

# **CA Identity Manager**

## **Installation Guide (JBoss)**

**r12.5**



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

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

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

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

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

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

The manufacturer of this Documentation is CA.

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

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

## CA Product References

This document references the following CA products:

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

## Contact CA

### Contact Technical Support

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

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

### Provide Feedback

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

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



# Contents

---

|                                                    |               |
|----------------------------------------------------|---------------|
| <b>Chapter 1: Installation Overview</b>            | <b>11</b>     |
| Sample CA Identity Manager Installations .....     | 11            |
| Basic Installation .....                           | 12            |
| Installation with a SiteMinder Policy Server ..... | 14            |
| High Availability Installation .....               | 16            |
| Identity Manager Server Architecture .....         | 16            |
| Provisioning Components Architecture .....         | 17            |
| Installation on UNIX and Console Mode .....        | 18            |
| Overall Installation Process .....                 | 18            |
| Installation Worksheet .....                       | 18            |
| <br><b>Chapter 2: Product Prerequisites</b>        | <br><b>19</b> |
| Installation Status .....                          | 19            |
| Prerequisite Knowledge .....                       | 20            |
| How to Install Prerequisite Components .....       | 20            |
| Install the CA Identity Manager Bookshelf .....    | 20            |
| Meet System Requirements .....                     | 21            |
| Check Hardware Requirements .....                  | 21            |
| Check Software Requirements .....                  | 23            |
| Create a Database .....                            | 24            |
| Check for Cumulative Releases .....                | 24            |
| Create a FIPS 140-2 Encryption Key .....           | 24            |
| (Optional) Configure a Policy Server .....         | 25            |
| JBoss Application Server .....                     | 26            |
| Collect Information for the Installer .....        | 26            |
| JBoss Information .....                            | 26            |
| Provisioning Information .....                     | 27            |
| Provisioning Components Passwords .....            | 28            |
| Database Information .....                         | 28            |
| SiteMinder Information .....                       | 29            |
| <br><b>Chapter 3: Standalone Installation</b>      | <br><b>31</b> |
| Installation Status .....                          | 31            |
| CA Identity Manager Components .....               | 31            |
| How to Perform a Standalone Installation .....     | 32            |
| Install All Components on One System .....         | 32            |

---

|                                                                           |           |
|---------------------------------------------------------------------------|-----------|
| Configure IPv6 Support .....                                              | 34        |
| Verify the Identity Manager Server Starts .....                           | 34        |
| <b>Chapter 4: Distributed Installation</b>                                | <b>35</b> |
| Installation Status .....                                                 | 35        |
| Distributed versus Clustered Installation .....                           | 36        |
| How to Perform a Distributed Installation .....                           | 36        |
| Perform a Distributed Installation .....                                  | 37        |
| Configure IPv6 Support .....                                              | 38        |
| Verify the Identity Manager Server Starts .....                           | 39        |
| Install Additional Components .....                                       | 39        |
| <b>Chapter 5: Installation on a JBoss Cluster</b>                         | <b>41</b> |
| Installation Status .....                                                 | 41        |
| How to Install CA Identity Manager on a JBoss Cluster .....               | 42        |
| Test the Default Multicast Address .....                                  | 42        |
| Create the First Cluster Node .....                                       | 43        |
| Add Cluster Nodes .....                                                   | 47        |
| Configure the JK Connector .....                                          | 48        |
| Start the JBoss Cluster .....                                             | 48        |
| Verify the Clustered Installation .....                                   | 49        |
| <b>Chapter 6: High Availability Provisioning Installation</b>             | <b>51</b> |
| Installation Status .....                                                 | 51        |
| How to Install High Availability Provisioning Components .....            | 52        |
| Install Provisioning Directories .....                                    | 52        |
| Perform Prerequisite Configuration for New Provisioning Directories ..... | 53        |
| Install Alternate Provisioning Directories .....                          | 54        |
| Provisioning Servers .....                                                | 56        |
| Router DSA for the Provisioning Server .....                              | 57        |
| Install Provisioning Servers .....                                        | 57        |
| Configure Provisioning Server Failover .....                              | 59        |
| Provisioning Server Disaster Recovery .....                               | 60        |
| Connector Servers .....                                                   | 60        |
| Connector Server Framework .....                                          | 60        |
| Load-Balancing and Failover .....                                         | 62        |
| Reliability and Scalability .....                                         | 62        |
| Multi-Platform Installations .....                                        | 63        |
| Install Connector Servers .....                                           | 64        |
| Configure Connector Servers .....                                         | 65        |
| C++ Connector Server on Solaris .....                                     | 70        |

---

|                                              |    |
|----------------------------------------------|----|
| Failover for Provisioning Clients .....      | 70 |
| Enable User Console Failover .....           | 71 |
| Enable Provisioning Manager Failover.....    | 72 |
| Test the Provisioning Manager Failover ..... | 72 |

## **Chapter 7: Optional Provisioning Component Installation 73**

|                                               |    |
|-----------------------------------------------|----|
| Installation Status .....                     | 73 |
| Install Optional Provisioning Components..... | 74 |
| Provisioning Manager Setup .....              | 75 |
| Connector Xpress .....                        | 75 |
| Connectors .....                              | 76 |

