GB depending on the number of accounts

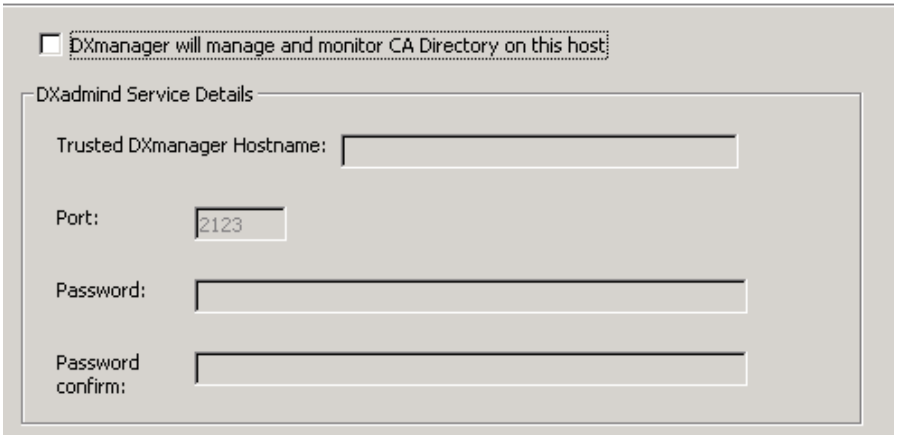
Component	Minimum	
Processor		64-bit processor and operating system, quad core
Swap/Paging Space	6 GB	

Install CA Directory

Before you install CA IdentityMinder, install CA Directory using the following steps:

1. Install CA Directory on the system where you plan to install the Provisioning Directory. A supported version of CA Directory is included on your installation media. For details on installation, download the CA Directory documentation from the support site.

   Note: When the installer asks about installing dxadmind for DXManager, you can safely clear this option. The Provisioning Directory does not use DXManager.



2. Install a second copy of CA Directory on the system where you plan to install the Provisioning Server. This installation is for routing purposes, so that the Provisioning Server can communicate with the remote Provisioning Directory.

Important! We recommend that you disable all antivirus software before installation. During the installation, If antivirus software is enabled, problems can occur. Verify that you enable your antivirus protection again after you complete the installation.

Create a FIPS 140-2 Encryption Key

When you run the CA IdentityMinder installer, you are given the option of enabling FIPS 140-2 compliance mode. For CA IdentityMinder to support FIPS 140-2, all components in a CA IdentityMinder environment must be FIPS 140-2 enabled. You need a FIPS encryption key to enable FIPS 140-2 during installation. A Password Tool for creating a FIPS key is located in the installation media at PasswordTool\bin.

Important! Use the same FIPS 140-2 encryption key in all installations. Verify that you safeguard the Password Tool generated key file immediately.

If you are using SiteMinder, be sure to set the ra.xml file correctly after CA IdentityMinder installation. See the procedure Adding SiteMinder to an Existing CA IdentityMinder Deployment in the *Configuration Guide*.

Create an Encryption Parameters File

During installation of the CA IdentityMinder server, you have the option to set encrypting parameters. You use this feature to customize encryption code by supplying user-defined parameters such as the key length for every encryption algorithm used by CA IdentityMinder, seed size and IV size for FIPS encryption key and the whole keys for non-FIPS algorithms - RC2 and PBE.

The parameters should be supplied as a properties file with the following possible keys: PBKey, PBSalt, PBKeySize, RCKey, RCKeySize, AEKey, AEKeySize, AESeedSize, AEIVSize.

Valid key size values allowed by the encryption algorithms are as follows:

- For PBE and RC2, the maximum key length is 128 bytes.
- For AES, the valid key sizes are 16, 24, and 32 bytes.

Important! Use the same Encrypting Parameters in all installations. You should not change encrypting parameters after installation.

(Optional) Integrate with SiteMinder

A SiteMinder Policy Server is an optional component that you install as described in the *CA SiteMinder® Installation Guide*. If you plan to make the Policy Server highly available, you configure it as a Policy Server cluster. You also install JCE libraries to enable communication with CA IdentityMinder.

To install a Policy Server:

1. Install the SiteMinder Policy Server. For details, see the *CA SiteMinder Policy Server Installation Guide*.
2. To make the Policy Server highly available, install it on each node that should be in the Policy Server cluster.

   Note: Each Policy Server in the cluster uses the same policy store.
3. Verify that you can ping the systems that host the Policy Server from the system where you plan to install the CA IdentityMinder Server.

To install the CA IdentityMinder Extensions for SiteMinder:

Before you install the CA IdentityMinder server, you add the extensions to each Policy Server. Assume that the Policy Server is on the system where you planned to install the CA IdentityMinder server. Then, you can install the extensions and the CA IdentityMinder server simultaneously. If so, omit this procedure.

1. Stop the CA SiteMinder services.
2. Set your default directory location to the root of the SiteMinder installation area.
3. Issue the following command:

   ```
   ./stop-all
   ```

   All SiteMinder executables shut down.
4. Install the CA IdentityMinder Extensions for SiteMinder. Do one of the following tasks:

   - **Windows:** From your installation media, run the following program in the top-level folder:
     `ca-im-release-win32.exe`
   - **UNIX:** From your installation media, run the following program in the top-level folder:
     `ca-im-release-sol.bin`

   release represents the current release of CA IdentityMinder.

5. Select Extensions for SiteMinder.
6. Complete the instructions in the installation dialog boxes.
7. Issue the following command:

   ```
   ./stop-all
   ```

   All SiteMinder executables shut down.
8. Issue the following command:

   ```
   ./start-all
   ```

   All SiteMinder executables start.

To install JCE Libraries:

The CA IdentityMinder server requires the Java Cryptography Extension (JCE) libraries if you are also using CA SiteMinder.

Before you install the CA IdentityMinder Server, perform these steps:

1. Download and install the Java Cryptography Extension Unlimited Strength Jurisdiction Policy Files.
2. Select the one that works with your application server and JDK.

   The download ZIP file includes a readme text file with installation instructions.

Create the Database

CA IdentityMinder requires a relational database to store objects and data for auditing, snapshots (reporting), workflow, and task persistence. Install a supported version of Oracle or Microsoft SQL Server and create a database.

When installing CA IdentityMinder, all of the database schemas are created automatically when the application server is started. However, after installing CA IdentityMinder, you can configure separate databases for auditing, snapshots (reporting), workflow, and task persistence. To create these databases, see the chapter on Separate Database Configuration.

Note: We strongly recommend a separate database for task persistence. Using a separate database provides the best performance.

WebSphere Application Server

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

Install WebSphere

CA IdentityMinder 12.6.4 works with Websphere 7, 8.0 or 8.5. If you need a new version of the IBM WebSphere, install the WebSphere server as described in IBM's documentation. During the installation, perform these actions:

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

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

When you create Websphere cell and node names, remember they are case sensitive in all operating systems. Please confirm that these names are in the correct case when you install CA IdentityMinder.

Disable Global Security

We recommend that you disable security before the installation. Verify that the Security Enabled option is unchecked. This action will ensure that the profile can be created without a problem.

After installation, enable global security. Note that workflow requires a user for CORBA naming services when global security is enabled. You add an IDM workflow user to WebSphere. In the WebSphere administrative console, locate the Naming area. Under CORBA naming service users, add the user IDM with appropriate permissions.

Verify WebSphere

Use the following tests to verify that WebSphere is working:

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

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

  For example:

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

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

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

  http://*hostname*/snoop

  For example:

  http://MyServer.MyCompany.com/snoop

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

For additional help with WebSphere, contact IBM customer support.

Configure WebSphere for CA IdentityMinder

Perform the following steps to ensure that your CA IdentityMinder installation succeeds on WebSphere.

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

Note: For more information, see your WebSphere documentation.

Important! Restart your WebSphere application server before starting the CA IdentityMinder installation.

Enable XA Transactions for Microsoft SQL Server

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

Follow these steps:

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

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

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

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

Configure SSL

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

Solaris Requirements

Provisioning Server Requirements

Verify /etc/system and verify the following minimum IPC kernel parameter values:

- set msgsys:msginfo_msgmni=32
- set semsys:seminfo_semmni=256
- set semsys:seminfo_semmns=512
- set semsys:seminfo_semmnu=256
- set semsys:seminfo_semume=128
- set semsys:seminfo_smmsl=128

- set shmsys:shminfo_shmmni=128
- set shmsys:shminfo_shmmin=4

Solaris 9 or 10 Requirements

Before installing provisioning software on Solaris 9 or 10, download and install the required patches.

1. Download the Sun Studio 10 patches for the Provisioning SDK from the following location:

   `http://developers.sun.com/prodtech/cc/downloads/patches/ss10_patches.html`

2. Download and install patch 117830.

   Note: Sun Studio 11 does not require patching.

3. Download Solaris 9 patches for all Provisioning components from the following location:

   `http://search.sun.com/search/onesearch/index.jsp`

4. Download and install 9_recommended.zip.

Linux Requirements

These requirements exist on a Linux system. If you have registered your Red Hat installation, we recommend that you use yum to install the packages. Otherwise, you can use rpm to install the packages.

Alternatively, use Add/Remove Software to resolve the dependencies, and unchecking the Only Native Packages filter option. Using this approach, you select and install the required i686 architecture dependencies.

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

CA IdentityMinder Server

Red Hat 5.x	Red Hat 6.x
glibc-2.5-65.i686.rpm	glibc-2.12-1.47.el6.i686.rpm
libXext-1.0.1-2.1.i386.rpm	libXext-1.1-3.el6.i686.rpm
libXtst-1.0.1-3.1.i386.rpm	libXtst-1.0.99.2-3.el6.i686.rpm
ncurses-devel-5.5-24.20060715.i386.rpm	ncurses-devel-5.7-3.20090208.el6.i686.rpm
ksh-20100202-1.el5_6.6.x86_64.rpm	ksh-20100621-12.el6.x86_64.rpm

Provisioning Server

Red Hat 5.x	Red Hat 6.x
compat-libstdc++-296-2.96-138.i386.rpm	compat-libstdc++-296-2.96-144.el6.i686.rpm
libstdc++-4.1.2-51.el5.i386.rpm	libstdc++-4.4.6-3.el6.i686.rpm
libidn-0.6.5-1.1.i386.rpm	libidn-1.18-2.el6.i686.rpm
libgcc-4.1.2-52.el5.i386.rpm	libgcc-4.4.6-3.el6.i686.rpm

CA IAM Connector Server

For Red Hat 5.x, no packages are required for the CA IAM CS. For Red Hat 6.x, install these packages in this order:

1. glibc-2.12-1.25.el6.i686.rpm
2. libX11-1.3-2.el6.i686.rpm
3. libxcb-1.5-1.el6.i686.rpm
4. libXtst-1.0.99.2-3.el6.i686.rpm
5. libXau-1.0.5-1.el6.i686.rpm
6. libXi-1.3-3.el6.i686.rpm
7. libXext-1.1-3.el6.i686.rpm
8. nss-softokn-freebl-3.12.9-3.el6.i686.rpm
9. libXmu-1.0.5-1.el6.i686.rpm
10. libXft-2.1.13-4.1.el6.i686.rpm
11. libXpm-3.5.8-2.el6.i686.rpm

Linux and FIPS

On a Linux system with FIPS enabled, ensure that sufficient entropy is available. CA IdentityMinder requires random data from /dev/random to perform essential cryptographic functions. If data in /dev/random is exhausted, CA IdentityMinder processes must wait for random data to be available. This waiting results in poor performance. Use rngd and rng-tools to ensure that /dev/random has sufficient data and reading processes are not blocked.

IPv6 Support

CA IdentityMinder supports IPv6 on the following operating systems:

- Solaris 10
- Windows XP SP2 or higher
- Windows 2003 SP2 or higher
- Windows 2008 or higher

Note: CA IAM CS does not support IPv6 on Microsoft Windows platforms. No JDK is available to work with IPv6 as of release time for CA IdentityMinder 12.6.4. If a JDK is released that works with IPv6, the CA IdentityMinder support matrix is updated on CA Support.

IPv6 Configuration Notes

Note the following points before configuring a CA IdentityMinder Environment that supports IPv6:

- For CA IdentityMinder to support IPv6 addresses, all components in the CA IdentityMinder implementation (including the operating system, JDK, directory servers, and databases) must also support IPv6 addresses.
- If CA IdentityMinder integrates with SiteMinder, the Web Server plug-in for the application server must also support IPv6.
- When you connect to SiteMinder or any database from CA IdentityMinder using a JDBC connection, specify the hostname not the IP address.
- The Report Server can be installed on a dual-stack host, which supports IPv4 and IPv6, but the communication to the server must be IPv4.
- When you configure a connection to the Report Server in the Management Console, the server name must be in IPv4 format.
- CA IdentityMinder does not support IPv6 link local addresses.
- In an IPv4/6 environment, if you want to configure CA Directory DSAs to listen on multiple addresses, add the additional addresses to your DSA knowledge files. For more information, see the CA Directory documentation.
- On a Windows 2008 system that uses IPv6, ensure that the IPv4 loopback address is enabled. Otherwise, the C++ Connector Server does not start.

Provisioning Directory on Windows 2008 with Pure IPv6 Not Supported

Due to a Sun Java Systems limitation, installing the Provisioning Directory on a Windows 2008 server with the IPv6 networking service uninstalled is not supported.

To work around with this issue, install the IPv6 service on the system and leave it disabled.

Complete the Installation Worksheets

The CA IdentityMinder installation program asks you for information about previously installed software and the software that you are installing. Verify that you provide hostnames (and not IP addresses) in the installer screens.

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

Provisioning Directory

Record the following Provisioning Directory and Provisioning Server information you need during the CA IdentityMinder installation.

Field Name	Description	Your Response
Provisioning Directory Hostname	The hostname of the Provisioning Directory system if it is remote. You need the hostnames for the primary and any alternate Provisioning Directories.	
Shared Secret	The special password for the Provisioning Directory. Use the same password for the primary and any alternate Provisioning Directories.	
Provisioning Server Hostname	The host names of the primary and any alternate Provisioning Servers.	

WebSphere Information

Record the following WebSphere information you need during the CA IdentityMinder installation:

Field Name	Description	Your Response
WebSphere Install Folder	The location of the application server home directory.	
Server Name	The name of the system on which the application server is running.	
Profile Name	The name of the profile you want to use for CA IdentityMinder.	

Field Name	Description	Your Response
Cell Name	The name of the cell in which the application server is located.	
Node Name	The name of the node in which the application server is located.	
Cluster Name	The cluster name for high-availability implementations. This is only needed if you plan on installing CA IdentityMinder in a clustered environment.	
Access URL and port	The application URL and port number of the system that will host the CA IdentityMinder Server (system that will host the application server).	

Database Connection Information

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

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

Field Name	Description	Your Response
Password	The password for the user account with administrative rights.	

Login Information

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

Field Name	Description	Your Response
Username	A username that you create to log in to the provisioning components. Avoid the username siteminder if you have that product installed. This name conflicts with CA SiteMinder.	
Provisioning Server password	A password for this Server.	
C++ Connector Server password	A password is needed for this server. Each C++ Connector Server can have a unique password.	
Provisioning Directory password	A password which Provisioning Server uses to connect to Provisioning Directory. For an alternate Provisioning Server, enter the Provisioning Directory password which is created for the primary Provisioning Server.	

SiteMinder Information

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

Field Name	Description	Your Response
Policy Server Host Name	The hostname of the SiteMinder Policy Server.	

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

UNIX and Console Mode Installation

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

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

release represents the current release of CA IdentityMinder

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

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

Non-Provisioning Installation

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

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

release represents the current release of CA IdentityMinder.

Chapter 3: Single Node Installation

This section contains the following topics:

Installation Status

This table shows you where you are in the installation process:

You Are Here	Step in Installation Process
	1. Install prerequisite hardware and software and configure your system as required.
X	**2. Perform one of these installations:** ■ **Single node installation** ■ **Installation on an application server cluster**
	3. (Optional) Create separate databases.
	4. (Optional) Install the Report Server.
	5.(Optional) Install alternate Provisioning Directories, alternate Provisioning Servers, and connector servers to support failover and load balancing.

CA IdentityMinder Components

In a single node installation, you install one copy of each component, but use two or more systems for where you install them.

Note: If you intend to install multiple copies of components for high availability, see the chapters on installation on a cluster and high-availability provisioning installation.

Install one of each of the following components on a system at your site:

- CA IdentityMinder Server—Installs the server that provides the core functionality of the product.
- CA IdentityMinder Administrative Tools—Installs tools such as the Provisioning Manager, which runs on a Windows system, the SDK for CA IAM CS, and Connector Xpress.

  Connector Xpress manages dynamic connectors, maps them to endpoints, and establishes routing rules. Dynamic connectors allow provisioning and management of SQL databases and LDAP directories.
- CA IdentityMinder Provisioning Server—Enables provisioning in CA IdentityMinder. Installation of this server includes the C++ Connector Server, which manages endpoints that use C++ connectors.
- CA IAM CS—Manages endpoints that use Java connectors. CA IAM CS is registered with the Provisioning Server when you install it.
- CA IdentityMinder Provisioning Directory Initialization—Configures a CA Directory instance to store provisioning data. Use the installation program on each system where CA Directory is installed.
- Extensions for SiteMinder—Extends the SiteMinder Policy Server if you are using it to protect CA IdentityMinder. Install these extensions on the same system as the Policy Server before you install the CA IdentityMinder Server.

How to Perform a Single Node Installation

Use the following checklist to perform a basic installation of CA IdentityMinder:

✓	Step
	1. Install CA IdentityMinder components on the systems required.
	2. Verify the CA IdentityMinder Server starts.
	3. Configure Provisioning Manager if installed on a remote system.
	4. Install optional provisioning components.

Install CA IdentityMinder Components

For a production environment, use separate systems for data servers. For example, we recommend that the Provisioning Directory and a database (SQL or Oracle) are on a separate system from the CA IdentityMinder Server and the Provisioning Server. If you are installing SiteMinder, you may also prefer to have it on a separate system. The Administrative Tools can be installed on any system.

Use the CA IdentityMinder installer to perform the installation on the systems required. In the procedures that follow, the step to run the installer refers to this program in your installation media's top-level folder:

- **Windows:**
  `ca-im-release-win32.exe`
- **UNIX:**
  `ca-im-release-sol.bin`

release represents the current release of CA IdentityMinder.

For each component that you install, be sure that you have the required information for installer screens, (see page 35) such as host names and passwords. If any issues occur during installation, check the installation logs (see page 163).

To install the Extensions for SiteMinder:

1. Log into the system where SiteMinder is installed as a Local Administrator (for Windows) or root (for Solaris).
2. Stop the SiteMinder services.
3. Run the installer and select Extensions for SiteMinder.

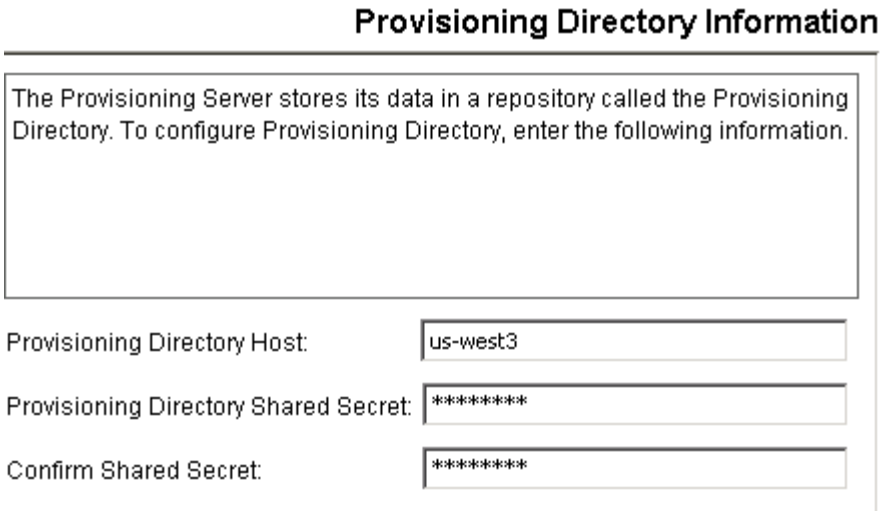
To install the CA IdentityMinder Server:

1. If you have installed SiteMinder on a separate system, be sure that you have installed the extensions for SiteMinder there also.
2. Log in to the system where the application server is installed as a Local Administrator (for Windows) or root (for Solaris).
3. Stop the application server.
4. Run the installer and select the CA IdentityMinder Server.
5. If you have SiteMinder on the local system, select Extensions for SiteMinder. If it is on a remote system, select Connect to Existing SiteMinder Policy Server.

To install the Provisioning Directory:

1. Log into the system as a Local Administrator (for Windows) or root (for Solaris).
2. Be sure that CA Directory is already installed on the system.

3. Run the installer and select the CA IdentityMinder Provisioning Directory Initialization.
4. Answer the question about deployment size. Consider the following guidelines, while allowing room for future growth:
   - Compact—up to 10,000 accounts
   - Basic—up to 400,000 accounts
   - Intermediate—up to 600,000 accounts
   - Large—more than 600,000 accounts
5. When you enter any password or shared secret in the installation, be sure to provide a password that you can recall when needed.



To install the Provisioning Server:

1. Log into the system as a Local Administrator (for Windows) or root (for Solaris).
2. Be sure that CA Directory is already installed and you have the details of the remote Provisioning Directory.
3. Run the installer and select the CA IdentityMinder Provisioning Server.

Configure Workflow for Your Profile

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

Follow these steps:

1. Start the WebSphere Console.
2. Navigate to Servers, Server Types, Application Servers, *server_name.*

3. Under Communications, Expand Ports.
4. Make note of the port used for the BOOTSTRAP_ADDRESS.
5. Edit Workpoint-client.properties file under iam_im.ear/config.

6. Locate the WebSphere section in this file.
   `# java.naming.provider.url=iiop://localhost:2809`
7. Replace 2809 with the profile's port that is used for the BOOTSTRAP_ADDRESS.
8. Restart this server.

Verify the CA IdentityMinder Server Starts

Follow these steps:

1. Start CA IdentityMinder as follows:
   - **Windows:**

     Click Start, Programs, IBM WebSphere, Application Server Network Deployment *version*, Profiles, Profile Name

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

- **UNIX:**

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

  b. Enter the following command:

  startserver *websphere_server*

  When you see a message that resembles the following, the server has completed its startup process:
  `Server server1 is open for e-business`

2. Access the Management Console and confirm the following points:
   - You can access the following URL from a browser:

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

     For example:

     http://MyServer.MyCompany.com:*port-number/*iam/immanage
   - The Management Console opens.
   - No errors are displayed in the application server log.
   - You do not receive an error message when you click the Directories link.
3. Verify that you can access an upgraded environment using this URL format:

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

Install Optional Provisioning Components

Optional Provisioning Components for CA IdentityMinder are in the im-pc-*release*.zip

release represents the current release of CA IdentityMinder.

The ZIP file includes the following:

Remote Agents

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

Password Synchronization Agents

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

Credential Provider

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

Bulk Loader Client/PeopleSoft Feed

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

CA IAM Connector Server SDK

Run the CA IAM Connector Server SDK installer from the CA IdentityMinder media (under \Provisioning) to install this component.

CCI Standalone

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

The CA IdentityMinder installer installs all connectors by default. However, in some cases, install an agent on an endpoint system you are managing before you can use the related connector.

Connectors run on the Provisioning Server and communicate with the systems managed by an endpoint. For example, systems running Active Directory Services (ADS) can be managed only if the ADS Connector is installed on the Provisioning Server.

Note: For more information about each connector, see the *Connectors Guide*

More information exists for these components in the following guides:

- Credential Provider (*Administration Guide)*
- Password Synchronization Agent (*Administration Guide)*
- Connector Xpress (*Connector Xpress Guide)*
- Agents for use with connectors (*Connectors Guide)*

Configure a Remote Provisioning Manager

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

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

Follow these steps:

1. Log in to the Windows system where you installed Provisioning Manager.
2. Go to Start, Programs, CA, IdentityMinder, Provisioning Manager Setup.

3. Enter the hostname of the Provisioning Server.
4. Click Configure.
5. For an alternate Provisioning Server, select the domain name from the pull-down list.
6. Click Ok.

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

Chapter 4: Installation on a WebSphere Cluster

This section contains the following topics:

Installation Status

This table shows you where you are in the installation process:

You Are Here	Step in Installation Process
	1. Install prerequisite hardware and software and configure your system as required.
X	**2. Perform one of these installations:** ■ **Single node installation** ■ **Installation on an application server cluster**
	3. (Optional) Create separate databases.
	4. (Optional) Install the Report Server.
	5. (Optional) Install alternate Provisioning Directories, alternate Provisioning Servers, and connector servers to support failover and load balancing.

WebSphere Cluster Setup

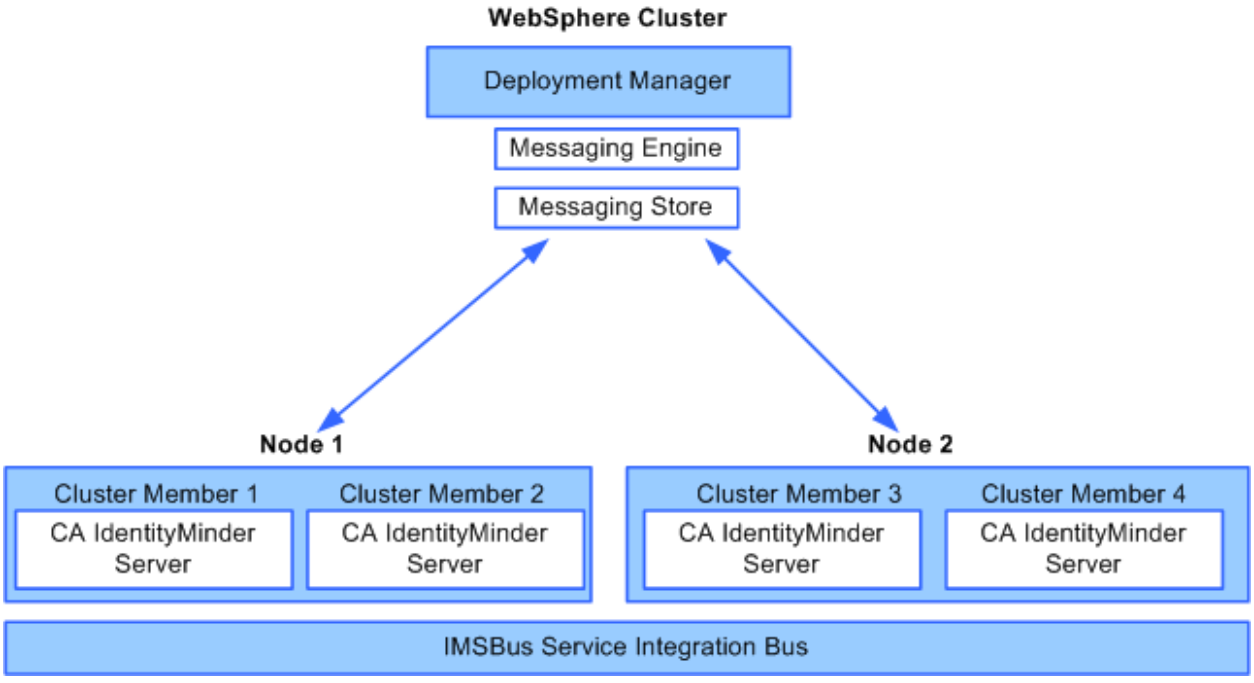
When you install software for a WebSphere cluster, you set up the following:

- One WebSphere Deployment Manager—Manages the other federated profiles in the cell through node agents.
- One or more nodes—Each node contains one or more cluster members (also called servers), which run the CA IdentityMinder Server.

- Node agent—A process that manages communication between the Deployment Manager and the federated profile.
- Service Integration Bus—Groups resources in WebSphere to simplify administration. The WebSphere cluster is added as a member of the bus.
- Message Engine—Provides messaging functionality for members of the service integration bus. One message engine exists for the cluster.
- Message Store—Stores messages and transaction status for the message engine.
- A Web Server—Distributes the load to the appropriate server and, if SiteMinder is installed, protects access to the cluster members.

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

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



WebSphere Cluster Prerequisites

Before you configure CA IdentityMinder on a WebSphere cluster, you should be familiar with the concepts and procedures for creating a WebSphere cluster. See the IBM WebSphere documentation for more information about WebSphere clusters.

Also, be sure you have performed the procedures in the "Installation Prerequisites" chapter.

Install WebSphere on each Node

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

Follow these steps:

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

   You use this profile to configure a connection to the Deployment Manager.
3. Start each node as follows:

   a. Navigate to *was_home*\WebSphere\AppServer\bin on the system where the managed node is located.

   b. Execute the startNode.bat\.sh command.
4. Confirm that a single cell has all the nodes associated with it at this location:
   was_home/profiles/*Deployment_Manager_Profile*/config/cells/*Cell_Name*/Nodes/

   You should see all federated nodes displayed as folder names.

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

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

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

Create the Cluster with One Member

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

Follow these steps:

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

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

How to Install CA IdentityMinder on a WebSphere Cluster

The following procedures describe how to install CA IdentityMinder on a WebSphere cluster.

✓	Step
	1. Run the installation from the deployment manager.
	2. Add cluster members.
	3. Assign the core group policy.
	4. Configure workflow for cluster members.
	5. Configure the proxy plug-in.

Objects Created by the Installation

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

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

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

- Distributed queues/topics targeted to the cluster
- Connection factories targeted to the cluster
- Data sources targeted to cluster

- iam_im-IMSBus, the Service Integration Bus for CA IdentityMinder
- Message engine store for the cluster
- Core group policies used by the message engine

Run the Installation from the Deployment Manager

Once you have created the WebSphere cluster, you can install CA IdentityMinder on it. To install the CA IdentityMinder on all cluster members, you use this procedure and the procedures that follow it.

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

Follow these steps:

1. Perform these steps if you are using Microsoft SQL server:
   a. Open SQL Management Studio.
   b. Locate the user who owns the message store database.
   c. Set that user's default schema to dbo.
2. Log into the system with the Deployment Manager.
   - On Windows, log in as the Windows Administrator.
   - On UNIX, log in as root.
3. Stop the first cluster member, the only cluster member that you have configured so far.
4. Start the Node Agent for that cluster member.
5. Stop the WebSphere Deployment Manager.
6. On the system that hosts the Deployment Manager, run the CA IdentityMinder installation.
   - Windows: From your installation media, run the following program:
     `ca-im-`*`release`*`-win32.exe`
   - UNIX: From your installation media, run the installation program. For example, for Solaris:
     `ca-im-`*`release`*`-sol.bin`

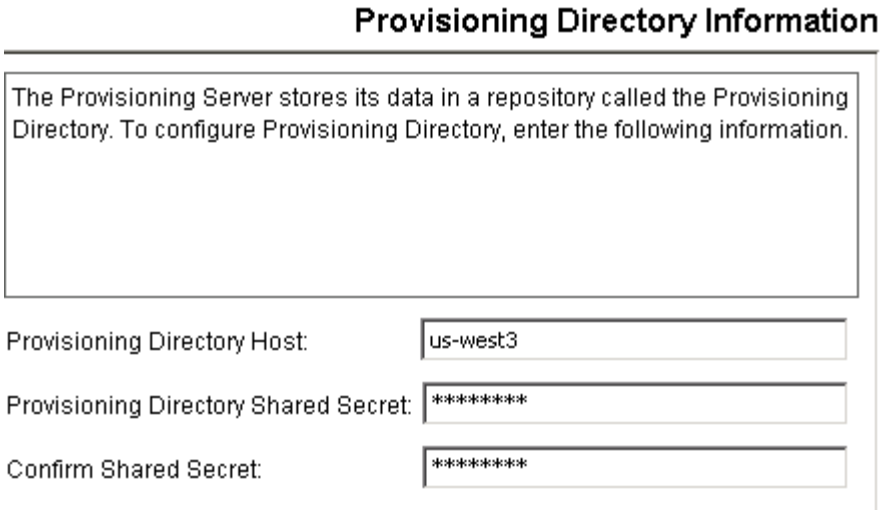
   release represents the current release of CA IdentityMinder.

   Important! Be sure that you have the collected the information needed by the installer, such as user names, host names, and ports.

7. Complete the Select Components section by including the CA IdentityMinder Server and any other components that you need on this system.

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

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



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

   The WebSphere section includes these fields:

   WebSphere Install Folder

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

Server Name

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

Profile Name

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

was_home/profiles/*Deployment_Manager_Profile*

Cell Name

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

Note: Cell names are case sensitive in all operating systems. Be sure to use the correct case.

Node Name

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

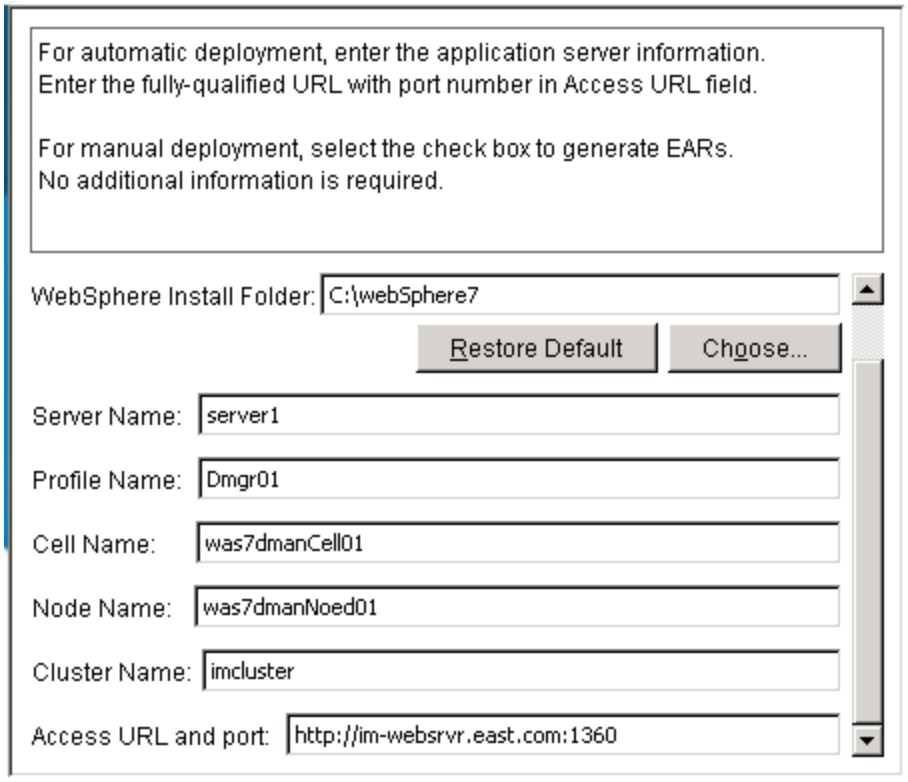
Note: Node names are case sensitive in all operating systems. Be sure to use the correct case.

Cluster Name

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

Access URL and port

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



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

      Enter the message store database.
    - Username

      Enter the user who owns the message store database.

- Password
- Schema name

  For Microsoft SQL Server, enter dbo.

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

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

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

Add Cluster Members

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

Follow these steps:

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

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

Assign the Core Group Policy

To enable high availability and workload management in the cluster, a core group policy now exists for the message engine. This policy, IMSPolicy, defines the preferred cluster member to use for the message engine. If that cluster member fails, the message engine switches to another cluster member, but returns to the preferred cluster member when it becomes available again.

Perform the following procedure once for each cluster member to add cluster members to this policy. For more information about this topic, see Setting up Preferred Servers in the Default Messaging Provider section of the WebSphere System Management and Administration Redbook.

Follow these steps:

1. In the WebSphere Console, locate the IMSpolicy.

   It is under Core Group, Default Core Group, Policies.

2. Select Preferred Servers.

   A list of Core Group Servers appears.

3. Add each cluster member under Preferred Servers.

   Do not select node agents or the Deployment Manager.

   The first cluster member in the list is the one that the messaging engine uses by default. Move the cluster member up or down in the list until they appear in the order in which they should be used.

4. Click OK to save the changes.

Configure Workflow for Cluster Members

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

Follow these steps:

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

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

Configure the Proxy Plug-In for the Web Server

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

Follow these steps:

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

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

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

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

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

Set the Virtual Host Alias

To enable access to any node beyond the first node in the cluster, use the value for WC_defaulthost port as a virtual host alias.

Follow these steps:

1. Go to the General Properties page.
2. Locate the Communications section.
3. Make a note of the value for WC_defaulthost port.
4. Go to the Hosts Alias page.

   This page is under Environment, Virtual host, default host.
5. Verify the port on the second node.

   The value must match the value for WC_defaulthost on the General Properties page.
6. If the values differ, change the Host Alias to match the General Properties value.
7. Repeat this procedure for each node beyond the first two nodes.

Start the WebSphere Cluster

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

Follow these steps:

1. Start a Policy Server that supports CA IdentityMinder.

   Note: If you have a Policy Server cluster, only one Policy Server should be running while you create CA IdentityMinder directories, create or modify CA IdentityMinder environments, or change WorkPoint settings.
2. Run the Deployment Manager.
3. On the first managed node, complete the following steps:
   a. Navigate to *was_home*\WebSphere\AppServer\profiles\Custom01\bin.
   b. Execute the startNode.bat\.sh command.

      The first managed node starts.
4. Repeat step 3 on each node in the cluster.
5. Start each cluster member in Servers, Clusters, *cluster_name*, Cluster Members in the WebSphere Administrative Console on the Deployment Manager.

6. Verify that the messaging engine for the cluster is running in Service integration, Buses, iam_im-IMSBus, Messaging Engines in the WebSphere Admin Console on the Deployment Manager.
7. If you have installed a SiteMinder Web Agent, start the Web Server where you installed the SiteMinder Web Agent and the application server proxy plug-in.

Verify the Clustered Installation

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

Follow these steps:

1. Start the databases used by the CA IdentityMinder server.
2. Start any extra Policy Servers and CA IdentityMinder nodes that you stopped.
3. Access the Management Console and confirm the following points:
   - You can access the following URL from a browser:

     http://*IdentityMinder_server_node:port*/iam/immanage

     For example:

     http://MyServer.MyCompany.com:*port-number/*iam/immanage
   - The Management Console opens.
   - No errors are displayed in the application server log.
   - You do not receive an error message when you click the Directories link.
4. Verify that you can access an upgraded environment using this URL format:

   http://*web_server_proxy_host*/iam/im/*environment*

Configure a Remote Provisioning Manager

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

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

Follow these steps:

1. Log in to the Windows system where you installed Provisioning Manager.
2. Go to Start, Programs, CA, IdentityMinder, Provisioning Manager Setup.
3. Enter the hostname of the Provisioning Server.