## **Chapter 8: SiteMinder Protection of CA Identity Manager 77**

|                                                                          |    |
|--------------------------------------------------------------------------|----|
| Installation Status .....                                                | 77 |
| How Resources are Protected .....                                        | 78 |
| How to Protect CA Identity Manager with SiteMinder .....                 | 78 |
| Install the SiteMinder Web Agent .....                                   | 79 |
| Install the Proxy Plug-In .....                                          | 80 |
| Start the Servers for JBoss .....                                        | 81 |
| Verify the Web Agent and Connector .....                                 | 81 |
| Configure the Policy Store for CA Identity Manager.....                  | 82 |
| Configure a Relational Database .....                                    | 82 |
| Configure Sun Java Systems Directory Server or IBM Directory Server..... | 83 |
| Configure Microsoft Active Directory .....                               | 83 |
| Configure Microsoft ADAM .....                                           | 85 |
| Configure CA Directory Server .....                                      | 85 |
| Configure Novell eDirectory Server .....                                 | 87 |
| Configure Oracle Internet Directory (OID) .....                          | 88 |
| Verify the Policy Store .....                                            | 88 |
| SiteMinder High Availability for a JBoss Cluster .....                   | 89 |
| Modify Policy Server Connection Settings .....                           | 89 |
| Add More Policy Servers .....                                            | 90 |
| Select Load Balancing or Fail Over .....                                 | 91 |

## **Chapter 9: Report Server Installation 93**

|                                          |    |
|------------------------------------------|----|
| Installation Status .....                | 93 |
| Reporting Architecture .....             | 94 |
| Reporting Considerations.....            | 95 |
| Hardware Requirements.....               | 95 |
| How to Install the Report Server.....    | 96 |
| Reports Pre-Installation Checklist ..... | 96 |

---

|                                                |     |
|------------------------------------------------|-----|
| Reporting Information .....                    | 97  |
| Install the CA Report Server .....             | 99  |
| Run the Registry Script .....                  | 101 |
| Copy the JDBC JAR Files .....                  | 101 |
| Deploy Default Reports .....                   | 101 |
| Verify the Reporting Installation.....         | 103 |
| How to Uninstall Reporting .....               | 103 |
| Uninstall the Report Server from Windows ..... | 103 |
| Uninstall the Report Server from UNIX.....     | 103 |
| Remove Leftover Items .....                    | 104 |

## **Chapter 10: Uninstallation and Reinstallation** **107**

|                                                                       |     |
|-----------------------------------------------------------------------|-----|
| How to Uninstall CA Identity Manager .....                            | 107 |
| Remove CA Identity Manager Objects with the Management Console .....  | 108 |
| Remove the CA Identity Manager Schema from the Policy Store .....     | 108 |
| Remove the CA Identity Manager schema from a SQL Policy Store .....   | 108 |
| Remove the CA Identity Manager schema from an LDAP Policy Store ..... | 109 |
| Uninstall CA Identity Manager Software Components .....               | 110 |
| Remove CA Identity Manager from JBoss .....                           | 110 |
| Reinstall CA Identity Manager .....                                   | 111 |

## **Appendix A: Unattended Installation** **113**

|                                             |     |
|---------------------------------------------|-----|
| How to Run an Unattended Installation ..... | 113 |
| Modify the Configuration File .....         | 113 |
| Initial Choices .....                       | 114 |
| Identity Manager Server .....               | 115 |
| Provisioning Components .....               | 117 |
| Extensions for SiteMinder.....              | 117 |
| Configuration File Format.....              | 119 |

## **Appendix B: Installation Log Files** **123**

|                            |     |
|----------------------------|-----|
| Log Files on Windows ..... | 123 |
| Log files on UNIX .....    | 124 |

## **Appendix C: Database Creation** **125**

|                                                 |     |
|-------------------------------------------------|-----|
| How to Create a Database Instance .....         | 125 |
| Create an MS SQL Server Database Instance ..... | 126 |
| Create an Oracle Database Instance .....        | 126 |
| Edit the Data Source .....                      | 127 |
| Run the SQL Scripts.....                        | 128 |

---

|                                                                    |            |
|--------------------------------------------------------------------|------------|
| Run the CreateDatabase Script for Workflow .....                   | 129        |
| <b>Appendix D: CA Identity Manager as a Windows Service</b>        | <b>131</b> |
| How to Configure Identity Manager as a Windows Service.....        | 131        |
| Install the Java Service Wrapper Files .....                       | 131        |
| Configure the Java Service Wrapper.....                            | 132        |
| Install the Windows Service .....                                  | 135        |
| Example of a wrapper.conf File .....                               | 136        |
| <b>Appendix E: Windows Services Started by CA Identity Manager</b> | <b>139</b> |
| <b>Appendix F: Installation Worksheet</b>                          | <b>141</b> |
| JBoss Information .....                                            | 141        |
| Provisioning Information .....                                     | 142        |
| Provisioning Components Passwords .....                            | 142        |
| Database Information .....                                         | 143        |
| SiteMinder Information.....                                        | 144        |
| Reporting Information.....                                         | 145        |
| <b>Appendix G: Installation Checklists</b>                         | <b>147</b> |
| How to Install Prerequisite Components .....                       | 147        |
| How to Perform a Standalone Installation .....                     | 147        |
| How to Perform a Distributed Installation .....                    | 148        |
| How to Install CA Identity Manager on a JBoss Cluster .....        | 148        |
| How to Install High Availability Provisioning Components .....     | 149        |
| How to Protect CA Identity Manager with SiteMinder .....           | 149        |
| How to Install the Report Server.....                              | 150        |
| How to Uninstall CA Identity Manager .....                         | 150        |
| <b>Index</b>                                                       | <b>153</b> |



# Chapter 1: Installation Overview

---

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

This section contains the following topics:

[Sample CA Identity Manager Installations](#) (see page 11)

[Basic Installation](#) (see page 12)

[Installation with a SiteMinder Policy Server](#) (see page 14)

[High Availability Installation](#) (see page 16)

[Installation on UNIX and Console Mode](#) (see page 18)

[Overall Installation Process](#) (see page 18)

[Installation Worksheet](#) (see page 18)