4. Click Configure.
5. For an alternate Provisioning Server, select the domain name from the pull-down list.
6. Click Ok.

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

Chapter 5: Separate Database Configuration

This section contains the following topics:

Installation Status

This table shows you where you are in the installation process:

You Are Here	Step in Installation Process
	1. Install prerequisite hardware and software and configure your system as required.
	2. Perform one of these installations: ■ Single node installation ■ Installation on an application server cluster
X	**3. (Optional) Create separate databases.**
	4. (Optional) Install the Report Server.
	5. (Optional) Install alternate Provisioning Directories, alternate Provisioning Servers, and connector servers to support failover and load balancing.

Create Separate Databases

CA IdentityMinder requires a relational database to store objects and data for auditing, snapshots (reporting), workflow, and task persistence. When installing CA IdentityMinder, all of the database schemas are created automatically when the application server is started. However, for scalability purposes, you may want to create a separate database to replace any one of the existing database schemas initially created by CA IdentityMinder during installation.

You can create a database instance for the following:

- Workflow
- Auditing
- Task Persistence
- Object Store
- Snapshots (reporting)
- Archive (task persistence archive)

Important! The Windows default locations for CA IdentityMinder database schema files are the following:

- Workflow: See the section, Run the CreateDatabase script.
- Auditing: C:\Program Files\CA\Identity Manager\IAM Suite\Identity Manager\tools\db
- Task Persistence: C:\Program Files\CA\Identity Manager\IAM Suite\Identity Manager\tools\db
- Object Store: C:\Program Files\CA\Identity Manager\IAM Suite\Identity Manager\tools\db
- Snapshots (reporting): C:\Program Files\CA\Identity Manager\IAM Suite\Identity Manager\imrexport\tools\db
- Archive (task persistence archive): C:\Program Files\CA\Identity Manager\IAM Suite\Identity Manager\tools\db

How to Create Separate Databases

To create separate databases for CA IdentityMinder:

✓	Step
	1. Create a Microsoft SQL Server or Oracle database instance for CA IdentityMinder.
	2. Create JDBC resources.
	3. Edit the data source.
	4. Set connection pool properties.
	5. (Optional) Run the SQL scripts.

Create an MS SQL Server Database Instance

Follow these steps:

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 the following default location:

   C:\Program Files\CA\Identity Manager\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 on the Security tab of the SQL Server Properties dialog for the server where the database is installed.

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

Create an Oracle Database Instance

Follow these steps:

1. Create a new tablespace.
2. Create a new user.
3. Grant the user rights to the new database.
   - Create/alter/drop tables
   - Create/alter/drop view
   - Create/alter/drop INDEX
   - Create/replace/drop stored procedures
   - Create/replace/drop functions
   - Create/drop sequence
   - Create/replace/drop triggers
   - Create/replace/drop types
   - Insert/select/delete records
   - CREATE SESSION / connect to database
4. Give DBA rights to the user.

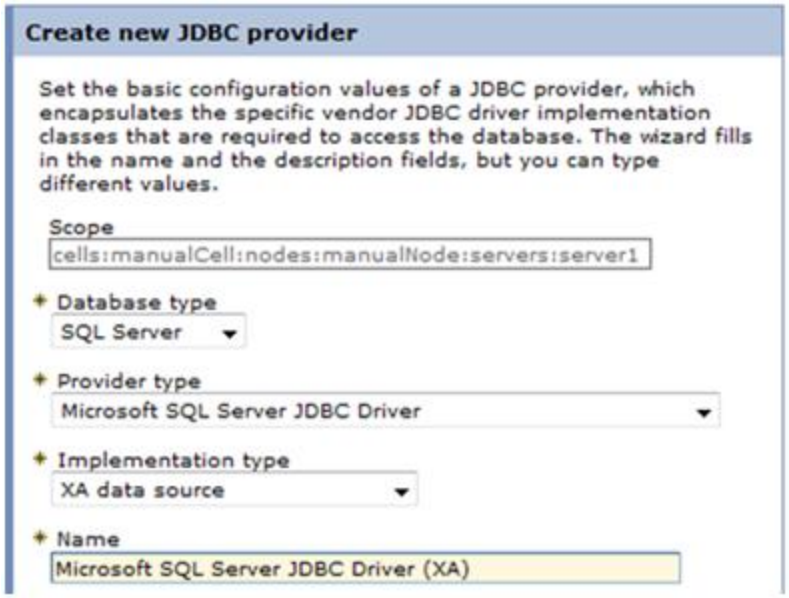
Note: For complete information about Oracle, see your Oracle documentation.

Create JDBC Resources

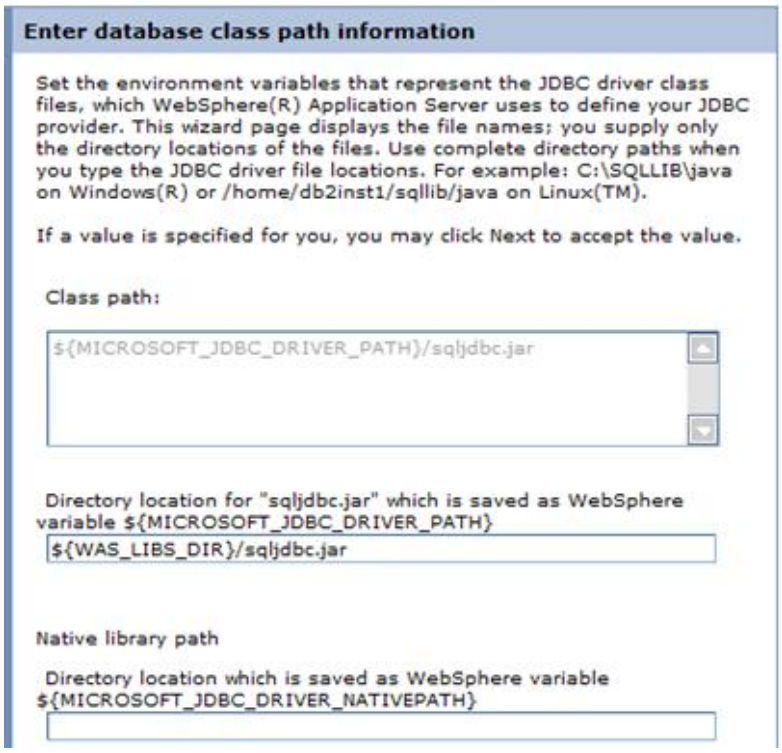
Follow these steps:

1. In the WebSphere Administrative Console, click Resources, JDBC, JDBC Providers.
2. For Scope, select Node=manualNode, Server=*server-name*.
3. Click New.

4. Complete the Create New JDBC provider page with your choices for your database. The following example shows Microsoft SQL Server as the JDBC provider.



5. Fill in the database class page information. The directory location for Microsoft SQL Server appears in the following example.

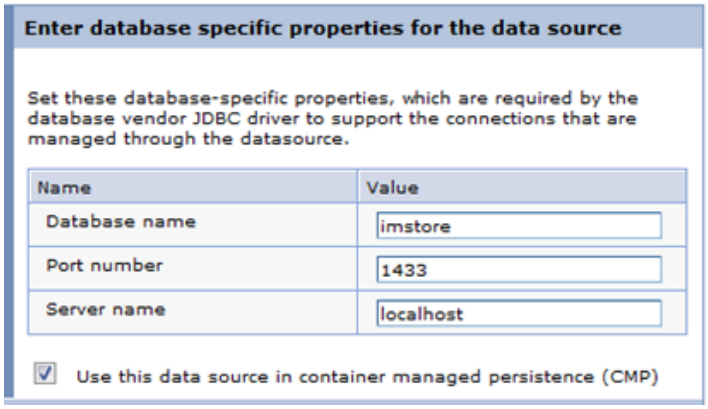


6. Validate the Summary page and click Finish.

Edit the Data Source

Follow these steps:

1. Within the WebSphere Administrative Console, click Resources, JDBC, Data sources.
2. For Scope, select Node=manualNode, Server=*server- name*.
3. Click New to create the data source as follows:
   - For Data source name, enter iam_im Object Store Data Source
   - For JNDI name, enter iam/im/jdbc/jdbc/objectstore
4. Select the JDBC provider.
5. Enter the database specific properties for your environment.

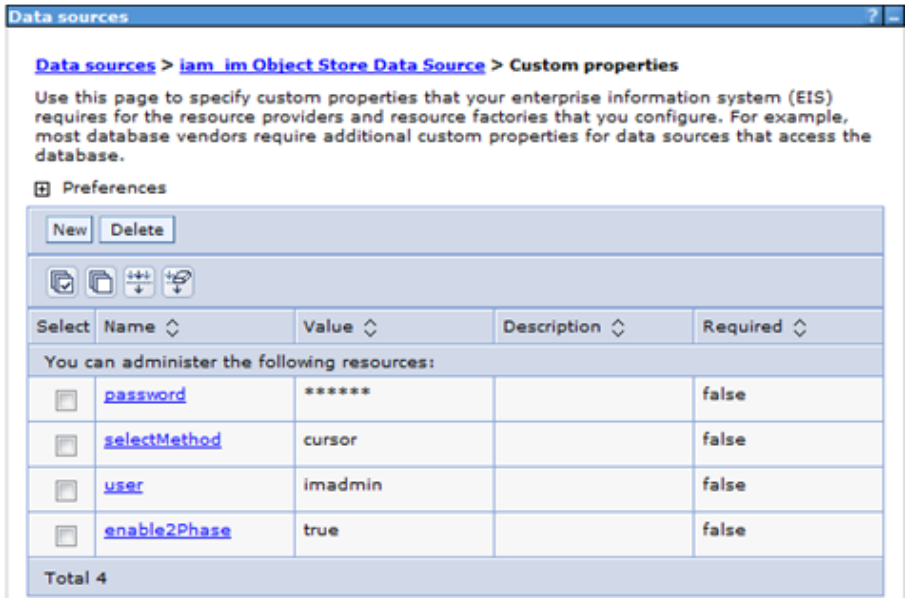


6. For Setup security aliases, accept the defaults.
7. On the Summary page, click Finish.
8. Save changes directly to the master configuration.
9. Add custom properties to the Data Source using the following steps:
   a. From the Data sources page, select iam_im Object Store Data Source.
   b. Under Additional Properties, select Custom properties.

c. Depending on your database**,** add the following properties

- **SQL:** user=<username>, password=<password>, enable2Phase=true, selectMethod=cursor
- **Oracle**: user=<username>, password=<password>

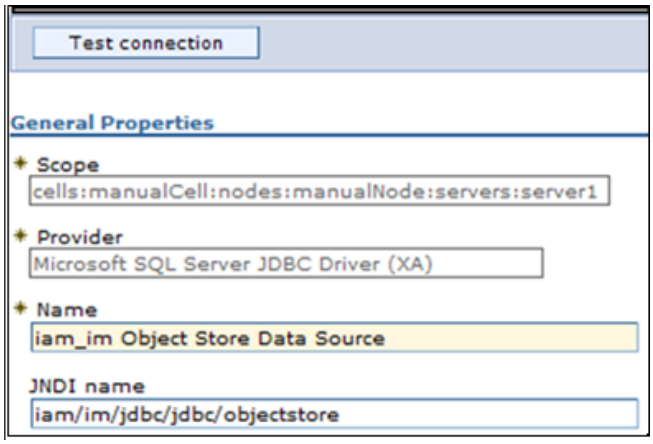
Note: Be sure that the JDBC provider is created as XA.



10. Save changes directly to the master configuration

    The database schema (SQL scripts) are automatically applied when you restart CA IdentityMinder.

11. Test the data source connection.



Failures are typically classpath or credentials related. If the test connection passed, then the Data Source configuration is complete.

12. Four additional data sources need to be configured. Repeat this procedure, but use the data sources and JNDI names in the following table:

Data Source	JNDI Name
iam_im Task Persistence Data Source	iam/im/jdbc/jdbc/idm
iam_im Workflow Data Source	iam/im/jdbc/jdbc/WPDS
iam_im Snapshots Data Source	iam/im/jdbc/jdbc/reportsnapshot
iam_im Archive Data Source	iam/im/jdbc/jdbc/archive

Set Connection Pool Properties

The default connection pool values need to be edited for all data sources to ensure proper performance. Set the connection pool properties as follows:

- Connection timeout: 10
- Maximum connections: 200
- Minimum connections: 5
- Reap time: 150
- Unused timeout: 300
- Aged timeout: 300
- Purge policy: FailingConnectionOnly

Run the SQL Scripts

SQL scripts are automatically run against the databases when CA IdentityMinder 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 CA IdentityMinder Administrative Tools.

Follow these steps:

1. Do one of the following:
   - Microsoft 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 (shown with the default Windows locations) depending on what the database was created for:
   - Task Persistence:
     - Microsoft SQL Server: C:\Program Files\CA\Identity Manager\IAM Suite\Identity Manager\tools\db\taskpersistence\sqlserver\idm_db_sqlserver.sql
     - Oracle on Windows: C:\Program Files\CA\Identity Manager\IAM Suite\Identity Manager\tools\db\taskpersistence\oracle9i\idm_db_oracle.sql
     - Oracle on UNIX: /opt/CA/IdentityManager/IAM_Suite/Identity_Manager/tools/db/taskpersistence/oracle9i/idm_db_oracle.sql
   - Auditing:
     - Microsoft SQL Server: C:\Program Files\CA\Identity Manager\IAM Suite\Identity Manager\tools\db\auditing\sqlserver\ims_mssql_audit.sql
     - Oracle on Windows: C:\Program Files\CA\Identity Manager\IAM Suite\Identity Manager\tools\db\auditing\oracle\ims_oracle_audit.sql
     - Oracle on UNIX: /opt/CA/IdentityManager/IAM_Suite/Identity_Manager/tools/db/auditing/oracle/ims_oracle_audit.sql
   - Snapshots:
     - Microsoft SQL Server: C:\Program Files\CA\Identity Manager\IAM Suite\Identity Manager\tools\imrexport\db\sqlserver\ims_mssql_report.sql
     - Oracle on Windows: C:\Program Files\CA\Identity Manager\IAM Suite\Identity Manager\tools\imrexport\db\oracle\ims_oracle_report.sql
     - Oracle on UNIX: /opt/CA/IdentityManager/IAM_Suite/Identity_Manager/imrexport/db/oracle/ims_oracle_report.sql
   - Workflow: See the Section "Run the SQL Scripts for Workflow."
3. Run the script file.
4. Verify that no errors appeared when you ran the script.

Run the Script for Workflow

CA IdentityMinder includes SQL scripts for setting up a new workflow database instance.

To run the CreateDatabase script:

Follow these steps:

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 CreateDatabase.bat or sh. The default location for this script is:

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

   UNIX: /opt/CA/IdentityManager/IAM_Suite/Identity_Manager/tools/Workpoint/install.

   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.sqlserver.jdbc.SQLServerDriver
   - For the JDBC URL, enter:

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

     SQL Server: jdbc:sqlserver://*wf_db_system*: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.

Chapter 6: Manual EAR Deployment

This section contains the following topics:

How to Deploy Manually

To manually deploy CA IdentityMinder 12.6.4 on WebSphere, you perform the following steps, which are explained in this chapter.

✓	Step
	1. Review the prerequisites.
	2. Create the primary resources.
	3. Assign the core group policy if you have a cluster.
	4. Generate the EAR files.
	5. Deploy the ca-styles5.1.1.ear.
	6. Deploy the iam_im.ear.
	7. Create Policy Server and workflow objects. (Required for all installations.)
	8. Create Message Driven Bean listener bindings.
	9. Edit the user_console.war.
	10. Connect to SiteMinder, if it is installed.

✓	Step
	11. Connect to RCM, if it is installed.
	12. Create a Provisioning Server shared secret.
	13. Perform post-deployment steps for the cluster.

Prerequisites to Manual Deployment

Review the following prerequisites before manually deploying CA IdentityMinder 12.6.4.

- Use the Create databases (see page 65) procedure to create the required JDBC resources, edit data sources, and set connection pool properties.
- Verify that you have met the WebSphere prerequisites (see page 28).
- Create a WebSphere cluster if you need high availability for the CA IdentityMinder server.

Create the Primary Resources

To create the JMS resources and the service integration bus, run a JACL script located in the WebSphere-tools folder. Based on your situation, use the single node or cluster procedure that follows.

To create the primary resources for a single node:

Follow these steps:

1. Open a command line and move to the following location:
   `websphere_home/profiles/profile_name/bin`
2. Run the imssetup.jacl as follows:
   `wsadmin -f websphere_tools/imssetup.jacl myNodeName myServerName`
3. To validate the resources were created, review the resource settings from the Webphere Administrative Console. Specifically:
   a. Check under Service Integration, Buses.

b. Check under Resources, JMS for the following items:

- Queue connection factories
- Topic connection factories
- Queues
- Topics
- Activation specifications

Each CA IdentityMinder resource begins with an iam prefix.

To create the primary resources for a cluster:

Follow these steps:

1. Copy the CreateCoreGroupPolicy.jacl from WAS_ROOT/bin to the Deployment Manager profile/bin folder.
2. Edit the IMSCoreGroupPolicy.properties for the following variables:
   - $WAS_CLUSTER$ - The cluster name. The entire string that contains this variable corresponds to the messaging engine name.
   - WAS_NODE - The node where the cluster member is created; it can be different from Deployment Manager Node name.
   - WAS_SERVER - The name of the cluster member.
3. Open a command line and move to the following location:
   `websphere_home/profiles/profile_name/bin`
4. Run the imsSetupCluster.jacl for each node of the cluster as follows:

   wsadmin -f *websphere_tools*/imsSetupCluster.jacl *NodeName ClusterMemberName ClusterName SchemaName*

   Note: SchemaName parameter is a string passed to imsSetupCluster.jacl to specify the schema name for the messaging engine associated with each cluster member. This string can be changed later.
5. To validate the resources were created, review the resource settings from the Webphere Administrative Console. Specifically:

   a. Check under Service Integration, Buses.

   b. Check under Resources, JMS for the following items:

   - Queue connection factories
   - Topic connection factories
   - Queues
   - Topics
   - Activation specifications

   Each CA IdentityMinder resource begins with an iam prefix.

Assign the Core Group Policy

To enable high availability and workload management in the cluster, a core group policy now exists for the message engine. This policy, IMSPolicy, defines the preferred cluster member to use for the message engine. If that cluster member fails, the message engine switches to another cluster member, but returns to the preferred cluster member when it becomes available again.

Perform the following procedure once for each cluster member to add cluster members to this policy. For more information about this topic, see Setting up Preferred Servers in the Default Messaging Provider section of the WebSphere System Management and Administration Redbook.

Follow these steps:

1. In the WebSphere Console, locate the IMSpolicy.

   It is under Core Group, Default Core Group, Policies.

2. Select Preferred Servers.

   A list of Core Group Servers appears.

3. Add each cluster member under Preferred Servers.

   Do not select node agents or the Deployment Manager.

   The first cluster member in the list is the one that the messaging engine uses by default. Move the cluster member up or down in the list until they appear in the order in which they should be used.

4. Click OK to save the changes.

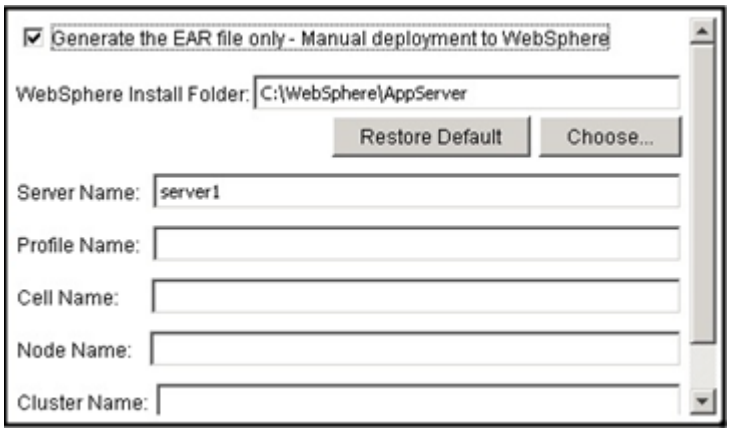
Generate the EAR Files

Follow these steps:

Run the CA IdentityMinder installer and select the Generate EAR file only option. The installer creates the following EAR files:

- WAS_IMR12.ear: This is the compressed iam_im.ear (the EAR file of the CA IdentityMinder application).
- WAS_caStyles.ear: This is the compressed castyles5.1.1.ear (the EAR file for the CA IdentityMinder style sheets).

These files are installed in the location that you specify during installation.



The installation also creates the following folders:

- *install_location*\IAM Suite\WebSphere-ear - Contains EAR files and exploded backup files
- *install_location*\IAM Suite\WebSphere-tools - Contains JACL scripts and other tools

Deploy the castylesr5.1.1.ear File

After generating the EAR files, you start by deploying the ca-styles5.1.1.ear.

Follow these steps:

1. In the WebSphere Administrative Console, click Applications, New Application, New Enterprise Application.
2. Supply the location of the ca-stylesr5.1.ear file.

3. Keep all default settings.
4. Under Select installation options, select the following options:
   - Distribute application
   - Create MBeans for resources
5. On the Map modules to servers page:
   - Verify that the cell and server name are listed.
   - Select the Module CA Styles r5.1.1.
6. On the Map virtual hosts for Web modules page, select Web module CA Styles R5.1.1.
7. Select default_host under Virtual host column.
8. Click Next, then Finish.

   The application is installed.
9. Save directly to the master configuration.
10. Click Applications, Application Types, WebSphere enterprise applications.
11. Select castyles5.1.1 and click Start.
12. Verify that the status field changed to Started.

Deploy the iam_im.ear

Two options exist for deploying the iam_im.ear to WebSphere. You can use a JACL script or you can use the WebSphere Administrative Console.

Deploy the iam_im.ear with a JACL Script

The simplest method to deploy the iam_im.ear is to use a JACL script.

Follow these steps:

To deploy the iam_im.ear with JACLs, perform the following steps.

1. Copy the compressed iam_im.ear file to the following directory.

   websphere_home/profiles/*profile_name*/bin
2. Open a command line and move to the preceding directory.
3. Run one of the following commands:

   Single Node: wsadmin -f *WebSphere-tools*/imsinstall.jacl *path_to_EAR*

   Cluster: wsadmin -f *WebSphere-tools*/imsinstall.jacl *path_to_EAR ClusterName*

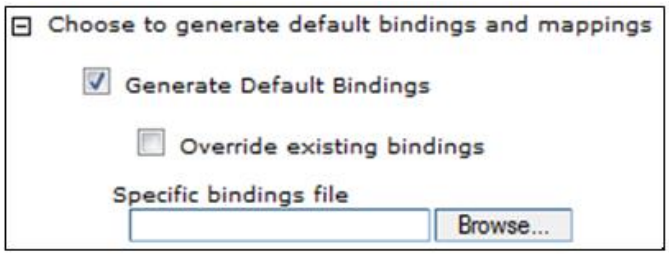
Important! If this procedure succeeds, continue to Edit the user_console.war (see page 84). If this procedure fails, use the procedure, Deploy the iam_im.ear from the WebSphere Administrative Console (see page 79).

Deploy the iam_im.ear from the WebSphere Administrative Console

If deploying the iam_im.ear using a JACL script did not work, use this procedure instead.

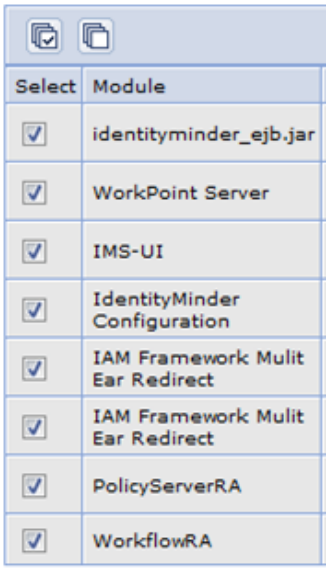
Follow these steps:

1. Log into the WebSphere Administrative Console.
2. Click Applications, New Applications, New Enterprise Application.
3. Click Install.
4. Supply the location of the EAR file that you generated.
5. Fill in the dialog as follows:
   a. Select Fast Path.
   b. Expand the Choose to generate default bindings and mappings.
   c. Select Generate Default Bindings.



6. On the Installation Options page, no changes are needed.

7. On the Map modules to servers page:
   a. Fill in the Clusters or Servers field as appropriate.
   b. Select all modules.



8. On the Map virtual hosts to Web modules page, select all modules.
9. Verify the Summary page appears similar to the following example:

Options	Values
Precompile JavaServer Pages files	No
Directory to install application	
Distribute application	Yes
Use Binary Configuration	No
Deploy enterprise beans	Yes
Application name	iam_im
Create MBeans for resources	Yes
Override class reloading settings for Web and EJB modules	No
Reload interval in seconds	
Deploy Web services	No
Validate Input off/warn/fail	warn
Process embedded configuration	No
File Permission	.*\.dll=755#.*\.so=755#.*\.a=755#.*\.sl=755
Application Build ID	Unknown
Allow dispatching includes to remote resources	No
Allow servicing includes from remote resources	No
Business level application name	
Asynchronous Request Dispatch Type	Disabled
Allow EJB reference targets to resolve automatically	No
Cell/Node/Server	Click here

10. Click Finish to deploy the ear.

    Note: This step takes some time to complete.

11. Save the installation directly to the master configuration.

Create Policy Server and Workflow Objects

If you succeeded in deploying the iam_im.ear by using the JACL script, you can omit this procedure.

Follow these steps:

1. In the WebSphere Administrative Console, click Servers, Server Types, WebSphere application servers.
2. On the Application servers page, click the *server-name*.
3. Under Applications, click Installed applications.
4. Click iam_im on the page that appears.
5. Under Modules, click Manage Modules.
6. Click PolicyServerRA in the list of modules.

7. Under Additional Properties, click Resource Adapter.
8. Under Additional Properties, click J2C connection factories.
9. Click New to create the object with the following values:

   Name: iam_im-PolicyServerConnection

   JNDI Name: iam/im/rar/nete/rar/PolicyServerConnection

10. In the messages box at the top of the screen, save directly to master configuration.
11. Follow these steps to create the Workflow connector object:
    a. Return to the Manage Modules page.

       To go to that page, repeat steps 1 through 5 or click Manage Modules in the breadcrumbs.

    b. Click WorkflowRA.

    c. Under Additional Properties, click Resource Adapter.

    d. Under Additional Properties, click J2C connection factories.

    e. Create the Workflow connector object with these values:

       Name: iam_im-Workflow

       JNDI Name: iam/im/rar/Workflow

Create Message Driven Bean Listener Bindings

If you succeeded in deploying the iam_im.ear by using the JACL script, you can omit this procedure.

Follow these steps:

1. In the WebSphere Administrative Console, go to Applications, Application Types, WebSphere Enterprise Applications.
2. Click iam_im.
3. Under Enterprise Java Bean Properties, select Message Drive Bean listener bindings.
4. Under Listener bindings, click Activation Specification.
5. For the identityminder_ejb.jar, fill in these values for each EJB module:

EJB	Listener Bindings
SubscriberMessageEJB	Target Resource JNDI Name: iam/im/ACT Destination JNDI name: iam/im/jms/queue/com.netegrity.ims.msg.queue
ServerCommandsEJB	Target Resource JNDI Name: iam/im/ServerCommand Destination JNDI name: iam/im/jms/topic/topic/ServerCommandTopic

EJB	Listener Bindings
RuntimeStatusDetailEJB	Target Resource JNDI Name: iam/im/jms/RuntimeStatusDetailQueue Destination JNDI name iam/im/jms/queue/queue/RuntimeStatusDetailQueue

6. For the WorkPoint Server, fill in these values for each EJB module:

EJB	Listener Bindings
ServerAutomatedActivityMDBean	Target Resource JNDI Name: iam/im/jms/wpServAutoActActSpec Destination JNDI name: iam/im/jms/queue/queue/wpServAutoActQueue
EventMDBean	Target Resource JNDI Name: iam/im/jms/wpEventActSpec Destination JNDI name: iam/im/jms/queue/queue/wpEventQueue
UtilityMDBean	Target Resource JNDI Name: iam/im/jms/wpUtilActSpec Destination JNDI name: iam/im/jms/queue/queue/wpUtilQueue

7. Click OK.
8. Save your changes directly to the master configuration.
9. Restart WebSphere.

Edit the user_console.war

Use this procedure to change the starting weight and reset the class loader order in the user_console.war file.

Follow these steps:

1. Click Application, WebSphere enterprise applications, iam_im.
2. Under Modules, click Manage modules.

3. Click IMS-UI.
4. Set the starting weight to 4000.
5. Set the class loader order to the following choice:

   Classes loaded with local class loader first (parent last)
6. Click Okay.
7. Save directly to the master configuration.

Edit the wpServer.Jar

Use this procedure to change the starting weight for the Workpoint Server JAR file.

Follow these steps:

1. Click Application, WebSphere enterprise applications, iam_im.
2. Under Modules, click Manage modules.
3. Click Workpoint Server.
4. Set the starting weight to 500.
5. Save directly to the master configuration.
6. Restart the WebSphere application server.

Connect to SiteMinder

To connect to a SiteMinder Policy Server, perform the following steps. For a cluster, perform these steps on each cluster member.

Follow these steps:

1. On the WebSphere application server system, navigate to *was_home*/bin/.
2. Edit the startServer.sh file. Add the following path to the SMPS variable under the Start CA IAM Suite section:

   was_home/profiles/*profile_name*/installedApps/*profile_name*/iam_im.ear/library
3. Start the WebSphere application server.
4. In the WebSphere Administrative Console, go to Application servers, *your_server*, Install Applications, IdentityMinder, Manage Modules, policyserver.rar, IdentityMingerPolicyServerRA, J2C connection factories.

5. Click on the object with the following JNDI name:

   nete/rar/PolicyServerConnection

6. Click on Custom Properties.

7. Set the following properties:

   - ValidateSMHeadersWithPS = true
   - Enabled = true
   - ConnectionUrl = hostname of the SiteMinder system
   - Username = SiteMinder administrative user
   - AdminSecret = SiteMinder administrative user password
   - AgentName = SiteMinder Agent name
   - AgentSecret = SiteMinder Agent secret

8. In the SiteMinder Administrative UI, create an Agent configuration object for the Agent protecting your WebSphere resources.

   Note: For more details on creating an Agent configuration, see the *SiteMinder Policy Server Configuration Guide*.

9. Navigate to the following location:

   was_home\config\cells*cellname*\applications\iam_im.ear\deployments\IdentityMinder\user_console.war\WEB-INF

10. Edit the web.xml file and set enabled=false for the AgentFilter and the FrameworkAuthFilter. For example:

```
   <filter-name>AgentFilter</filter-name>
     <filter-class>com.netegrity.proxy.AgentFilter</filter-class>
        <init-param>
            <param-name>EnableAgent</param-name>
            <param-value>false</param-value>
        </init-param>
 <filter-name>FrameworkAuthFilter</filter-name>

    <filter-class>com.netegrity.webapp.authentication.FrameworkLoginFilter</f
ilter-class>
        <init-param>
            <param-name>Enable</param-name>
            <param-value>false</param-value>
        </init-param>
```

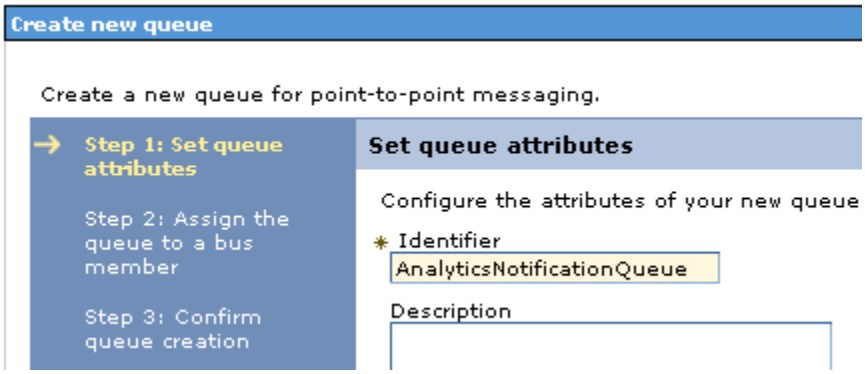
11. Run the CA IdentityMinder installer on the SiteMinder system and install the Extensions for SiteMinder.

Connect to RCM

If you have Role and Compliance Manager (RCM) in your installation, configure WebSphere to connect to RCM.

Follow these steps:

1. Log in to the WebSphere Administrative Console.
2. Create a queue as a bus destination as follows:
   a. Click Service Integration, Buses.
   b. Click iam_im-IMSBus.
   c. Under Destination Resources, click Destinations.
   d. Click New.
   e. Click Queue.
   f. For Identifier, enter AnalyticsNotificationQueue.



3. Create a JMS queue as follows:
   a. Click Resources, JMS, Queues.
   b. Click New.
   c. Click Default messaging provider.
   d. Supply these values for the following fields:

      Name

      AnalyticsNotificationQueue

      JNDI Name

      iam/im/jms/queue/analytics/AnalyticsNotificationQueue

Bus Name

IMSBus

Queue Name

AnalyticsNotificationQueue

4. Create an activation specification for the queue as follows:
   a. Click Resources, JMS, Activation Specifications.
   b. Click New.
   c. Click Default messaging provider.
   d. Supply these values:

Name

AnalyticsNotificationQueueActSpec.

JNDI Name

iam/im/jms/analytics/AnalyticsNotificationQueue/ActSpec

Destination JNDI name

iam/im/jms/queue/analytics/AnalyticsNotificationQueue

This name must match the JNDI Name created in Step 3.

Create a Provisioning Server Shared Secret

You need to create a shared secret to communicate with the CA IdentityMinder server.

Follow these steps:

1. Generate an encrypted shared secret using the Password Tool.
2. Update the Provisioning Server shared secret in the systemWideProperties.properties file.

Perform Post-Deployment Steps for the Cluster

If you are performing manual EAR deployment to a cluster, perform the following procedures that apply to deployment on a cluster.

Add Cluster Members

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

Follow these steps:

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

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

Assign the Core Group Policy

To enable high availability and workload management in the cluster, a core group policy now exists for the message engine. This policy, IMSPolicy, defines the preferred cluster member to use for the message engine. If that cluster member fails, the message engine switches to another cluster member, but returns to the preferred cluster member when it becomes available again.

Perform the following procedure once for each cluster member to add cluster members to this policy. For more information about this topic, see Setting up Preferred Servers in the Default Messaging Provider section of the WebSphere System Management and Administration Redbook.

Follow these steps:

1. In the WebSphere Console, locate the IMSpolicy.

   It is under Core Group, Default Core Group, Policies.
2. Select Preferred Servers.

   A list of Core Group Servers appears.
3. Add each cluster member under Preferred Servers.

   Do not select node agents or the Deployment Manager.

   The first cluster member in the list is the one that the messaging engine uses by default. Move the cluster member up or down in the list until they appear in the order in which they should be used.
4. Click OK to save the changes.

Configure Workflow for Cluster Members

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

Follow these steps:

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

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

Configure the Proxy Plug-In for the Web Server

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

Follow these steps:

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

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

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

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

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

Start the WebSphere Cluster

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

Follow these steps:

1. Start a Policy Server that supports CA IdentityMinder.

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

2. Run the Deployment Manager.
3. On the first managed node, complete the following steps:
   a. Navigate to *was_home*\WebSphere\AppServer\profiles\Custom01\bin.
   b. Execute the startNode.bat\.sh command.

      The first managed node starts.
4. Repeat step 3 on each node in the cluster.
5. Start each cluster member in Servers, Clusters, *cluster_name*, Cluster Members in the WebSphere Administrative Console on the Deployment Manager.
6. Verify that the messaging engine for the cluster is running in Service integration, Buses, iam_im-IMSBus, Messaging Engines in the WebSphere Admin Console on the Deployment Manager.
7. If you have installed a SiteMinder Web Agent, start the Web Server where you installed the SiteMinder Web Agent and the application server proxy plug-in.

Verify the Clustered Installation

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

Follow these steps:

1. Start the databases used by the CA IdentityMinder server.
2. Start any extra Policy Servers and CA IdentityMinder nodes that you stopped.

3. Access the Management Console and confirm the following points:
   - You can access the following URL from a browser:

     http://*IdentityMinder_server_node:port*/iam/immanage

     For example:

     http://MyServer.MyCompany.com:*port-number/*iam/immanage
   - The Management Console opens.
   - No errors are displayed in the application server log.
   - You do not receive an error message when you click the Directories link.
4. Verify that you can access an upgraded environment using this URL format:

   http://*web_server_proxy_host*/iam/im/*environment*

Chapter 7: Report Server Installation

This section contains the following topics:

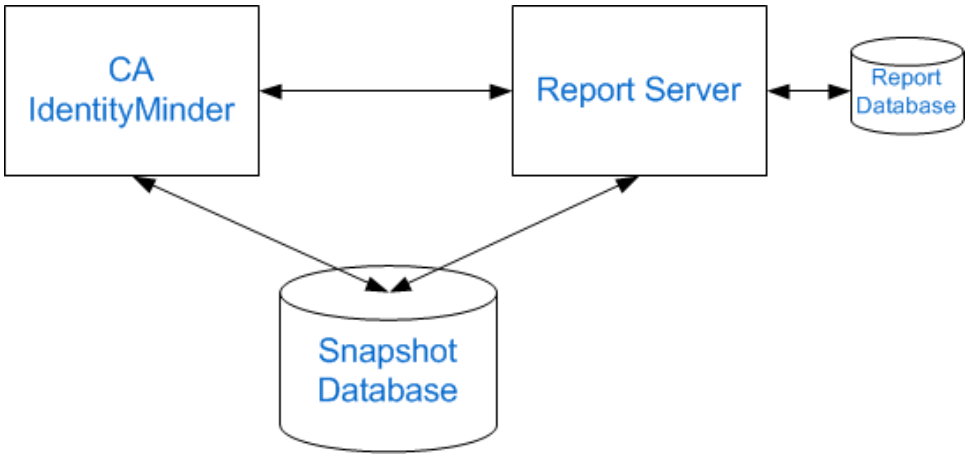
Installation Status

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 and configure your system as required.
	2. Perform one of these installations: ■ Single node installation ■ Installation on an application server cluster
	3. (Optional) Create separate databases.
X	**4. (Optional) Install the Report Server.**
	5. (Optional) Configure the SSL Certificate in the Report Server.
	6. (Optional) Install alternate Provisioning Directories, alternate Provisioning Servers, and connector servers to support failover and load balancing.

Reporting Architecture

In CA IdentityMinder, the reporting setup requires the three major components in the following diagram:



Note: The Snapshot Database in this illustration graphic could also be the Audit Database or Workflow Database.

Report Server

Also known as CA Business Intelligence, this server generates reports, communicating directly with CA IdentityMinder and the Snapshot Database.

Report Database

The database where the CA Report Server (Business Objects) stores its own data.