## Sample CA Identity Manager Installations

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

## Basic Installation

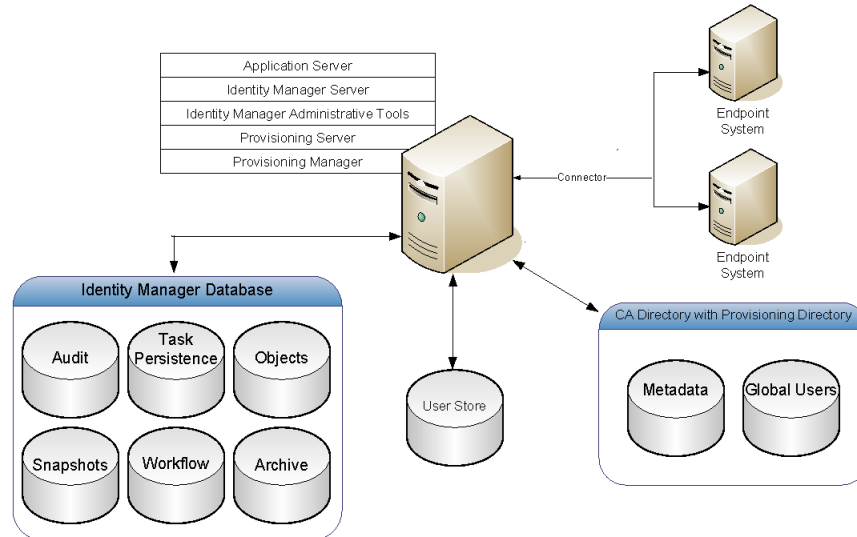
In all CA Identity Manager installations, the Identity Manager Server is installed on an application server. After you install the application server, you use the CA Identity Manager Installer to install the software you need. In a basic installation, all software components are installed on the same system.

Two types of basic installation exist:

- A standalone installation -- all software is on one system, suitable for product demonstration
- A distributed installation -- one copy of each component is installed, but components are on different systems

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

The accounts exist in managed endpoints defined by the account templates. The following figure is an example of a basic CA Identity Manager installation with Provisioning:



### Identity Manager Server

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

### Identity Manager Administrative Tools

Provides tools and samples for configuring and using CA Identity Manager. The tools include configuration files, scripts, utilities, and jar files that you use to compile custom objects with CA Identity Manager 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

### Identity Manager Database

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

**Note:** For a complete list of supported relational databases, see the CA Identity Manager Support Matrix on the [CA Identity Manager support site](#).

### Identity Manager User Store

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

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

### Identity Manager 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.

### Identity Manager Provisioning Directory

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

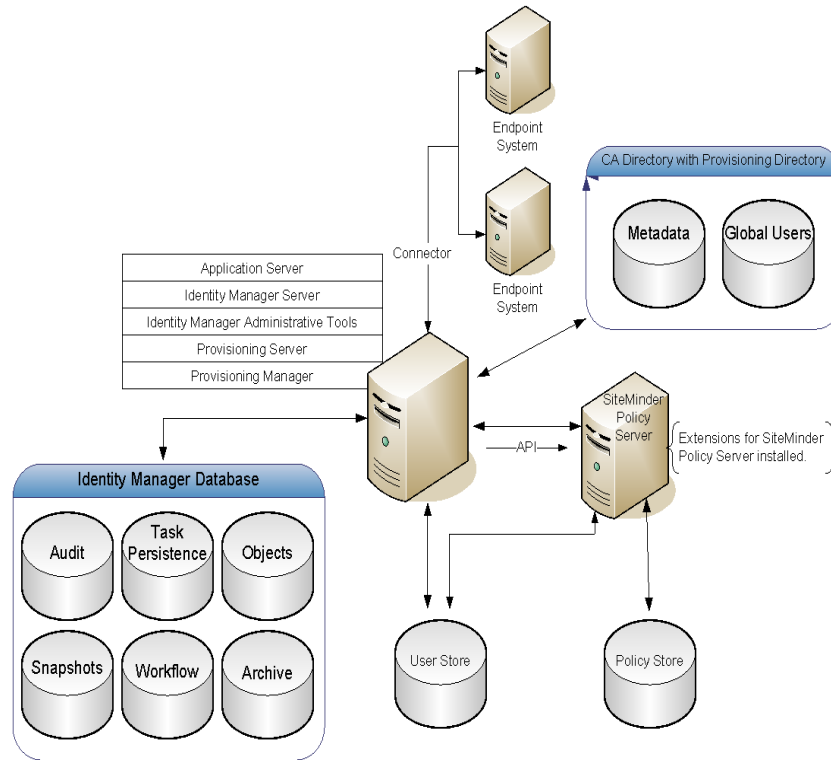
### Identity Manager Provisioning Manager

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 Identity Manager Administrative Tools or can be installed separately from those tools.

**Note:** This application runs on Windows only.

## Installation with a SiteMinder Policy Server

CA Identity Manager can be integrated with a SiteMinder Policy Server, which provides advanced authentication and protection for your Environment. The following figure is an example of a CA Identity Manager installation with a CA SiteMinder Web Access Manager Policy Server:



### Identity Manager Server

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

### Identity Manager Administrative Tools

Provides tools and samples for configuring and using CA Identity Manager. The tools include configuration files, scripts, utilities, and jar files that you use to compile custom objects with CA Identity Manager 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

### Identity Manager Database

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

**Note:** For a complete list of supported relational databases, see the CA Identity Manager Support Matrix on the [CA Identity Manager support site](#).

### Identity Manager User Store

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

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

### SiteMinder Web Agent

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

### SiteMinder Policy Server

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

### Extensions for SiteMinder Policy Server

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

## High Availability Installation

Before installing CA Identity Manager, consider what your goals are. For example, you may want a resilient implementation that consistently provides good performance. You may also want to make the implementation scalable, so you can easily add users and systems over many different network operating systems, security systems, databases, and groupware products.

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

A high-availability implementation addresses the following requirements:

- The Identity Manager Server can be installed on an application server to allow failover to any of the nodes in the cluster, providing uninterrupted access to users.
- The Provisioning Directory uses a CA Directory router to route Provisioning Server directory traffic using the X.500 protocol.
- CA Identity Manager includes the connector servers that can be configured 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.

## Identity Manager Server Architecture

An Identity Manager 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 Identity Manager implementation, a group of several systems may all have an Identity Manager Server installed. These systems share the work that is performed by the Identity Manager Server.

**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 Identity Manager User Console, Identity Manager Management Console and the Provisioning Manager. You can group clients 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, that is, the connection stays active until the server fails. In case of a failure, the client checks 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 may choose to deploy connector servers on systems that are close in the network to the endpoints. For example, if you have many UNIX /etc endpoints, you might have one connector server installed on each of these servers so that each connector server controls only the endpoint on the server where it is installed.

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

- CA Directory Repository tier (Provisioning Directory)

You can use another CA Directory router to send server requests to Provisioning Directories. You can replicate multiple Provisioning Directories for load-balancing, failover, or both.

## Installation on UNIX and Console Mode

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-imr12.5-aix.bin`
- For LINUX, use: `ca-im-imr12.5-linux.bin`

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

- For the main installation, add `-i console`. For example:  
`./ca-im-12.0-sp02-sol.bin -i console`
- For installation of provisioning components, add `-console`.

## Overall Installation Process

To install CA Identity Manager, perform the following steps:

1. Install the prerequisite hardware and software and configure your system as required.
2. Install the CA Identity Manager components on one system or several systems or install the Identity Manager Server on an application server cluster.
3. (Optional) Install alternate Provisioning Directories, alternate Provisioning Servers, and connector servers.
4. (Optional) Install optional provisioning components.
5. (Optional) Protect CA Identity Manager with SiteMinder.
6. (Optional) Install the report server.

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

## Installation Worksheet

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

# Chapter 2: Product Prerequisites

---

This section contains the following topics:

[Installation Status](#) (see page 19)

[Prerequisite Knowledge](#) (see page 20)

[How to Install Prerequisite Components](#) (see page 20)

[Install the CA Identity Manager Bookshelf](#) (see page 20)

[Meet System Requirements](#) (see page 21)

[JBoss Application Server](#) (see page 26)

[Collect Information for the Installer](#) (see page 26)

## Installation Status

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

| You Are Here | Step in Installation Process                                                                                                                            |
|--------------|---------------------------------------------------------------------------------------------------------------------------------------------------------|
| X            | <b>1. Install prerequisite hardware and software and configure your system as required.</b>                                                             |
|              | 2. Perform one of these installations:                                                                                                                  |
|              | ■ Standalone installation                                                                                                                               |
|              | ■ Distributed installation                                                                                                                              |
|              | ■ Installation on an application server cluster                                                                                                         |
|              | 3. (Optional) Install alternate Provisioning Directories, alternate Provisioning Servers, and connector servers to support failover and load balancing. |
|              | 4. (Optional) Install optional provisioning components as needed.                                                                                       |
|              | 5. (Optional) Protect CA Identity Manager with SiteMinder.                                                                                              |
|              | 6. (Optional) Install the report server.                                                                                                                |

## Prerequisite Knowledge

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

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

## How to Install Prerequisite Components

To install the prerequisite hardware and software for CA Identity Manager:

|  Step         |
|------------------------------------------------------------------------------------------------|
| 1. Install the CA Identity Manager bookshelf.                                                  |
| 2. Make your system meet the hardware and software requirements.                               |
| 3. Set up the application server as required.                                                  |
| 4. Record the information you will need to supply during the CA Identity Manager installation. |

## Install the CA Identity Manager Bookshelf

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

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

**To use the Bookshelf**

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

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

## Meet System Requirements

Before installing CA Identity Manager, make sure your systems have the right hardware, software, and configuration required.

### Check Hardware Requirements

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

## Check Software Requirements

Before you install CA Identity Manager, do the following:

1. On the system where you plan to install the Identity Manager Server.

- Install the application server
- Install a supported Java Development Kit (JDK) or Java Runtime Environment (JRE) for CA Identity Manager on the application server system.

If you are installing on a 64-bit operating system, be sure the JDK or JRE is the 64-bit version.

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

2. Install CA Directory so you can use provisioning in CA Identity Manager. A supported version of CA Directory is included on your installation media.

For details on installation of CA Directory, download the documentation from the support site. If support is added for other versions of CA Directory, those versions will be added to the [CA Identity Manager Support Matrix](#).

**Important!** For a production environment, you need at least two copies of CA Directory, one on the system where you plan to install the Provisioning Directory and one on the system where you plan to install the Provisioning Server. The latter is for routing purposes, so that the Provisioning Server can communicate with the remote Provisioning Directory.

3. Install a supported relational database: Microsoft SQL Server or Oracle.

When you run the CA Identity Manager installer, provide the database information when prompted. All database schemas are created automatically when the application server starts.

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

## Create a Database

Create a database for CA Identity Manager. This database is used to store objects and data for auditing, snapshots (reporting), workflow, and task persistence. When you run the CA Identity Manager installer, provide the database information when prompted, and all the database schemas are created automatically. However, you must first create the database. Full details exist in the Database Creation appendix.

## Check for Cumulative Releases

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

### To check for CA Identity Manager Cumulative Releases

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

## Create a FIPS 140-2 Encryption Key

When you run the CA Identity Manager installer, you are given the option of enabling FIPS 140-2 compliance mode. For CA Identity Manager to support FIPS 140-2, all components in a CA Identity Manager 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 and be sure that you safeguard the key file once generated by the Password Tool.

## (Optional) Configure a Policy Server

A SiteMinder Policy Server is an optional component that you install as described in the *SiteMinder Installation Guide*. If you plan to make the policy server highly available, you configure it as a policy server cluster.