CA IdentityMinder

CA IdentityMinder allows you to export CA IdentityMinder object data to the Report Database.

Snapshot Database

A separate database containing the snapshot data of objects in CA IdentityMinder

Important! The Report Server uses Business Objects Enterprise. If you already have a Report Server in your environment and want to use it with CA IdentityMinder, the minimum version required by CA IdentityMinder is CA Business Intelligence 3.3 SP1.

Reporting Considerations

Consider the following before installing the Report Server:

- Installing the Report Server can take up to two hours.

- If JBoss is installed on the computer where you are installing the Report Server, port conflicts may occur. If Apache Tomcat is the web server, you can locate JBoss port information in the following files:
  - jboss-service.xml

    Default location: *jboss_home*\server*server_configuration*\conf
  - server.xml

    Default location:
    jboss_home\server*server_configuration*\deploy\jboss-web.deployer

  jboss_home

  Specifies the JBoss installation path.

  server_configuration

  Specifies the name of your server configuration.

  Default value: default

  Note: Restart JBoss if you make changes to either of these files.

Hardware Requirements

The hardware requirements for the Report Server are based on the operating system. See the PDF with the filename that matches your operating system in the *installer-media-root-directory*/Docs folder.

Note: For more information about supported OS versions and databases, see the Business Objects website.

How to Install the Report Server

The following checklist describes the steps to install the reporting feature of CA IdentityMinder:

✓	Step
	1. Review the report pre-installation checklist.
	2. Gather reporting information.
	3. Open ports required by the Report Server.
	4. Install the Report Server (CA Business Intelligence).
	5. Run the Registry Script.

✓	Step
	6. Copy the JDBC JAR files.
	7. Bypass the proxy server.
	8. Deploy the default reports.
	9. Perform a post-installation step.

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

Reports Pre-Installation Checklist

Print the following checklist to be sure that you meet the minimum system and database requirements before installing the Report Server:

- Be sure that the Windows or UNIX system on which you are installing the Report Server meets the minimum system requirements.
- If you create a database instance for the Snapshot Database, run the following scripts on the new database:
  - Microsoft SQL: C:\Program Files\CA\Identity Manager\IAM Suite\Identity Manager\tools\imrexport\db\sqlserver\ims_mssql_report.sql
  - Oracle: C:\Program Files\CA\Identity Manager\IAM Suite\Identity Manager\tools\imrexport\db\oracle\ims_oracle_report.sql

    To execute these scripts, the database user needs DBA, connect, and resource roles and system privileges to create tables, indexes, sessions and views with global query rewrite permission.
- On UNIX, set the following parameters as global in the local .profile files:
  - ORACLE_BASE: the top-level directory where Oracle is installed.
  - ORACLE_HOME: the path to the Oracle root directory under ORACLE_BASE
  - LD_LIBRARY_PATH: $ORACLE_HOME/lib32:$ORACLE_HOME/lib

    If Oracle is a 64-bit installation, use lib32. Use SQL Plus to connect to the oracle database instance to determine if it is a 64-bit installation.
  - ORACLE_SID: the SID name used in the tnsnames.ora file.
  - JAVA_HOME: the path to the Java root directory. Business Objects installs a JDK in the following location:

    `report_server_home/jre`

    Note: JDK 1.5 is the minimum version supported for reports.

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

  Note: Be sure that the CASHCOMP environment variable is empty.

- On UNIX systems:
  - 3 GB of free space is required under /tmp.
  - You need access to a non-root user account to install the Report Server.

    This user should have a home directory in the local file system. For example, the following command creates a user with a local home directory:

    ```
    useradd -u 505 -g 0 -d /export/home/cabi -m cabi
    ```

    Also, add the non-root user to the install group and any group for which the root user is a member.
  - Enter the database server name in the /etc/hosts file if the database server is not on the same system as the Report Server. (If you have DNS, this step is unnecessary.)
  - If you encounter problems, inspect the SDK.log under these locations:

    /opt/CA/SharedComponents/CommonReporting3/ca-install.log

    /opt/CA/SharedComponents/CommonReporting3/CA_Business_Intelligence_InstallLog.log

Reporting Information

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

Field Name	Description	Your Response
Administrator Password	Defines the password to log in to the Business Objects Infoview console.	
User Name	Identify the username for the Report Database.	
Password	Identify the administrative password credentials for the Report Database.	

Field Name	Description	Your Response
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, Report Server installer can install Tomcat.	
Tomcat Port Numbers	The Tomcat connection, redirect, and shutdown ports. **Note:** If you install the Report Server on the same system as the CA IdentityMinder, be sure that the Tomcat connection port does not conflict with the port number you specified for the application server URL when installing the CA IdentityMinder.	

Open Ports for the Report Server

For CA IdentityMinder and the Report Server to communicate successfully, the following ports must be opened.

- The Central Management Server (CMS) port: 6400
- The Report Server web application port:
  - JBoss/Tomcat: 8080
  - WebLogic: 7001
  - WebSphere: 9080

  Note the following:
  - This port is not the application server port for the CA IdentityMinder Server.
  - The web server ports are provided during the Report Server installation. If you use different ports during the installation, those ports must be opened through the firewall when the Report Server is deployed in production.
  - The Report Server does not connect to the application server used by CA IdentityMinder.
- All database ports that CA IdentityMinder has configured for the reporting and auditing databases. The CA IdentityMinder Server must send database information to the Report Server, so these ports must be opened. For example, if the Snapshot Database is an Oracle database, the Report Server needs the Oracle port open outbound.

Install the CA 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.

Important! For a production environment, install the Report Server on a separate system from the system with the CA IdentityMinder Server. If you want to install the Report Server on the same system as the CA IdentityMinder Server for demonstration purposes, do not choose the default tomcat ports 8080 and 1099 if JBoss is using those ports.

Note: CA IdentityMinder supports CA Business Intelligence 3.3 SP1 (which is Business Objects XI 3.0 SP6).

Run the Windows Installer

Install the Report Server using the Windows installation wizard (Disk1\InstData\VM\Install.exe) found on the Report Server media.

Note: The Report Server is available for download on the CA Support site, under CA IdentityMinder product downloads.

Follow these steps:

1. Exit all applications.
2. Download the Report Server and unzip it.
3. Navigate to Disk1\InstData\VM and double-click the installation executable.

   The installation wizard starts.
4. Use the gathered reporting information to install the Report Server.

   Note the following:

   - Select a New install during installation. Select SQL Anywhere, Oracle or SQL Server as the Report Database. If you must set non-default ports to avoid port conflicts, select a Custom install, but select SQL Anywhere, Oracle or SQL Server for the Report Database.
   - Select Tomcat as the web server, deselecting IIS.
   - If you are installing the Report Server on the same system as CA IdentityMinder, select the Tomcat connection port carefully. Verify that it does not conflict with the port number you specified for the application server URL when installing CA IdentityMinder. However, we recommend installing the Report Server on a different system than the CA IdentityMinder Server in a production environment.

5. Review the installation settings and click Install.

   The Report Server is installed.

Run the UNIX Installer

Add execute permissions to the install file by running the following command:
`chmod+x /cabi-solaris-3_3_10/cabiinstall.sh`

Important! The installer may crash if executed across different subnets. To avoid this problem, install the Report Server directly on the host system.

Follow these steps:

1. Log in as the non-root user you created to install the Report Server.
2. Exit all applications.
3. Download the Report Server and untar it.

   Note: The Report Server is available for download on the CA Support site, under CA IdentityMinder product downloads.
4. Open a command window and navigate to where the install program is located.
5. Enter the following command:

   `/cabi-solaris-3_3_10/cabiinstall.sh`
6. Use the gathered reporting information to install the Report Server. Note the following:

   Select a New install during installation. Select SQL Anywhere, Oracle or SQL Server as the Report Database. If you must set non-default ports to avoid port conflicts, select a Custom install, but select SQL Anywhere, Oracle or SQL Server as the Report Database.

   - Select Tomcat as the web server.
   - The installer installs the Report Server to /opt/CA/SharedComponents/CommonReporting3. Specifying another location does not change the installation location. So the /opt/CA directory must have non-root user permissions or the installation fails.
7. Review the installation settings and click Install.

   The Report Server is installed.

Run the Linux Installer

Follow these steps:

1. Install and start up an X-server on your client operation system.

   You can download X-Win32 from this location:

   `http://www.starnet.com/products/xwin32/download.php`

2. Log on to Linux by using the Business Objects installation account and run the following commands:

   ```
   bash$ export DISPLAY=$YOURXWin32ClientMACHINENAME:0.0
   bash$ echo &DISPLAY
   bash$ cd $INSTALLDIR/bobje/setup/
   bash$ source env.sh
   bash$ regedit
   ```

   where $INSTALLDIR is where the report server is installed.

3. Switch to the X-win32 client system.

   A Registry Editor message appears indicating that the configuration succeeded.

4. Create a registry category under the following HKEY_LOCAL_MACHINE location:

   HKEY_LOCAL_MACHINE\Software\Business Objects\Suite 12.0\Crystal Reports\DatabaseOptions

5. Add a key named MergeConnectionProperties under the DatabaseOptions category and set the value to Yes.

6. Add a key named MergeConnectionProperties under the following HKEY_CURRENT_USER location:

   HKEY_CURRENT_USER\Software\Business Objects\Suite 12.0\Crystal Reports\DatabaseOptions

7. Set the value for MergeConnectionProperties to Yes.

8. Refresh or schedule a report in Infoview to confirm the installation succeeded.

Run the Registry Script

For CA IdentityMinder to change data sources for reports in the Report Server, run the mergeConnection script.

Note: On a 64-bit system, omit this procedure. The Report Server is a 32-bit application, so you use the 32-bit side of the registry. On a 64-bit system, open REGEDT32 directly from System32, and create the MergeConnectionProperties key with the Type REG_SZ and value Yes. Create the key in this location:
`@HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Business Objects\Suite 12.0\Crystal Reports`

On Windows, perform the following steps:

1. Copy the mergeConnection script from the system with the CA IdentityMinder Admin toolkit to the Report Server. On the system with the toolkit, the default location for this script is as follows:

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

2. Run the mergeconnections_3.0.reg script and respond to the prompts that appear.
3. Click Start, Program Files, CA, Report Server, Central Configuration Manager.
4. Start all services, including Tomcat and the BO Server service.

On UNIX and Linux, perform the following steps:

1. Check for Windows control characters in the mergeconnections script.

   If you downloaded the software using FTP in binary mode, these characters do not appear in this script. If you used another download method, use the dos2unix command to remove these characters.

2. Copy the mergeconnections_3.0.cf script from the system with the CA IdentityMinder Admin toolkit to the Report Server. On the system with the toolkit, the default location for this script is as follows:

   /opt/CA/IdentityManager/IAM_Suite/Identity_Manager/tools/ReportServerTools

   On the Report Server system, place the script in this location:

   installation-directory/bobje/enterprise120/generic

3. Source in the environment variables for BusinessObjects Enterprise, as follows:

   source *installation-directory*//bobje/setup/env.sh

4. Run the following script, as follows:

   ./configpatch.sh mergeconnections_3.0.cf

   Select 1 as the option when prompted.

   Note: On Linux systems, set the environment variable as follows before you run the script:

   export _POSIX2_VERSION=199209

5. Restart crystal processing servers as follows:

   a. Log in as the non root user you used to install the Report Server.

   b. Issue these commands:

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

Copy the JDBC JAR Files

Follow these steps:

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

   Note: Copy sqljdbc.jar from Tools\lib\jdbcdrivers\1.2 to use the 1.2 driver that is compatible with the Report Server.
3. Open the CRConfig.xml file, found in the following location:
   - Windows: CA\SC\CommonReporting3\common\4.0\java
   - UNIX: /opt/CA/SharedComponents/CommonReporting3/bobje/java
4. Add the location of the JDBC JAR files to the Classpath. For example:
   - Windows: <Classpath>report_server_home\common\4.0\java\lib\sqljdbc.jar; report_server_home\ common\4.0\java\lib\ojdbc14.jar …</Classpath>
   - UNIX: <Classpath>${BOBJEDIR}/java/lib/sqljdbc.jar:${BOBJEDIR}/java/lib/ojdbc14.jar: …</Classpath>
5. Save the file.
6. Restart the Report Server as follows:
   - For Windows, do the following:
     a. Go to Start, Program Files, BusinessObjects XI *version*, BusinessObjects Enterprise, Central Configuration Manager.

        The Central Configuration Manager opens.

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

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

Bypass the Proxy Server

If you are using a proxy server to channel outbound requests on the system where CA IdentityMinder is installed, you need to bypass the proxy server. For details, see: Java Networking and Proxies.

Deploy Default Reports

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

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

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

Follow these steps:

1. Gather the following information about the Report Server:
   - Hostname
   - Administrator name
   - Administrator password
   - Snapshot database type
2. Copy all content from the Reports installer-root-directory/disk1/cabi/biconfig folder to the *im_admin_tools_dir*/ReportServerTools folder.
3. Set the JAVA_HOME variable to the 32-bit version of the JDK1.5 you installed.

4. Run one of the following commands:

   - For a Microsoft SQL Snapshot Database:

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

   - For an Oracle Snapshot Database:

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

   Note: In a UNIX operating environment, be sure that biconfig.sh has execute permissions.

5. View the biconfig.log file found in the location where you ran the command in Step 4.

6. Verify that the default reports installed successfully. Inspect the end of the log file for status; a successful install appears as follows:

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

BusinessObjects XI 3.x Post-Installation Step

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

Follow these steps:

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

   Input.*report_server_hostname*.InputFileRepository

5. Click Save.
6. Under the Server Name column, search for Output File Repository server and double-click the name.
7. In the Server Name text box, enter the following:

   Output.*report_server_hostname*.OutputFileRepository

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

Secure the Report Server Connection on WebSphere

CA IdentityMinder and Report Server communicate over a non-secure connection. You can secure the connection between Report Server and CA IdentityMinder using Secure Sockets Layer (SSL) connection.

An SSL connection ensures that the communication is encrypted when data is accessed from the Report Server. Before you configure the SSL, verify that the BO (Business Objects) Server is HTTPS enabled. To secure the connection with SSL, you can either use a self-signed certificate or use a certificate from the Certified Authority (CA).

To configure the SSL connection using the Retrieve from Port page, retrieve a signer certificate from a remote SSL port. The system connects to the specified remote SSL host and port, and receives the signer certificate during the handshake using an SSL configuration.

Follow these steps:

1. In the WebSphere console, under Security tasks, click the SSL certificate and key management.
2. Under Related items, click Keystores and certificates.

   A list of keystores is displayed.
3. Click NodeDefaultTrustStore link from the list of keystores.

   General Properties page is displayed.
4. Under Additional Properties, click Signer certificates.
5. Click Retrieve from port button.
6. Provide values for the following fields:

   Host

   Specifies the report server host name to which you connect when attempting to retrieve the signer certificate from the SSL port.

   Port

   Specifies the SSL port to which you connect when attempting to retrieve the signer certificate.

   Note: In a network deployment environment, specify the appropriate secure sockets layer (SSL) port number when attempting to retrieve the signer certificate from a remote SSL port.

   - Use the port number that is associated with the port name, WC_adminhost_secure, when you retrieve a signer certificate from the deployment manager.
   - Use the port number that is associated with the port name, CSIV2_SSL_MUTUALAUTH_LISTENER_ADDRESS, when you retrieve a signer certificate from a node.

Verify that all the certificates are available before they are retrieved from the deployment manager or from base servers.

SSL configuration for outbound connection

Specifies the SSL configuration to connect to the previously specified SSL port. The previously specified SSL port configuration is also the SSL configuration that contains the signer after retrieval. The SSL configuration does not need to have a trusted certificate for the SSL port as it is retrieved during validation and presented here.

Alias

Specifies the certificate alias name of the signer certificate referred in the key store that is specified in the SSL configuration.

7. Click Retrieve Signer Information.

   The information about the signer certificate is displayed.

8. Click Apply or Save.

   The certificate is storedin the keystore. The SSL certificate is now configured.

Verify the Reporting Installation

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

- In the Central Management Console, be sure that all services are running.
- Be sure that your Report Database is running.

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

Silent Installation

For more information about silent installation of the Report Server, see the *CA Business Intelligence Installation Guide.* The Report Server documentation is available in one of the following locations when you extract the Report Server installer files:

- **Windows**: *install_root_directory*\Docs\CABI_Impl_ENU.pdf
- **UNIX:** *install_root_directory*/Docs/ENU/CABI_Impl_ENU.pdf

How to Uninstall Reporting

You uninstall the Report Server when it is no longer required on the system. For more information, see the CA Business Intelligence documentation.

After uninstalling the Report Server, Remove Leftover Items (see page 110).

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 system from failing.

Remove Windows Items

Follow these steps:

1. Navigate to *report_server_home*.

   report_server_home specifies the Report Server installation path.
2. Open the BusinessObjects Enterprise 12 folder, and delete the following folders:
   - Data
   - java
   - Logging
   - Samples
   - Web Content
   - Web Services
   - win32x86
3. Return to the Report Server folder.
4. Open the common folder.
5. Open the 4.0 folder, and delete the following folders:
   - crystalreportviewers115
   - java

You have completed removing leftover items.

Remove UNIX Items

Following are the steps to remove leftover Report Server items on UNIX:

Follow these steps:

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

   /opt/CA/SharedComponents
2. Delete the CommonReporting3 folder.

You have completed removing leftover items.

Chapter 8: Connector Server Installation

This section contains the following topics:

Connector Server Prerequisites

See the following sections for the steps you take to prepare for connector server installation.

System Requirements

You do not need to install CA IAM CS on the same computer as the Provisioning Server or CA IdentityMinder Server.

Some connectors require an agent on the endpoint. For more information, check the Connectors Guide and the Endpoint Guides.

The installation program for CA IAM CS includes its own Java Virtual Machine, so you do not need to install Java separately.

Time Zone Considerations

In a typical environment, times are stored in the Provisioning Server and on various endpoints referred to by CA IAM CS. No need exists for components to run on servers that have the same time zone. However, they should all use the same absolute time.

File Locations

The default Windows and UNIX directories are listed in the following table. Your actual installation directories depend on your operating system and selections during the installation process.

Path Notation	Default Directory	
	Windows	**UNIX**
im-home	C:\Program Files\CA\Identity Manager	/opt/CA/IdentityManager
imps-home	C:\Program Files\CA\Identity Manager\Provisioning Server	/opt/CA/IdentityManager/ProvisioningServer
cs-home	C:\Program Files\CA\Identity Manager\Connector Server	/opt/CA/IdentityManager/ConnectorServer
cs-sdk-home	C:\Program Files\CA\Identity Manager\Connector Server SDK	/opt/CA/IdentityManager/ConnectorServerSDK
conxp-home	C:\Program Files\CA\Identity Manager\Connector Xpress	/opt/CA/IdentityManager/ConnectorXpress

32-bit and 64-bit Applications

CA IAM CS is a 64-bit application. C++ Connector Server (CCS) is a 32-bit application. If it is installed on a 64-bit operating system, CCS runs as a 32-bit application.

Some connectors require third-party clients to be present on the CCS host. For example, Oracle Applications require Oracle Client and DB2 requires DB2 Connect. Some of these third-party applications come in both 32-bit and 64-bit modes. Install the 32-bit client if you want to manage endpoints on CCS.