### To install a policy server

1. Install the SiteMinder Policy Server. For details, see the *CA SiteMinder Web Access Manager Policy Server Installation Guide*.
2. If you plan 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. Check that you can ping the systems that host the Policy Server from the system where you plan to install the Identity Manager Server.

### To install the Identity Manager Extensions for SiteMinder

Before installing the Identity Manager server, you need to add the extension to each policy server. If the Policy Server is on the system where you plan to install the Identity Manager server, you can install the extensions and the Identity Manager server simultaneously. If so, omit this procedure.

1. Stop the SiteMinder services.
2. Install the Identity Manager Extensions for SiteMinder. Do one of the following:
  - **Windows:** From your installation media, run the following program in the top-level folder:  
`ca-im-r12.5-win32.exe`
  - **UNIX:** From your installation media, run the following program in the top-level folder:  
`ca-im-r12.5-sol.bin`

The CA Identity Manager installer opens.

3. Complete the instructions in the CA Identity Manager installation dialog boxes.

## JBoss Application Server

When using JBoss as the application server, note the following:

- The Identity Manager Server is a J2EE application that is deployed on a supported application server.

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

- The IdentityMinder.ear is deployed in the *jboss\_home/server/default/deploy* folder.
- Install the required version of the JDK before installing the Identity Manager Server. You can download the JDK from Sun's web site at the following URL:  
<http://java.sun.com>
- Be sure to install JBoss in a directory pathname that contains no spaces.
- Once you have completed the verification, shut down the application server to prepare for the CA Identity Manager installation.
- The Application Server connects to the Provisioning Server and other servers by SSL. See the Application Server documentation for information on configuring SSL, including information on certificates and keys.

## Collect Information for the Installer

The CA Identity Manager installation program asks you for information about previously installed software and the software that you are installing. If you are running the CA Identity Manager installer on an IPv6 system, ensure that you provide hostnames (and not IP addresses) in the installer screens.

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

## JBoss Information

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

| Field Name   | Description                                                                                       | Your Response |
|--------------|---------------------------------------------------------------------------------------------------|---------------|
| JBoss Folder | The location of the application server home directory. The path should <i>not</i> contain spaces. |               |

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

## Provisioning Information

### Provisioning Directory Information

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

| Field Name                           | Description                                                                                                                                  | Your Response |
|--------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------|---------------|
| Provisioning Directory Hostname      | The hostname of the Provisioning Directory system.<br><br>You need the hostnames for the primary and any alternate Provisioning Directories. |               |
| Port                                 | The port number of the Provisioning Directory system.                                                                                        |               |
| Provisioning Server Hostname         | The hostname names of each Provisioning Server.<br><br>You need the hostnames for the primary and any alternate Provisioning Servers.        |               |
| Provisioning Directory Shared Secret | The special password for the Provisioning Directory. Use the same password for the primary and any alternate Provisioning Directories.       |               |

## Provisioning Components Passwords

Record the following passwords you need during the Provisioning Server and C++ Server installation.

| Field Name             | Description                                                                                                                                                                                                      | Your Response |
|------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------|
| Provisioning Server    | A password for this Server.                                                                                                                                                                                      |               |
| C++ Connector Server   | A password needed for this server. Each C++ Connector Server can have a unique password.                                                                                                                         |               |
| Provisioning Directory | A password used by Provisioning Server to connect to Provisioning Directory.<br><br>For an alternate Provisioning Server, enter the Provisioning Directory password created for the primary Provisioning Server. |               |

## Database Information

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

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

| Field Name            | Description                                                                                                  | Your Response |
|-----------------------|--------------------------------------------------------------------------------------------------------------|---------------|
|                       | database.                                                                                                    |               |
| Service/Database Name | The database identifier.                                                                                     |               |
| Username              | The username for database access.<br><b>Note:</b> This user must have administrative rights to the database. |               |
| Password              | The password for the user account with administrative rights.                                                |               |

## SiteMinder Information

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

| Field Name                        | Description                                                                                                         | Your Response |
|-----------------------------------|---------------------------------------------------------------------------------------------------------------------|---------------|
| Policy Server Host Name           | The hostname of the SiteMinder Policy Server.                                                                       |               |
| SiteMinder Administrator Name     | The administrator username for the SiteMinder Policy Server.                                                        |               |
| SiteMinder Administrator Password | The administrator user password for the SiteMinder Policy Server.                                                   |               |
| SiteMinder Folder (Solaris Only)  | The location of SiteMinder on the system with a SiteMinder Policy Server installed.                                 |               |
| SiteMinder Agent Name             | The AgentName in the ra.xml file under "IdentityMinder.ear\policyserver.rar\META-INF.<br>Enter it in cipher text.   |               |
| SiteMinder Shared Secret          | The AgentSecret in the ra.xml file under "IdentityMinder.ear\policyserver.rar\META-INF.<br>Enter it in cipher text. |               |



# Chapter 3: Standalone Installation

---

This section contains the following topics:

[Installation Status](#) (see page 31)

[CA Identity Manager Components](#) (see page 31)

[How to Perform a Standalone Installation](#) (see page 32)

## 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            | <b>2. Perform one of these installations:</b> <ul style="list-style-type: none"><li>■ <b>Standalone installation</b></li><li>■ <b>Distributed installation</b></li><li>■ <b>Installation on an application server cluster</b></li></ul> |
|              | 3. (Optional) Install alternate Provisioning Directories, alternate Provisioning Servers, and connector servers to support failover and load balancing.                                                                                 |
|              | 4. (Optional) Install optional provisioning components as needed.                                                                                                                                                                       |
|              | 5. (Optional) Protect CA Identity Manager with SiteMinder.                                                                                                                                                                              |
|              | 6. (Optional) Install the report server.                                                                                                                                                                                                |

## CA Identity Manager Components

The main CA Identity Manager components include the following:

- Identity Manager Server—The server that provides the core functionality of the product.
- Identity Manager Administrative Tools—Tools such as the Provisioning Manager, which provides an additional interface to endpoint systems.

- Identity Manager Provisioning Server—The server that handles all provisioning requests and works with endpoint systems.
- Identity Manager Provisioning Directory—A directory to store provisioning data.
- Extensions for SiteMinder—Extensions required for the SiteMinder Policy Server if you are using it to protect CA Identity Manager. If the Policy Server is on the same system where you are installing CA Identity Manager, you can install CA Identity Manager and the extensions simultaneously. Otherwise, install the extensions before installing CA Identity Manager.

## How to Perform a Standalone Installation

Use the following checklist to perform a standalone installation of CA Identity Manager:

| ✓ | Step                                                            |
|---|-----------------------------------------------------------------|
|   | 1. Install the components of CA Identity Manager on one system. |
|   | 2. Configure support for IPv6 if required.                      |
|   | 3. Verify the Identity Manager Server starts.                   |

### Install All Components on One System

You may decide to install all components of CA Identity Manager on a single system.

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

**To install the main CA Identity Manager components on one system**

1. Make sure that you have the required [information for installer screens](#) (see page 26), such as host names and passwords.
2. Ensure that CA Directory is already installed on the system.
3. Stop the application server.
4. Log in as a Local Administrator (for Windows) or root (for Solaris).
5. Run the CA Identity Manager installer from your installation media's top level folder:

- **Windows:**

ca-im-r12.5-win32.exe

- **UNIX:**

ca-im-r12.5-sol.bin

The CA Identity Manager installer opens.

6. Check all of the following components to install on a single system:
  - Identity Manager Server
    - Connect to SiteMinder Policy Server
  - Identity Manager Administrative Tools

**Note:** Provisioning Manager is only installed on a Windows system.
  - Identity Manager Provisioning Server
  - Identity Manager Provisioning Directory

**Note:** CA Directory must already be installed on the system.
  - Extensions for SiteMinder
7. Complete the instructions in the CA Identity Manager installer dialog boxes.

When installing the Provisioning Directory, you are asked to choose a deployment size. For an installation of all software on one system, choose Compact or Basic:

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

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

If any issues occur during installation, check the [installation logs](#) (see page 123).

## Configure IPv6 Support

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

### To configure IPv6 on a JBoss application server

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

## Verify the Identity Manager Server Starts

To start CA Identity Manager on JBoss, you use the `run_idm.bat` file for Windows, or the `run_idm.sh` file on UNIX. This file is located in the `bin` directory where JBoss is installed.

### To verify that the Identity Manager Server starts

1. To start the Identity Manager Server, do one of the following:
  - **Windows:** Go to Start, Programs, CA, Identity Manager, Start Identity Manager Server.
  - **UNIX:** Enter the following command from the `jboss_home/bin` directory:  
`./run_idm.sh`
2. Access the Management Console and confirm the following:
  - You can access the following URL from a browser:  
`http://im_server:port/idmmanage`  
For example:  
`http://MyServer.MyCompany.com:port-number/idmmanage`
  - The Management Console opens.
  - No errors are displayed in the application server log.
  - You do not receive an error message when you click the Directories link.

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

# Chapter 4: Distributed Installation

---

This section contains the following topics:

[Installation Status](#) (see page 35)

[Distributed versus Clustered Installation](#) (see page 36)

[How to Perform a Distributed Installation](#) (see page 36)

[Install Additional Components](#) (see page 39)

## 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            | <b>2. Perform one of these installations:</b> <ul style="list-style-type: none"><li>■ <b>Standalone installation</b></li><li>■ <b>Distributed installation</b></li><li>■ <b>Installation on an application server cluster</b></li></ul> |
|              | 3. (Optional) Install alternate Provisioning Directories, alternate Provisioning Servers, and connector servers to support failover and load balancing.                                                                                 |
|              | 4. (Optional) Install optional provisioning components as needed.                                                                                                                                                                       |
|              | 5. (Optional) Protect CA Identity Manager with SiteMinder.                                                                                                                                                                              |
|              | 6. (Optional) Install the report server.                                                                                                                                                                                                |

## Distributed versus Clustered Installation

A distributed installation occurs when you install components on different systems. 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 in your distributed installation:

- Identity Manager Server—The server that provides the core functionality of the product.
- Identity Manager Administrative Tools—Install tools such as the Provisioning Manager, which runs on a Windows system.
- Identity Manager Provisioning Server—Enables provisioning in CA Identity Manager.
- Identity Manager Provisioning Directory Initialization—Configures a directory to store provisioning data. Use the installation program on each system where CA Directory is installed.
- Extensions for SiteMinder—Extend the SiteMinder Policy Server if you are using it to protect CA Identity Manager. Install these extensions on the same system as the Policy Server before you install the Identity Manager Server.

## How to Perform a Distributed Installation

Use the following checklist to perform a distributed installation of CA Identity Manager:

| ✓                                                       | Step |
|---------------------------------------------------------|------|
| 1. Install CA Identity Manager on the systems required. |      |
| 2. Configure support for IPv6 if required.              |      |
| 3. Verify that the Identity Manager Server starts.      |      |

## Perform a Distributed Installation

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 Identity Manager 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 Identity Manager 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-r12.5-win32.exe

- **UNIX:**

ca-im-r12.5-sol.bin

For each component that you install, make sure that you have the required [information for installer screens](#) (see page 26), such as host names and passwords. If any issues occur during installation, check the [installation logs](#) (see page 123).

### 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 Identity Manager Server

1. If you have installed SiteMinder on a separate system, ensure that you have installed the extensions for SiteMinder there also.
2. Log into 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 Identity Manager 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. Ensure that CA Directory is already installed on the system.