Linux Requirements

For Red Hat 5.x, no packages are required for the CA IAM CS. For Red Hat 6.x, install these packages in this order:

1. glibc-2.12-1.25.el6.i686.rpm
2. libX11-1.3-2.el6.i686.rpm
3. libxcb-1.5-1.el6.i686.rpm
4. libXtst-1.0.99.2-3.el6.i686.rpm
5. libXau-1.0.5-1.el6.i686.rpm
6. libXi-1.3-3.el6.i686.rpm
7. libXext-1.1-3.el6.i686.rpm
8. nss-softokn-freebl-3.12.9-3.el6.i686.rpm
9. libXmu-1.0.5-1.el6.i686.rpm
10. libXft-2.1.13-4.1.el6.i686.rpm
11. libXpm-3.5.8-2.el6.i686.rpm

For a non-FIPS mode installation, Linux also requires the following command, which generates entropy:

```
/sbin/rngd -r /dev/urandom -o /dev/random -t 1
```

If the CA IAM CS installation does not succeed, repeat this command.

Install CA IAM CS

To host, route to, and manage Java connectors, install CA IAM CS. If you plan to install more than one CA IAM CS, see the chapter on High Availability Provisioning Installation for additional guidelines.

Important! We recommend that you disable all antivirus software before installing CA IAM CS or its SDK. If anti-virus software is enabled while installation processes are taking place problems can occur. Remember to reenable your antivirus protection after you complete installation.

Follow these steps:

1. Log into the system as a Windows administrator or a UNIX or Linux root user.
2. Ensure that the time settings (see page 113) on all computers that will host connector servers match.
3. For Linux systems, ensure that the prerequisite packages (see page 115) are installed.
4. Launch the installer.

   You can install CA IAM CS using the main installer that installs all CA IdentityMinder components, or you can navigate to the following subfolder and run the *setup* file.

   `Provisioning\ConnectorServer`
5. Select the setup type (Typical or Custom). If you choose Typical, you cannot change the installation location, but you can change everything else.
6. Enter an installation path (Custom setup type only).
7. Configure Connector Server C++ Management:
   - None—Does not install CCS. If you install CCS later, it will not be managed by CA IAM CS.
   - Local—Installs CCS on the same computer as CA IAM CS. CCS will be managed by CA IAM CS.
   - Remote—Configures CA IAM CS to manage an existing remote CCS.

8. (Recommended) Register the CA IAM CS installation with a provisioning server. For more information, see Provisioning Server Registration (see page 119).

   Use the following information:

   Domain

   Defines the Provisioning Server domain.

   Server Host

   Defines the Provisioning Server.

   Server Port

   Defines the port on which the Provisioning Server runs.

   Username

   Specifies the Provisioning Server administrator.

   Password

   Defines the Provisioning Server administrator password.

9. (Optional) Register with the Cloud CA IAM CS. When you connect a cloud version of the connector server with an on-premises version, the two connector servers can communicate to manage connections to cloud and on-premises endpoints.

10. Configure a password and the following ports:

    Message broker ports

    The message broker sends messages between instances of CA IAM CS on different computers:

    - HTTP port (default 22001)
    - HTTPS port (default 22002)

    Web ports

    You can log in to CA IAM CS though a web interface, using these ports:

    - HTTP port (default 20080)
    - HTTPS port (default 20443)

    RMI Registry port

    You can use this port to view information about the running Java process (default 1099).

11. (Optional) Configure an HTTP Proxy. The details of this proxy can be used for the following applications:

    - When communicating with a cloud connector server.
    - When creating a Google Apps or Salesforce endpoint. For these endpoints, you can either use this HTTP proxy or no proxy. You cannot specify a different proxy. To change the HTTP proxy details, run this installation program again, and enter the new proxy details.

    Note: If your organization has a direct connection to the internet, we recommend that you do not set up an HTTP proxy.

    Use the following information to set up the HTTP proxy:

    Host

    Specifies the name of the HTTP proxy server that you want to use to connect to endpoints.

    Port

    Specifies the port on which CA IAM CS can access the HTTP proxy.

    Domain

    Specifies the domain of the HTTP proxy.

    Username

    Specifies the user name you want to use to log in to the proxy server.

    Note: We recommend that you specify a user name and password if your organization's proxy server requires authentication.

    Password

    Specifies the domain password for the HTTP proxy.

12. (Optional) Activate FIPS 140-2 Compliance Mode.
13. Click Next.

    The installation program installs CA IAM CS, and then creates a new service. On Windows this is added to Services, and on UNIX it is a script.

Provisioning Server Registration

CA Technologies recommends that you always register CA IAM CS with the Provisioning Server. Registering tells the Provisioning Server to use the CA IAM CS being installed to manage all the static connectors that have been deployed to it. If you want a different connector server to manage a specific static or dynamic connector, you can use Connector Xpress to specify the instance of CA IAM CS that you want to manage the connector.

It is also possible to use Connector Xpress to create new namespaces in a Provisioning Server, where the connector has already been deployed to a particular instance of CA IAM CS. Either use bundled template files, or where they are not available, create a project by importing the connector's metadata. When the metadata is available, deploy a new namespace.

Note: For more information see the *Connector Xpress Guide*.

Install the C++ Connector Server

When you install CA IAM CS, you can install the C++ Connector Server (CCS). The procedure in this topic applies for a single connector server. If you plan to install more than one CCS, see the chapter on High Availability Provisioning Installation.

Follow these steps:

1. Run the following program where you unpacked the install package.
   - **Windows:**
     `Provisioning\Provisioning Server\setup.exe`
   - **UNIX:**
     `Provisioning/ProvisioningServer\setup.bin`
2. Complete the instructions in the installer dialog boxes.

   This installation program also gives you the option to install alternate Provisioning Servers. However, for that component, a different procedure applies.

Install CA IAM CS Silently

You can install CA IAM CS silently. Before you run a silent installation, create a response file.

Note: Use fully qualified path names when generating and running response files. For example, responsefile.txt is not valid but C:\responsefile.txt is valid.

Follow these steps:

1. In a command window, navigate to the following location within the extracted installation files:

   `Servers/ConnectorServer`

2. To create a response file enter the following command and then enter the required values in the template:

   `setup –options-template` *`filename`*

3. Start the silent installation using the following command:

   `setup –options` *`filename`* `-silent`

Note: To create a response file and install CA IAM CS at the same time, use the following command:

`setup -options-record` *`filename`*

Install the SDK for CA IAM CS

To learn how to write connectors by looking at worked examples, install the SDK for CA IAM CS, and the sample connectors. These examples are described in the *Connectors Programming Guide*.

Important! Install the SDK on a different computer from the computer where you installed the CA IAM CS.

Follow these steps:

1. Locate the CA IdentityMinder installation download or other media, then extract the product files (ZIP or TAR).
2. Navigate to the following subfolder:

   `Provisioning/ConnectorServerSamples`

   Note: In this folder, the compressed file *jcs-connector-sdk* contains the SDK itself. The other files each contain one sample connector.
3. Copy the files from this folder to the following subfolder:

   `Provisioning/ConnectorServer`
4. Run the installation program for CA IAM CS.

Note: For more information about the SDK for CA IAM CS, read the *cs-sdk-home*/Readme.txt.

More information:

File Locations (see page 114)

Install the Connector Samples

Important! We recommend that you use the sample connectors only in a test environment. We do not support the sample connectors. Therefore, no uninstallation program exist for these samples.

Extract the installer for your operating environment and the samples archive to the same folder before performing an install.

Set Up JDBC Support

For some connectors you must activate JDBC connection yourself. The installer cannot activate these connectors because we cannot legally ship some drivers and licenses with CA IAM CS, or because these connectors require additional manual configuration before activation.

Important! After you upgrade to a newer version of the connector server, run the following procedures again.

Set Up License Files for the DB2 for z/OS Connector

The DB2 for z/OS connector uses JDBC, and it requires a license file to connect to the DB2 endpoint. The license file is available only if you already have a license for DB2 Connect.

For information, see the following IBM technotes:

- IBM technote: Location of the db2jcc_license_cisuz.jar file
- IBM technote: DB2 JDBC driver is not licensed for connectivity

Follow these steps:

1. Install or upgrade CA IAM CS.

   The installation registers CA IAM CS with the provisioning server, creates the DBZ endpoint type, and populates it with its associated metadata.

2. Find *db2jcc_license_cisuz.jar*, which is in the following location on the DB2 Connect activation CD:

   `/db2/license`

3. Copy the license file to the following location on the CA IAM CS computer:

   `cs_home``/jcs/resources/jdbc`

4. Run the *jdbc_db2_zos* script in the same location.

   This script creates a bundle that contains the license file, which you deploy using CA IAM CS.

5. Log in to CA IAM CS.
6. At the top, click the Connector Servers tab.
7. In the Connector Server Management area, click the Bundles tab.
8. Add the new bundle:

   Note: You can deploy the OSGI bundle from the connector server GUI or copy the jar files to ca-home/jcs/data/bundles/restore. Then restart the connector server and wait up to ten minutes for it to load.

   a. In the Bundles area on the right, click Add.

   b. Browse to the bundle that the script created, then select the connector server on which this connector will be available.

   c. Click OK.

      The new bundle appears in the Bundles list.

9. Find the main connector bundle in the Bundles list, then right-click its name in the list and select Refresh Imports from the popup menu.

CA IAM CS can now connect to DB2 endpoints.

Set Up License Files for the Sybase Connector

To connect to a Sybase endpoint, CA IAM CS requires a file from the Sybase SDK for JDBC. You must also have a license for Sybase.

Note: Sybase can only be administered as a DYN/JDBC endpoint.

Follow these steps:

1. Find the following driver file. You can download this from http://www.sybase.com, and it is also included on your Sybase product media:

   `jConnect-6_05.zip`

2. Extract the following file from the ZIP:

   `jConnect-6_0\classes\jconn3.jar`

3. Copy the jconn3.jar file into the following location:

   `conxp_home/lib/`

4. Stop and restart any Connector Xpress sessions.

5. In a command window, navigate to the following location:

   `cs-home/jcs/resources/jdbc`

6. Run the following script:

   - Windows: jdbc_sybase_post_install.bat
   - UNIX: jdbc_sybase_post_install

   This script creates a bundle that contains the license file, which you deploy using CA IAM CS.

7. Log in to CA IAM CS.

8. At the top, click the Connector Servers tab.

9. In the Connector Server Management area, click the Bundles tab.

10. Add the new bundle:

    Note: You can deploy the OSGI bundle from the connector server GUI or copy the jar files to ca-home/jcs/data/bundles/restore. Then restart the connector server and wait up to ten minutes for it to load.

    a. In the Bundles area on the right, click Add.

    b. Browse to the bundle that the script created, then select the connector server on which this connector will be available.

    c. Click OK.

       The new bundle appears in the Bundles list.

11. Find the main connector bundle in the Bundles list, then right-click its name in the list and select Refresh Imports from the popup menu.

CA IAM CS can now connect to Sybase endpoints.

Set Up Windows Authentication for the SQL Server Connector

Microsoft SQL Native Authentication on Windows can only be activated when both Connector Xpress and CA IAM CS are running on Windows operating systems. The required library sqljdbc_auth.dll is bundled with Connector Xpress, or you can download it from Microsoft.

If you plan to use Connector Xpress, it must run on the same domain as the Microsoft SQL Server endpoint. Also, SQL Server must be configured to allow the user to access the appropriate database instances.

Follow these steps:

1. Update the CA IAM CS service to run as the required Windows user.

   By default the service is set to run as the local SYSTEM user. However, if you are using trusted authentication, run the service as a domain user. Perform these steps:

   a. Click Start, Control Panel, Administrative Tools, Services.

   b. Right-click CA IdentityMinder-Connector Server (Java), then click Properties.

   c. Select the Account check box, and then complete the details of the domain user under which you want to run the service.

2. Stop and restart the CA IAM CS service.

3. When you set up Microsoft SQL datasource in Connector Xpress, select the Native check box on the Edit Sources dialog.

   Connector Xpress adds the following to the JDBC URL used for the connection:

   ```
   integratedSecurity=true
   ```

   Note: For more information about configuring data sources, see the *Connector Xpress Guide*.

More Information about Setting Up Connectors

For more information about connectors and the required components, see the *Connectors Guide*. This guide includes information about which components to install where, and also specific instructions for each endpoint type.

Chapter 9: High Availability Provisioning Installation

Based on the guidelines in this chapter, you implement high availability for provisioning components by installing alternate Provisioning Servers and Provisioning Directories, and connector servers for C++ and Java connectors.

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 and configure your system as required.
	2. Perform one of these installations: ■ Single node installation ■ Installation on an application server cluster
	3. (Optional) Create separate databases.
	4. (Optional) Install the Report Server.
X	**5. (Optional) Install alternate Provisioning Directories, alternate Provisioning Servers, and connector servers to support failover and load balancing.**

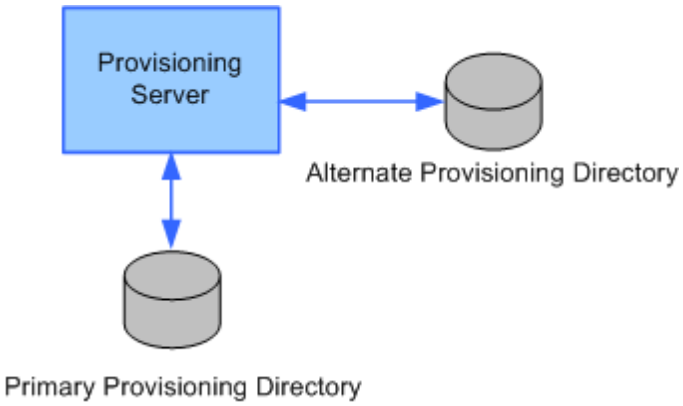
How to Install High Availability Provisioning Components

The following table describes the steps involved in installing provisioning components for high availability:

✓	Step
	1. Install primary and alternate Provisioning Servers and provisioning directories for load balancing and failover.
	2. Install several connector servers for load balancing and failover.
	3. Enable clients of the provisioning server to fail over.

Redundant Provisioning Directories

To support failover, you can install primary and alternate Provisioning Directories. For example, you may have two systems, one with the Provisioning Server and the primary Provisioning Directory on it. The second system has the alternate Provisioning Directory. If the primary Provisioning Directory fails, the alternate Provisioning Directory is assigned automatically.



Follow these steps:

1. Install the primary Provisioning Directory using the Provisioning Directory installer from where you unpacked the install package.
   - **Windows:**
     Unpacked-Install-Package\Provisioning\Provisioning Directory\setup.exe
   - **UNIX:**
     Unpacked-Install-Package/Provisioning/ProvisioningDirectory/setup
2. Install one or more alternate Provisioning Directories. See the next section.

Install Alternate Provisioning Directories

Once you have performed the prerequisite configuration required, you can install alternate Provisioning Directories.

Follow these steps:

1. Log in as a Local Administrator (for Windows) or root (for Solaris) into the system where you plan to install the alternate Provisioning Directory.
2. Be sure that CA Directory is installed on this system.
3. Copy custom schema files to the %DXHOME%/config/schema directory if any of the following is true for the primary Provisioning Directory:
   - COSX (etrust_cosx.dxc) has been modified
   - LDA connector (etrust_lda.dxc) is installed
   - A custom C++ connector schema has been created

   The Provisioning Directory installation checks the %DXHOME%/config/schema directory for extra schema files named etrust_*.dxc, and adds them to the group schema file, impd.dxg. If the custom schema files are not copied locally, data replication between the Provisioning Directories fails.
4. Run the Provisioning Directory installer from where you unpacked the install package.
   - **Windows:**
     Unpacked-Install-Package\Provisioning\Provisioning Directory\setup.exe
   - **UNIX:**
     Unpacked-Install-Package/Provisioning/ProvisioningDirectory/setup
5. Select High Availability, and respond to the questions about the hostnames for systems where other Provisioning Directories are installed and which system is the primary Provisioning Directory.

6. Respond to other questions using the same answers given during the primary Provisioning Directory installation for:
   - Deployment Size
   - Shared Secret
   - FIPS key
7. Respond to this question based on how and when you want to replicate data from the Primary Provisioning Directory:
   `Do you want to start replication to the Provisioning Directory.`

   If you are upgrading from a previous release, you may have a significant amount of data to replicate. You should deselect the checkbox if you do not want replication to start at this time. After the installation, you would then need to copy an LDIF data dump or online backup files from an existing Provisioning Directory and load the data or start the DSAs manually, which will start automatic replication.

Important! If alternate Provisioning Directory installation failed, data replication may have occurred before the failure. If so, the master and alternate Provisioning Directories have a record that replication occurred. If you now reinstall the alternate Provisioning Directory, that data is not replicated again. Instead, use the High Availability Configuration command on the primary and alternate Provisioning Directories to remove and add back the alternate Provisioning Directory before you reinstall it.

Reconfiguring Systems with Provisioning Directories

If needed, you can change the configuration of which systems have a Provisioning Directory.

Follow these steps:

1. Log into the system where the primary Provisioning Directory is installed.
2. On a command line prompt, navigate to the highavailability sub-directory where you installed the Provisioning Directory. For example:

   ```
   cd C:\\Program Files\CA\Identity Manager\Provisioning Directory\highavailability
   ```
3. Enter this command:

   ```
   highavailability.bat
   ```

   The command displays a summary of the current configuration: the domain name, the hostname of each Provisioning Server and Provisioning Directory, and which one is the Primary Provisioning Directory.

4. Respond to prompts for the hostnames for each alternate Provisioning Directory that you plan to add.

   If you plan to install alternate Provisioning Servers, you can add their hostnames now by responding to the prompts.

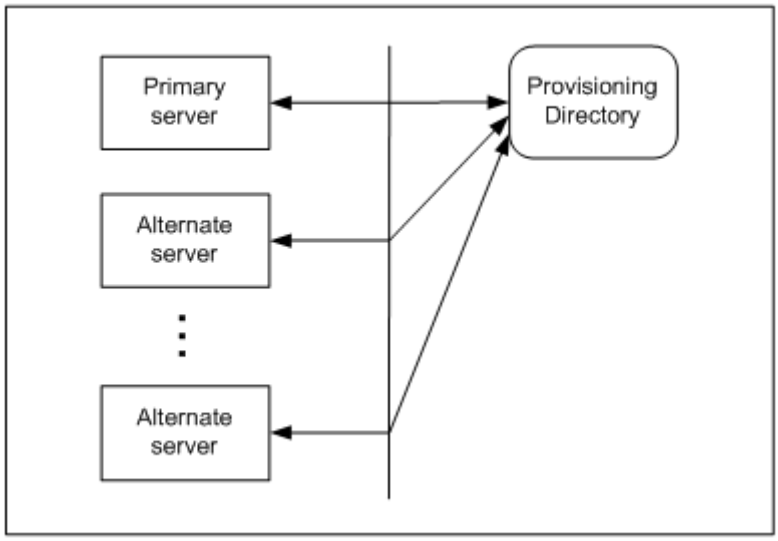
5. Log in to all other Provisioning Directory and Provisioning Servers and repeat steps 2 through 4.

   The configuration on each system needs to match.

Redundant Provisioning Servers

Multiple Provisioning Servers share the workload of a provisioning domain, providing performance, scalability, and high availability. The first Provisioning Server installed is called the primary Provisioning Server. Additional servers are called alternate Provisioning Servers.

As shown in this illustration, you can configure multiple alternate Provisioning Servers for one primary Provisioning Server.



In this illustration, three Provisioning Servers are configured to serve the provisioning domain. All servers are configured to use the Provisioning Directory of the primary Provisioning Server installation.