3. Run the installer and select the Identity Manager 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 (64 bit only)—up to 600,000 accounts
  - Large (64 bit only)—more than 600,000 accounts

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

#### To install the Provisioning Server

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

## Configure IPv6 Support

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

#### To configure IPv6 on a JBoss application server

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

## Verify the Identity Manager Server Starts

To start CA Identity Manager on JBoss, you use the `run_idm.bat` file for Windows, or the `run_idm.sh` file on UNIX. This file is located in the `bin` directory where JBoss is installed.

### To verify that the Identity Manager Server starts

1. To start the Identity Manager Server, do one of the following:
  - **Windows:** Go to Start, Programs, CA, Identity Manager, Start Identity Manager Server.
  - **UNIX:** Enter the following command from the `jboss_home/bin` directory:  
`./run_idm.sh`
2. Access the Management Console and confirm the following:
  - You can access the following URL from a browser:  
`http://im_server:port/idmmanage`  
For example:  
`http://MyServer.MyCompany.com:port-number/idmmanage`
  - The Management Console opens.
  - No errors are displayed in the application server log.
  - You do not receive an error message when you click the Directories link.

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

## Install Additional Components

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

### To install additional components

1. Stop the application server.
2. From your installation media's top-level folder, run the following program:
  - **Windows:**  
`ca-im-r12.5-win32.exe`
  - **UNIX:**  
`ca-im-r12.5-sol.bin`

The CA Identity Manager installer opens.

3. To install one or more of the following components, select it and continue with the installation:

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

**Note:** If a component is already installed, CA Identity Manager reinstalls that component if it is selected. To prevent CA Identity Manager from reinstalling the component, clear it before continuing.

4. Complete the instructions in the CA Identity Manager installation dialog boxes.

# Chapter 5: Installation on a JBoss Cluster

This section contains the following topics:

[Installation Status](#) (see page 41)

[How to Install CA Identity Manager on a JBoss Cluster](#) (see page 42)

[Configure the JK Connector](#) (see page 48)

[Start the JBoss Cluster](#) (see page 48)

[Verify the Clustered Installation](#) (see page 49)

## 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.                                                                                                                                                    |
| <b>X</b>     | <b>2. Perform one of these installations:</b> <ul style="list-style-type: none"><li>■ <b>Standalone installation</b></li><li>■ <b>Distributed installation</b></li><li>■ <b>Installation on an application server cluster</b></li></ul> |
|              | 3. (Optional) Install alternate Provisioning Directories, alternate Provisioning Servers, and connector servers to support failover and load balancing.                                                                                 |
|              | 4. (Optional) Install optional provisioning components as needed.                                                                                                                                                                       |
|              | 5. (Optional) Protect CA Identity Manager with SiteMinder.                                                                                                                                                                              |
|              | 6. (Optional) Install the report server.                                                                                                                                                                                                |

## How to Install CA Identity Manager on a JBoss Cluster

The following procedures describe how to set up multiple JBoss application servers with the same Identity Manager application on each server. In this type of cluster, each JBoss application server acts independently of the other application servers.



### Step

- 
1. [Test the Default Multicast Address](#) (see page 42)
  2. [Create the First Cluster Node](#) (see page 43)
  3. [Add Cluster Nodes](#) (see page 47)
- 

### Test the Default Multicast Address

The run\_idm script uses a multicast address, either the default address or an alternative address supplied by your network administrator.

#### To test the default multicast address

1. Run sender on first node as follows:
  - a. Navigate to jboss-home-1/server/all/lib.
  - b. Run: `java -cp jgroups.jar org.jgroups.tests.McastSenderTest -mcast_addr 224.10.10.10 -port 5555`
2. Run receivers on other nodes in the cluster as follows:
  - a. Navigate to jboss-home-N/server/all/lib.
  - b. Run: `java -cp jgroups.jar org.jgroups.tests.McastReceiverTest -mcast_addr 224.10.10.10 -port 5555`
3. Send a message from the first node as follows:
  - a. On the console of the first node, enter any text and press enter.
  - b. Confirm that a reply appears, to acknowledge the text was sent.
  - c. Confirm that the message appears on the console of all other nodes in the cluster.
  - d. If either the send or receive test fails, ask your network administrator to provide a multicast address that works and repeat this test.

## Create the First Cluster Node

You begin creating the JBoss cluster by creating the first node. On Windows, IPv6 is not supported for a JBoss cluster with the current release of the JDK. Each node must be an IPv4 system or part of an IPv4/IPv6 stack.

This procedure refers to the *admin\_tools*, which represented the location where the Administrative Toolkit is installed. The default location for this toolkit follows:

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

### To create the first cluster node

1. Install the Identity Manager server on one of the systems intended to be part of the cluster.
  - **Windows:** From your installation media, run the following program:  
ca-im-r12.5-win32.exe
  - **UNIX:** From your installation media, run the following program:  
ca-im-r12.5-sol.bin

**Note:** To avoid contention over workpoint.log in *jboss\_home/bin* directory, each node on one system needs a separate *jboss\_home*.
2. Be sure to supply the port number that corresponds to the configuration of JBoss. Ports 1099 and 8080 are used by default. However, if these ports are used by other applications on the system, conflicts occur. For example, Oracle by default starts XDB service on port 8080. Either, JBoss or the other application should be configured to use a different port.

**JBoss Application Server Information**

Please enter information for the application server.

Note: In the Application Server URL field, enter the fully-qualified URL including port number.

JBoss Folder (no spaces):

App Server URL and port:

3. On Windows systems, edit run\_idm.bat in the *jboss\_home\bin* directory:
  - a. Uncomment the cluster-related parts of run\_idm.bat.

- b. If the [multicast address test](#) (see page 42) failed, add a multicast address preceded by the -u argument.