Router DSA for the Provisioning Server

The Provisioning Server communicates through a CA Directory router DSA, and not directly to the Provisioning Directory. The router DSA, imps-router, is installed with the Provisioning Server installer. This DSA accepts requests from the Provisioning Server and routes them to the appropriate Provisioning Directory DSA (impd-co, impd-main, impd-inc, or impd-notify) depending on the prefix.

In a high-availability installation, the imps-router DSA has connection information for Provisioning Directory DSA on at least one alternate Provisioning Directory system. If a primary Provisioning Directory DSA becomes unavailable, the router DSA attempts to use an alternate DSA.

The imps-router DSA has been assigned ports 20391, 20391, 20393 (for address, SNMP, and console respectively).

Note: In previous releases of this software, the etrustadmin DSA used port 20391. Any connections to 20391 on the Provisioning Directory system fail unless the Provisioning Directory and Provisioning Server are on the same system. Therefore, reroute these connections to port 20391 on the Provisioning Server system.

For CA Directory DSAs running on one system to communicate with DSAs on another system, they must have connection information for each other. So during Provisioning Directory installation, you identify each Provisioning Server that can connect to it.

Install Provisioning Servers

To support failover, you can install primary and alternate Provisioning Servers.

Follow these steps:

1. Install the primary Provisioning Server using the Provisioning Server installer from where you unpacked the install package.
   - **Windows**:
     Unpacked-Install-Package\Provisioning\Provisioning Server\setup.exe
   - **UNIX or Linux**:
     Unpacked-Install-Package/Provisioning/ProvisioningServer/setup
2. Install one or more alternate Provisioning Servers. See the next section.
3. Enter the alternate Provisioning Server host and port number when you enable provisioning in the CA IdentityMinder Management Console. For details, see the *Configuration Guide*.

Install Alternate Provisioning Servers

Once you have performed the prerequisite configuration involving the highavailability command, you can install one or more Provisioning Servers.

Follow these steps:

1. Log in as a Local Administrator (for Windows) or root (for Solaris) on each system that will host an alternate Provisioning Server.
2. Make sure that CA Directory is installed on this system.
3. Copy custom schema files to the %DXHOME%/config/schema directory if any of the following is true for the primary Provisioning Directory:
   - COSX (etrust_cosx.dxc) has been modified
   - LDA connector (etrust_lda.dxc) is installed
   - A custom C++ connector schema has been created

   The Provisioning Directory installation checks the %DXHOME%/config/schema directory for extra schema files named etrust_*.dxc, and adds them to the group schema file, impd.dxg. If the custom schema files are not copied locally, the Provisioning Server will not route any custom schema.
4. Run the Provisioning Server installer from where you unpacked the install package.
   - **Windows**:
     Unpacked-Install-Package\Provisioning\Provisioning Server\setup.exe
   - **UNIX**:
     Unpacked-Install-Package/Provisioning/ProvisioningServer/setup
5. Complete the instructions in the installer dialog boxes.

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

Reconfiguring Systems with Provisioning Servers

If needed, you can change the configuration of which systems have a Provisioning Server.

Follow these steps:

1. Log into the system where the primary Provisioning Directory is installed.
2. On a command line prompt, navigate to the location where you installed the Provisioning Directory or Provisioning Server. You find the highavailability sub-directory there. For example:

   ```
   cd C:\\Program Files\CA\Identity Manager\Provisioning Directory\highavailability
   ```

3. Enter this command:

   `highavailability.bat`

   The command displays a summary of the current configuration: the domain name, and the hostname of each Provisioning Server and Provisioning Directory.

4. Respond to the prompts to provide the hostnames required for each Provisioning Server that you want to add.

   If you plan to also install alternate Provisioning Directories, you can add their hostnames now by responding to the command prompts.

5. Log in to each system that will host a Provisioning Directory and repeat Steps 2 through 4.

   The configuration on each system needs to match.

Configure Provisioning Server Failover

For CA IdentityMinder to distinguish the primary from the alternate Provisioning Server, you create server definitions in JIAM in the Management Console. You create these definitions in the directory object associated with the CA IdentityMinder directory for your environment. During initialization, CA IdentityMinder reads any failover server definitions defined in that object, adding them to the JIAM failover server definitions.

Note: For details on setting up server definitions, see the *Configuration Guide*.

Redundant Connector Servers

With the Connector Server Framework (CSF), you can run multiple Connector Servers and configure the Provisioning Servers to communicate with Connector Servers in specific contexts.

As a result, the Provisioning Server can:

- Support Connector Servers on different platforms to manage endpoint types that are unavailable on the platform where the Provisioning Server is installed.
- Communicate with multiple Connector Servers, which each manage a different set of endpoint types or endpoints. Therefore, endpoint types or endpoints can be managed on a parallel basis to achieve load balancing.

Installing Multiple Connector Servers

When you configure multiple instances of a connector server as network peers, they automatically synchronize the password used by their administrative account. For this reason, we recommend that you set the same account details during installation.

If you install multiple instances of a connector server on the same computer, ensure that each instance uses unique port numbers. If any port numbers are used by more than one instance of a connector server, the servers will behave unpredictably.

Connector Server Framework

The use of several Connector Servers is called the Connector Server Framework. The Connector Server Framework has two important characteristics:

- Scalability - multiple connector servers may share the load of working on a set of endpoints.

  For example, a lengthy exploration of an endpoint on one connector server does not influence the ability to operate on an endpoint that is being controlled by another Connector Server

- Communication channel security - communication between Provisioning Server and connector server is encrypted using TLS.

  If an endpoint type uses a proprietary protocol to communicate between the connector server and endpoints of that protocol, the extent of use of the proprietary protocol may be limited to a local network, or even to just local communication inside one server.

When deciding on an implementation strategy, consider these factors so that you protect the Connector Servers in your organization against unauthorized access:

- The Connector Server may be configured to disclose passwords in clear text.

  Any person with access to the system running the Connector Server and with sufficient privileges to modify the configuration of the Connector Server and to restart the Connector Server can make the Connector Server log passwords appear in clear text.

  The Connector Server is based on the open source slapd process. The instructions to make a slapd process log incoming passwords in clear text are in the public domain, for example, by looking at the manual pages at http://www.openldap.org

- The Connector Server is only protected by a bind password.

  The Connector Server trusts any client who connects to it and is able to provide the proper credentials, such as Bind DN and Bind Password. The Connector Server does not know if the connection comes from a Provisioning Server or not. Any user with internal access may disclose the bind password, then connect to the Connector Server from another server, and so have administrator privileges over the endpoints controlled by the Connector Server.

- The Connector Server is not protected against brute force attacks on the bind password

  Unlike the Provisioning Server, the Connector Server is not protected against repeated attempts at binding with different passwords. An attacker may therefore try to guess the password by brute force attack. Should an attacker succeed in guessing the bind password, then the road is open for the attacker to control the endpoints under control of the Connector Server.

For these reasons you are advised to design your implementation such that

- The same organizational unit is responsible for administrative access to all Provisioning Servers and connector servers.
- Your connector servers are suitably protected by firewalls or similar such that the ports may not be reached by unauthorized means.
- The ability to connect to Provisioning Servers and connector servers on non-TLS ports should be disabled in your production environments.

If you install multiple connector servers on one computer, make sure that each instance uses a unique set of port numbers.

Load-Balancing and Failover

Failover and load-balancing of connector requests is achieved by each provisioning server based on the CSF configuration defined using csfconfig or Connector Xpress.

Each provisioning server consults the CSF configuration that applies to it and determines which Connector Servers it should use to access each endpoint or endpoint type. Failover and load-balancing occur when there are multiple connectors servers configured to serve the same endpoint or endpoint type.

Failover and load-balancing are unified and cannot be controlled separately. One cannot indicate that a particular connector server is to remain idle except when needed for failover. Instead, a provisioning server that is configured to use two or more connector servers interchangeably will distribute work between these connector servers (load balancing) during normal operation. Should one or more of the Connector Server become unavailable, the remaining connector servers will provide failover support for the unavailable connector servers.

Reliability and Scalability

With the Connector Server Framework (CSF), the Connector Server high availability features increase reliability and scalability.

Reliability is enhanced by having multiple Connector Servers serve a Provisioning Server, so it can continue to function if one or more Connector Servers become unavailable.

For example, if one Connector Server manages the UNIX endpoint type and another manages the Active Directory endpoint type; and the Active Directory Connector Server becomes unavailable, the Provisioning Server can still manage the UNIX endpoint types.

Scalability is achieved by having a mechanism to add more Connector Servers to manage an increasing amount of endpoint types or endpoints. For example, if the number of endpoint types increases to 100, the Provisioning Server can be configured to have 20 Connector Servers, with each Connector Server managing five endpoint types. Or configure 20 Connector Servers with each Connector Server managing overlapping sets of 10 endpoint types to allow for failover and load balancing behaviors as well.

Multi-Platform Installations

The Connector Server Framework is the configuration of Connector Servers that exist on multiple systems, which could be Windows or Solaris systems.

The following use cases are supported:

- Use Case 1
  - Provisioning Server and connector server installed on a Solaris system.
  - A second Connector Server installed on a Windows system, serving the non-multi-platform connectors.
- Use Case 2
  - Provisioning Server and connector server installed on a Windows system.
  - A second Connector Server installed on Solaris system, serving the multi-platform connectors.
  - A third Connector Server installed on a remote Windows system, serving the other connectors.

- Use Case 3
  - Provisioning Server installed on a Windows or Solaris system and a Connector Server installed on the same system.
  - Multiple additional Connector Servers installed on Windows or Solaris systems, serving as endpoint agents. This scenario is important for cases where the connector is using a proprietary or un-secured communication channel. Using this topology, the important segment of network traffic is secured by the standard Provisioning Server to Connector Server communication protocol and not by the proprietary protocol.

Configure Connector Servers

You configure the Connector Server Framework by using the csfconfig command or by using Connector Xpress. The csfconfig command uses the data in the Windows Registry (or UNIX counterpart created for Provisioning Server) to connect to a Provisioning Server. The csfconfig command must run on the system where one of the Provisioning Server runs.

Using the command, you can:

- Add or modify a Connector Server connection object with information such as the connector server, host, and port.
- Define for which endpoints or endpoint types the connector server is used; possibly varying this definition for alternate provisioning servers.
- Delete the Connector Server connection information object.
- List all connector server connection objects in a domain.
- Show one or all connector server connection objects for one or all connector servers

The csfconfig command uses the authorizations provided by a global user credential, so that global user must have the necessary administrative privileges to manipulate the appropriate ConfigParam and ConfigParamContainer objects.

csfconfig Command

To use the csfconfig command, the command line syntax is:

```
csfconfig [--help[=op]] [operation] [argument]
```

You can use these arguments in any order. The operation argument is required unless you are using the --help argument.

The --help[=op] option provides minimal on-line help. The "=op" argument may be used to list the arguments that are required or optional for the operation. For example, "--help=add" will provide a description of the add operation, while "--help" will provide general information.

If help is requested, other arguments are ignored and no request is sent to the server.

Note: The domain parameter can be omitted as it is always the domain used in the whole installation.

The following operations are available.

add

Add a new CS connection object. A name will be generated by this operation if one is not specified by the user. Required arguments: auth, host, pass. Optional arguments: authpwd, br-add, desc, domain, name, port, usetls, debug.

addspec

Adds a branches specialization for one provisioning server.

When you have installed alternative provisioning servers, sometimes a connector server is not to be used by all of these Provisioning Servers. Or sometimes different provisioning servers will want to use the same connector servers for different branches (endpoint types or endpoints). A branches specialization is a list of branches that is specific to one provisioning server. Only provisioning servers without a specialization will use the branches specified in the main CS connection object. Required arguments: auth, name, server. Optional arguments: authpwd, br-add, domain, debug.

list

List all CS connection objects. Required arguments: auth. Optional arguments: authpwd, domain, debug.

modify

Modify a CS connection object. Required arguments: auth, name. Optional arguments: authpwd, br-add, br-rem, desc, domain, host, pass, port, usetls, debug.

modspec

Edits a specialization created by addspec. Required arguments: auth, name, server. Optional arguments: authpwd, br-add, br-rem, domain, debug.

remove

Remove an existing CS connection object. Required arguments: auth, name. Optional argument: authpwd, debug.

remspec

Removes a specialization created by addspec. Required arguments: auth, name, server. Optional arguments: authpwd, domain, debug.

modify

Modify a CS connection object. Required arguments: auth, name. Optional arguments: authpwd, br-add, br-rem, desc, domain, host, pass, port, server, tls, usetls.

show

Show a specific CS connection object or show all CS connection objects. The output shows the host and port of the connector server if it is available. Required arguments: auth. Optional arguments: authpwd, name, domain, debug.

Each operation takes several arguments in the form “name=value”. Spaces are not allowed before or after the “=” symbol, and if the value contains any spaces, the argument must be quoted appropriately for the platform (Windows or UNIX). Except as noted, the value must be provided, and must be non-empty.

The following arguments are used for the operations as noted above:

auth=<value>

Identify the global user for authentication.

Value format: “name” where name is the global user's name.

authpwd=<value>

Identify a file containing just the global user's password on the first line. If this argument is not specified, the user will be prompted for a password.

Value format: any appropriate operating system file path.

br-add=<value>

Add a new branch. This argument may be specified multiple times to add multiple branches.

Value format: “[[endpoint,]endpoint type][@[domain]]”. Use a branch of “@” by itself to represent all branches. Add “endpoint type” or “endpoint,endpoint type” to identify a specific endpoint type or endpoint.

br-rem=<value>

Remove an existing branch. This argument may be specified multiple times to remove multiple branches.

Value format: same format as specified for br-add.

debug=<value>

Turns on trace logging for the command. Tracing messages are written to the file PSHOME\logs\etaclientYYYYMMDD.log file.

Value format: The value “yes" enables logging.

desc=<value>

Provide an arbitrary description for the object. If not specified in an add operation, it will default to the value of the host argument.

Value format: an arbitrary string.

domain=<value>

Define the default domain. If not specified, the domain specified in the auth argument is used as the default.

As the value can only be the default, this parameter can always be omitted

host=<value>

Define the name of the host on which the Connector Server runs.

Value format: any legal host name or IP address.

name=<value>

The name of the Connector Server object. If not specified during Add, csfconfig will assign a name and display what name was created.

Value format: A case-insensitive string of one or more characters consisting of upper-case English letters (A-Z), lower-case English letters (a-z), digits (0-9), hyphen(-) or underscore(_).

pass[=<value>]

Define the file containing the password for the Connector Server connection object. If the value is not specified, the user will be prompted.

Value format: any appropriate OS file path.

Important! The password you must specify is the password you entered when you installed that Connector Server or you changed subsequent to install by running the pwdmgr utility on that Connector Server system.

port=<value>

Define the port number for the object. This must be a valid number for a port where the Connector Server listens for connections.

Value format: an integer.

server[=<value>]

In addspec, modspec and remspec commands, define the name of the Provisioning Server that is served by the Connector Server . The branches defined in a specialization override, for a particular provisioning server, the branches defined in the CS configuration object by add and modify commands.

Value format: the name of the host where the Provisioning Server is running as returned by the system's hostname command.

Note: The Connector Server configuration objects are stored with the other domain configuration parameters in the provisioning directory. While the Connector Server configuration parameters cannot be viewed or changed with the provisioning manager directly, one can use the provisioning manager (System task, Domain Configuration button) to get a list of known provisioning servers. To do this, open the “Servers” parameter folder and the known provisioning servers will be listed.

usetls[=<value>]

Indicate if TLS should be used to communicate with the Connector Server. The value is optional for the add operation only, in which case it defaults to “yes.” .

Value format: a string “yes” or “no”.

Upon successful completion of the add operation, the name of the newly created Connector Server connection object will be listed. If the name parameter is missing, a name is generated. For example:

```
Created CS object with name = SA000
```

For most operations, successful or not, the status and a message (if any) will be shown. For example:

```
The host name, port number, or TLS flag was successfully changed. The branch settings
were successfully changed.
```

For some errors, such as invalid command line parameters, no status code or server error message is displayed. In these cases, a simple statement of the error will be shown. For example:

```
$ csfconfig add
No authentication information supplied.
For on-line help, use "--help [=<op>]"
```

csfconfig Command Examples

To specify that the UNIX and CA Access Control endpoint types should be served by the Connector Server running on host "sunserver01" and the remaining endpoint types served by a Connector Server running on host "windows02", issue the following commands.

Each command execution prompts you for the etaadmin password.

```
csfconfig add \
auth="etaadmin" \
br-add="UNIX – etc" \
br-add="UNIX – NIS-NIS plus Domains" \
br-add="Access Control" \
host="sunserver01" \
usetls="yes"

csfconfig add \
auth="etaadmin" \
br-add="@" \
host="windows02" \
usetls="yes"
```

C++ Connector Server on Solaris

If you install C++ Connector Server (CCS) on UNIX, it has some limitations. For information, see CCS on Windows and UNIX.

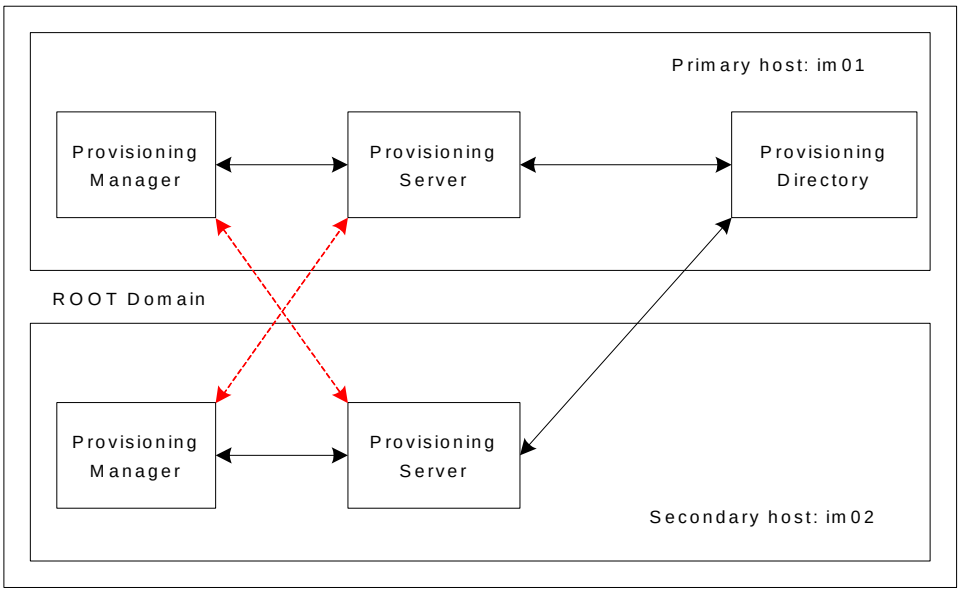
Failover for Provisioning Clients

Client-tier configuration includes the following tasks:

- Configure the Windows client-tier failover
- Configure the Provisioning Manager to communicate with their local Provisioning Servers, and fail over to the remote Provisioning Server

You use the same Provisioning Manager dialog to accomplish both of these tasks, on each server in turn.

The configuration shown in the following illustration lets Provisioning Manager submit identity provisioning requests to one Provisioning Server and fail over to another server:



The Provisioning Manager sends requests to the default Provisioning Server and fails over to another server.

Enable User Console Failover

If the application server for the CA IdentityMinder Server fails, it does not receive Provisioning Server updates. As a result, the CA IdentityMinder User Console does not show provisioning changes. Therefore, you should configure an alternate URL for the CA IdentityMinder Server.

Follow these steps:

1. Launch the Provisioning Manager.
2. Click System, CA IdentityMinder Setup.
3. Fill in the host name and port for another system in the cluster.
4. Fill in the environment.

   It must be the same one that is on the primary URL.
5. Click Add.

Enable Provisioning Manager Failover

You can enable Provisioning Manager failover on both the primary and secondary host servers. When this procedure is complete, you will have configured each server for failover to the other.

Follow these steps:

1. Launch the Provisioning Manager.
2. Select File, Preferences, and select the Failover tab.
3. Mark the Enable Failover check box. By default, the local Provisioning Server is already defined.
4. Click Add.
5. Enter the host name of the remote Provisioning Server.

   For example, on im01, enter the server host for im02. On im02, enter the server host for im01.
6. Enter 20389 for the LDAP port value and 20390 for the LDAP/TLS port value, respectively.
7. Adjust the preference order by moving the entries up and down in the list.
8. Click OK.
9. Restart the Provisioning Manager to enable your changes.

Test the Provisioning Manager Failover

You can test your client failover configuration by performing the following procedure:

Follow these steps:

1. Stop the CA IdentityMinder - Provisioning Server service on one domain server.
2. Issue one or more operations using Provisioning Manager for this server installation.

   Since you stopped the CA IdentityMinder - Provisioning Server service locally, the traffic flows to the failover domain server. If it does not, check your configuration and try the test again.

Appendix A: Uninstallation and Reinstallation

This section contains the following topics:

How to Uninstall CA IdentityMinder

To fully uninstall CA IdentityMinder, remove CA IdentityMinder software components and clean up the CA IdentityMinder-specific configuration in your application server. The following checklist describes the steps to uninstall CA IdentityMinder:

✓	Step
	1. Delete CA IdentityMinder objects with the Management Console.
	2. (Optional) If you used SiteMinder, remove the CA IdentityMinder schema from the policy store or remove the Policy Server. For more information, see the *CA SiteMinder Web Access Manager Policy Server Installation Guide*.
	3. Use the highavailability command to uninstall Provisioning Directories and Provisioning Servers from this location: *Unpacked-Install-Package*\Provisioning\Provisioning Directory\highavailability
	4. Uninstall the CA IdentityMinder components.
	5. Remove CA IdentityMinder configuration information from the application server.

Remove CA IdentityMinder Objects with the Management Console

In order to remove objects created automatically by CA IdentityMinder when you configure environments and directories, use the Management Console.

1. Open the Management Console:

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

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 CA IdentityMinder Schema from the Policy Store

If you were using a SiteMinder Policy Server, remove the CA IdentityMinder schema from the policy store.

Remove the CA IdentityMinder schema from a SQL Policy Store

On systems where you installed the CA IdentityMinder Extensions for SiteMinder, remove the CA IdentityMinder schema. The default location for the command to remove the schema follows:

- SQL Server:
  `C:\Program Files\CA\Identity Manager\IAM Suite\Identity Manager\tools\policystore-schemas\MicrosoftSQLServer`
- Oracle:
  `UNIX`:
  `/opt/CA/IdentityManager/IAM_Suite/Identity_Manager/tools/policystore-schemas/OracleRDBMS`

  `Windows`: `C:\Program Files\CA\Identity Manager\IAM Suite\Identity Manager/tools/policystore-schemas/OracleRDBMS`

Remove the CA IdentityMinder schema from an 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. For more information, see the documentation for your directory.

Follow these steps:

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 CA IdentityMinder Software Components.
   - If you are using CA Directory as a policy store, remove the etrust_ims.dxc file from *dxserver_home*\config\schema.

     where *dxserver_home* is the install location of CA Directory.

     Note: There are no other steps required to remove the schema from a CA Directory Server. Continue with Uninstall CA IdentityMinder Software Components.
   - If you are using another LDAP directory as a policy store, skip to Step 2.
2. Navigate to the policystore-schemas folder. These are the default locations:
   - **Windows:** C:\Program Files\CA\Identity Manager\IAM Suite\Identity Manager\tools\policystore-schemas
   - **UNIX:** /opt/CA/IdentityManager/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.

   Note: For more 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

Directory Type	LDIF File
Sun Java Systems (Sun One, iPlanet)	sunone\sunone-delete-ims8.ldif

Uninstall CA IdentityMinder Software Components

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

To uninstall CA IdentityMinder software components on Windows:

Follow these steps:

1. Go to Start, Control Panel, Add/Remove Programs and select CA IdentityMinder.
2. Select CA IdentityMinder.
3. Click Change/Remove.

   All non-provisioning components are uninstalled.
4. For any provisioning components, use the individual component installer to uninstall the component.

   Note: Although you install Provisioning Manager with Administrative Tools, you use the Provisioning Manager installer to uninstall this component.

To uninstall CA IdentityMinder software components on UNIX:

Follow these steps:

1. Navigate to the following location:

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

   `sh uninstall.sh`

   Follow the on-screen instructions.
3. For any provisioning components, use the individual component installer to uninstall the component.

Remove CA IdentityMinder from WebSphere

After uninstalling CA IdentityMinder software, you can remove the CA IdentityMinder configuration from your application server by using the WebSphere Administrative Console or by executing scripts from the command line.

To remove CA IdentityMinder using the Administrative Console:

Follow these steps:

1. Open the WebSphere Administrative Console using the following URL:

   http://*websphere_server*:9060/admin
2. Select Applications, Enterprise Applications.
3. In the Enterprise Applications screen, select the check box next to CA IdentityMinder and click Stop.
4. Select the check box next to CA IdentityMinder and click Uninstall.
5. If you installed the SiteMinder EAR and SiteMinder Agent EAR, stop these applications, and uninstall them as described previously.
6. Click Save.
7. Click Save to save changes to the master configuration.
8. Remove the ca-stylesr5.1.1.ear file.

   Note: Only remove the ca-stylesr5.1.1.ear if no other CA product is using it.

To remove CA IdentityMinder using the command line:

Follow these steps:

CA IdentityMinder includes two scripts that you can use to remove CA IdentityMinder from the WebSphere application server:

- Uninstall script (uninstallApp.jacl)—Stops the CA IdentityMinder application, then removes it from WebSphere.
- Cleanup script (Ims6Cleanup.jacl) —Removes the CA IdentityMinder resources, such as those created by running the uninstallApp.jacl.

  Note: Running the Cleanup script removes resources that are used by all CA IdentityMinder installations running on the same application server. If you have CA IdentityMinder installations on the same system that you do not want to delete, do not run the Cleanup script. Also, this script does *not* remove any data sources created by CA IdentityMinder.

To remove CA IdentityMinder using the command line, perform the following procedure.

1. From the command line, navigate to *websphere_home*\bin.
2. Be sure that the WebSphere application server is running.
3. Run the Uninstall script as follows:
   - **Windows:** wsadmin -f uninstallApp.jacl
   - **Unix:** ./wsadmin.sh -f uninstallApp.jacl
4. Run the Cleanup script as follows:
   - **Windows:** wsadmin -f Ims6Cleanup.jacl *websphere_node*
   - **Unix:** ./wsadmin.sh -f Ims6Cleanup.jacl *websphere_node*

   where *websphere_node* is the name of the WebSphere node where CA IdentityMinder was installed.
5. Remove the ca-stylesr5.1.1.ear file.

   Note: Only remove the ca-stylesr5.1.1.ear if no other CA product is using it.
6. Remove the service integration bus as follows:
   a. In the WebSphere Administrative Console, go to Service Integration, Buses.
   b. Remove iam_im-IMSBus.
   c. Stop the application server.
   d. Remove the *node_name.server_name*.IMSBus directory under *websphere_home*\profiles*websphere_profile*\databases\com.ibm.ws.sib\

Reinstall CA IdentityMinder

You can reinstall any of the CA IdentityMinder software components by rerunning the installer. When you run the installer, it detects any CA IdentityMinder 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 CA IdentityMinder 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.

Appendix B: Unattended Installation

This section contains the following topics:

How to Run an Unattended Installation

Follow these steps:

1. Modify the im-installer.properties file.
2. Run the following command:
   - **Windows:**
     `ca-im-release-win32.exe -f im-installer.properties -i silent`
   - **UNIX:**
     `./ca-im-release-sol.bin -f im-installer.properties -i silent`

Modify the Configuration File

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

Note the following 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.

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.
DEFAULT_COMPONENTS	Enter one or more components: ■ Server - CA IdentityMinder Server ■ Exten - Extensions to the Policy Server ■ Admin - CA IdentityMinder 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 CA IdentityMinder Server.
DEFAULT_GENERIC_USERNAME	Generic login information for CA IdentityMinder components that are installed.
DEFAULT_GENERIC_PASSWORD	Generic password information for CA IdentityMinder components that are installed.
DEFAULT_FIPS_MODE	Select if you want to enable FIPS 140-2 compliance.
DEFAULT_FIPS_KEY_LOC	Enter the path to the FIPS key location.

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.

CA IdentityMinder Server

If you plan to install the CA IdentityMinder Server, enter values for the following:

Parameter	Instructions
DEFAULT_APP_SERVER	Enter, Weblogic, WebSphere, or JBoss

Parameter	Instructions
DEFAULT_APP_SERVER_URL	Enter full URL of the application server hosting CA IdentityMinder, including the port.
DEFAULT_JAVA_HOME	Path to JRE or JDK for CA IdentityMinder.
Additional Database Parameters	
DEFAULT_DB_HOST	Enter the hostname of the system hosting the CA IdentityMinder database.
DEFAULT_DB_PORT	Enter the port of the system hosting the CA IdentityMinder database.
DEFAULT_DB_NAME	Enter the name of the CA IdentityMinder database.
DEFAULT_DB_USER	Enter the administrative username for the CA IdentityMinder database.
DEFAULT_DB_PASSWORD	Enter the password for the administrative user of the CA IdentityMinder database.
DEFAULT_DB_TYPE	Enter the type of database used for the CA IdentityMinder database.
Additional JBoss Parameter	
DEFAULT_JBOSS_FOLDER	Enter the full pathname of the directory where you installed the JBoss application server. For example, C:\jboss-5.1
Additional WebLogic Parameters	
DEFAULT_BINARY_FOLDER	Enter the full directory path of the directory where you installed WebLogic. For example: C:\Oracle\Middleware\weblogic\
DEFAULT_DOMAIN_FOLDER	Enter the full path and directory name for the WebLogic domain you created for CA IdentityMinder.
DEFAULT_SERVER_NAME	Enter the name of the WebLogic server instance you created for use with CA IdentityMinder.

Parameter	Instructions
DEFAULT_BEA_CLUSTER	Enter the cluster name for the WebLogic cluster.
Additional WebSphere Parameters	
DEFAULT_WEBSPHERE_FOLDER	Enter the full pathname of the directory where you installed CA IdentityMinder 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	Enter the location of the WebSphere profile files.
DEFAULT_WAS_CLUSTER	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.
DEFAULT_PS_USER	Enter the user name of the Policy Server administrator.
DEFAULT_PS_PW	Enter the password of the Policy Server administrator.

Provisioning Components

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_DEPLOYMENT_SIZE	Enter the size of your Provisioning Directory deployment.
DEFAULT_DIRECTORY_IMPS_HOSTNAMES	Enter the hostnames of all Provisioning Servers that will connect to the Directory.
DEFAULT_DOMAIN_NAME	Enter 'im' 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.

Extensions for SiteMinder

To install the extensions for a SiteMinder Policy Server, enter the following:

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.

Configuration File Format

The im-installer.properties file is located in the CA IdentityMinder installation directory. For example:

- **Windows**: C:\Program Files\CA\CA Identity Manager\install_config_info
- **UNIX**: /opt/CA/IdentityManager/install_config_info/im-installer.properties

The following is an example of the im-installer.properties file created during a CA IdentityMinder installation:

```
############################################################
### Silent input properties file for the IM R12.5SP7 installer ###
############################################################

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

# 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\Identity Manager
DEFAULT_INSTALL_FOLDER=

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

#Optionally enable management console security - a default user will be created with
the generic login credentials above.
DEFAULT_SECURE_MANAGEMENT_CONSOLE=

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

 #Select the deployment type that suits your needs (1,2,3 or 4): 1. Compact 2. Basic
3. Intermediate (64 Bit only) 4. Large (64 Bit only)
DEFAULT_DEPLOYMENT_SIZE=
DEFAULT_DIRECTORY_IMPS_HOSTNAMES=
DEFAULT_DOMAIN_NAME=
DEFAULT_DIRECTORY_HOST=
DEFAULT_DIRECTORY_PORT
#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 Identity Manager, Admin Tools,
Provisioning Manager and Provisioning Server
DEFAULT_FIPS_MODE=
#Complete path of the FIPS key file. For e.g. C:\\Program Files\\FIPSkey.dat
DEFAULT_FIPS_KEY_LOC=

#Use custom encryption properties for encrypting sensitive data
DEFAULT_KEY_PARAMS_ENABLED=
#Abs path of the encrpytion properties file. E.g. C:\\Program
Files\\keyParams.properties
DEFAULT_KEY_PARAMS_LOC=


#Identity Manager Application Server information
#   App Server
#   Valid values:  JBoss, WebLogic, WebSphere
DEFAULT_APP_SERVER=
DEFAULT_APP_SERVER_URL=

#Path to JDK for the JBOSS Application Server. No input required for other Application
Servers
DEFAULT_JAVA_HOME=

#JBoss info
DEFAULT_JBOSS_FOLDER=
DEFAULT_JBOSS_PROFILE=
DEFAULT_JBOSS_SERVER_ID=

#Weblogic info
DEFAULT_BINARY_FOLDER=
DEFAULT_DOMAIN_FOLDER=
DEFAULT_SERVER_NAME=
DEFAULT_BEA_CLUSTER=

#WebSphere info
DEFAULT_WEBSPHERE_FOLDER=

#WAS_NODE Value: $WAS_HOME$\installedApps\$WAS_NODE$ or
$WAS_HOME$\config\cells\$WAS_CCELL$\nodes\$WAS_NODE$. These should be same.
DEFAULT_WAS_NODE=

#WAS_SERVER Value:
$WAS_HOME$\config\cells\$WAS_CELL$\nodes\$WAS_NODE$\servers\$WAS_SERVER$
DEFAULT_WAS_SERVER=

#WAS_CELL Value: $WAS_HOME$\config\cells\$WAS_CELL$
DEFAULT_WAS_CELL=
```

```
#WAS_PROFILE Value: $WEBPHERE_HOME$\profiles\$WAS_PROFILE$
WAS_PROFILE=

#WAS_CLUSTER Value: $WAS_HOME$\config\cells\$WAS_CELL$\clusters\$WAS_CLUSTER$
DEFAULT_WAS_CLUSTER=

DEFAULT_WAS_NO_AUTO_DEPLOY=$WAS_NO_AUTO_DEPLOY$

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

#8.1 Migration
# SiteMinder Agent Name
DEFAULT_AGENT_NAME=
# SiteMinder Shared Secret
#DEFAULT_AGENT_PW=<For silent install, insert PS Shared Secret here and uncomment
line.>
# Automatically migrate. Valid values (true/false)
DEFAULT_MIGRATE_DIR_ENV=
# Directory to export to
DEFAULT_DIR_ENV_EXPORT=

#Policy Server Extensions info
#   Location of CsSmPs-<Instance name> folder
DEFAULT_PS_ROOT=
#You can use the SiteMinder Policy Server and a SiteMinder Web Agent to provide advanced
security
# for CA Identity Manager environments. Valid values (true/false)
DEFAULT_USE_SITEMINDER=

#Database Info
DEFAULT_DB_HOST=
DEFAULT_DB_PORT=
DEFAULT_DB_NAME=
DEFAULT_DB_USER=
#DEFAULT_DB_PASSWORD=<For silent install, insert database password here and uncomment
line.>

#Following are permissible values: mssql2005 or oracle10
DEFAULT_DB_TYPE=

#WAS Message Engine Database Info
DEFAULT_ME_HOST=
DEFAULT_ME_PORT=
DEFAULT_ME_NAME=
```

```
DEFAULT_ME_USER=
#DEFAULT_ME_PASSWORD=<For silent install, insert database password here and uncomment
line.>
DEFAULT_ME_SCHEMA=

#Upgrading from IM8.1sp2
#       If you have data stores located on separate servers or you wish to install
them on separate
#       servers, you can specify them below. Otherwise if you wish to have all the
data stores on
#       the same server, change the DEFAULT_DB_* properties from above.

#Object Store Datastore Info
#DEFAULT_OS_DB_HOST=
#DEFAULT_OS_DB_PORT=
#DEFAULT_OS_DB_NAME=
#DEFAULT_OS_DB_USER=
#DEFAULT_OS_DB_PASSWORD=<For silent install, insert database password here and
uncomment line.>

#Task Persistence Datastore Info
#DEFAULT_TP_DB_HOST=
#DEFAULT_TP_DB_PORT=
#DEFAULT_TP_DB_NAME=
#DEFAULT_TP_DB_USER=
#DEFAULT_TP_DB_PASSWORD=<For silent install, insert database password here and
uncomment line.>

#Audit Datastore Info
#DEFAULT_AUDIT_DB_HOST=
#DEFAULT_AUDIT_DB_PORT=
#DEFAULT_AUDIT_DB_NAME=$AUDIT_DB_USER$
#DEFAULT_AUDIT_DB_PASSWORD=<For silent install, insert database password here and
uncomment line.>

#Reporting Snapshot Datastore Info
#DEFAULT_RS_DB_HOST=
#DEFAULT_RS_DB_PORT=
#DEFAULT_RS_DB_NAME=
#DEFAULT_RS_DB_USER=
#DEFAULT_RS_DB_PASSWORD=<For silent install, insert database password here and
uncomment line.>

#Workflow Datastore Info
#DEFAULT_WF_DB_HOST=
#DEFAULT_WF_DB_PORT=
#DEFAULT_WF_DB_NAME=
#DEFAULT_WF_DB_USER=
```

```
#DEFAULT_WF_DB_PASSWORD=<For silent install, insert database password here and
uncomment line.>

# Automatically Upgrade Workflow DB
DEFAULT_UPGRADE_WF_DB=

# Automatically Migrate Task Persistance
DEFAULT_MIGRATE_TP=$

# HTTP Proxy settings
DEFAULT_HTTP_PROXY_ENABLED=
DEFAULT_HTTP_PROXY_HOST=
DEFAULT_HTTP_PROXY_PORT=
DEFAULT_HTTP_PROXY_DOMAIN=
DEFAULT_HTTP_PROXY_USERNAME=
DEFAULT_HTTP_PROXY_PASSWORD=
```

Appendix C: Installation Log Files

The log files are stored based on where you unpack the installation package. The following examples may have different top-level directories than these default locations.

This section contains the following topics:

Log Files on Windows

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

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

The CA IdentityMinder Server installer logs are written to the following default locations:

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

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

Example:

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

Log files on UNIX

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

/opt/CA/IdentityManager/

The CA IdentityMinder Server installer logs are written to the following default location:

/opt/CA/IdentityManager/install_config_info

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

Appendix D: Windows Services Started by CA IdentityMinder

The following are the services started on Windows when you install and start all components of CA IdentityMinder:

- CA Directory *hostname*-impd-co
- CA Directory impd-inc
- CA Directory impd-main
- CA Directory impd-notify
- CA Directory impd-router
- CA IdentityMinder Connector Server (C++)
- CA IdentityMinder Connector Server (Java)
- CA IdentityMinder Provisioning Server
- Enterprise Common Services (Transport)
- Enterprise Common Services GUI Framework
- Enterprise Common Services Store-And-Forward Manager

This list of services may useful to you for troubleshooting purposes.

Index

S

T

U

V

W