The format with a *multicast-address* follows:

```
set ARGS=
set SERVER=default/deploy
:loop
if [%1] == [] goto endloop
set ARGS=%ARGS% %1
if [%1] == [-c] set SERVER=%2/farm
shift
goto loop
:endloop
ARGS=%ARGS% -g IdmPartition -u multicast-address
```

4. If you are installing on a system that supports IPv6/IPv4, modify the following property in the JAVA\_OPTS entry:

```
set IDM_OPTS=%IDM_OPTS% -Djava.net.preferIPv4Stack=true
```

5. For Solaris systems, edit `run_idm.sh` in the `jboss_home\bin` directory:
  - a. Uncomment cluster-related parts of `run_idm.sh`.
  - b. If the [multicast address test](#) (see page 42) failed, add a multicast address preceded by the `-u` argument.

The format for that line appears at the end of this section:

```
SERVER=default/deploy
ARGS=
    until [-z "$1"]
    do
        ARGS="${ARGS} $1"
        if [ $1 = '-c' ]
        then
            SERVER=$2/farm
        fi
        shift
    done
ARGS="${ARGS} -g IdmPartition -u multicast-address"
```

- c. If you are installing on a system that supports IPv6, modify *one* of the following properties in the `JAVA_OPTS` entry:
    - For IPv6 only systems, uncomment the following entry:  
`IDM_OPTS="$IDM_OPTS -Djava.net.preferIPv6Addresses=true"`
    - For IPv6/IPv4 systems, uncomment the following entry:  
`IDM_OPTS="$IDM_OPTS -Djava.net.preferIPv4Stack=true"`
6. Copy the following files of `jboss_home\server\default\deploy` to `jboss_home\server\all\farm`:
  - `imworkflowdb-ds.xml`
  - `reportsnapshot-ds.xml`
  - `imauditdb-ds.xml`
  - `imarchivedb-ds.xml`
  - `imtaskpersistencedb-ds.xml`
  - `objectstore-ds.xml`
  - `castylesr5.1.1.ear`
  - `IdentityMinder.ear`
7. Copy `login-config.xml` from `jboss_home\server\default\conf` to `jboss_home\server\all\conf`.
8. Copy the following files from `jboss_home\server\default\lib` to `jboss_home\server\all\lib`:
  - `sqljdbc.jar` (If MS-SQL is the object store)
  - `ojdbc14.jar` (If Oracle is the object store)

9. Set up JMS connection factory, topics and queues definitions as follows:

- a. Copy  
`admin_tools\samples\Cluster\JBoss\deploy-hasingleton\jms\workflow-service.xml` to `jboss_home\server\all\deploy-hasingleton\jms`.
- b. Remove  
`jboss_home\server\all\farm\IdentityMinder.ear\META-INF\workflow-service.xml`.
- c. Locate the `jbossmq-destinations-service.xml` in  
`jboss_home\server\all\deploy-hasingleton\jms`.
- d. Add JMS topic and queue definitions to this file by copying in the content of the file:

`jboss_home\server\all\farm\IdentityMinder.ear\META-INF\jbossmq-destinations-service.xml`

**Important!** Copy the content only in between the server tags.

- e. Remove these files:

`jboss_home\server\all\farm\IdentityMinder.ear\META-INF\jbossmq-destinations-service.xml`.

`jboss_home\server\all\farm\IdentityMinder.ear\identityminder_ejb.jar\META-INF\jbossmq-destinations-service.xml`

10. Copy `admin_tools\samples\Cluster\JBoss\IdentityMinder.ear` over  
`jboss_home\server\all\farm\IdentityMinder.ear`

11. If Workflow Designer is installed, copy  
`admin_tools\samples\Cluster\JBoss\IdentityMinder.ear\config\workpoint-client.properties` to `<CA ROOT>\IAM Suite\Identity Manager\tools\Workpoint\conf`.

12. Make these changes for HTTP load balancing with sticky sessions:

- Modify  
`jboss_home\server\all\deploy\jboss-web.deployer\META-INF\jboss-service.xml` by changing the `UseJK` attribute to `true`.
- Modify `jboss_home\server\all\deploy\jboss-web.deployer\server.xml` by adding a tag in this format:  
`jvmRoute="worker1"` to `<Engine ...>`

**Important!** If you are installing a JBoss cluster on an IPv6/IPv4 stack, modify the sample files on each system and replace `jnp://localhost` with `jnp://host-name` used in `run_idm.bat` or `run_idm.sh`. Modify all `jboss.xml` files.

If any issues occur during installation, check the [installation logs](#) (see page 123).

## Add Cluster Nodes

### To add cluster nodes

If you need to run additional nodes of JBoss on the same system, modify the port assignments of JBoss based on the vendor instructions. You will need to modify the JNDI names in the procedure to create the first cluster node, so that it uses the correct port number.

Also, modify files from step 6 in the procedure to create the first cluster node; include the changed port number for this node.

The location of the new JBoss node is *jboss\_home\_n*. It may or may not reside on the same system as the first node of the cluster.

1. Copy the following files from *jboss\_home\bin* to the additional cluster node location: *jboss\_home\_n\bin*:
  - `workpoint_client.policy`
  - `run_idm.bat`  
Remember to change the *host-name* used by the `-b` argument to the name of the system where you copy this file.
  - `run_idm.ico`
2. Copy the following files from *jboss\_home\server\all\deploy-hasingleton\jms\* to *jboss\_home\_n\server\all\deploy-hasingleton\jms\*:
  - `jbossmq-destinations-service.xml`
  - `workflow-service.xml`
3. For HTTP load balancing with sticky sessions:
  - Modify *jboss\_home\_n/server/all/deploy/jboss-web.deployer/META-INF/jboss-service.xml* to set the `UseJK` attribute to `true`.
  - Modify `%JBOSS_HOME_N%\server\all\deploy\jboss-web.deployer\server.xml`, by adding this tag:  
`jvmRoute="workerN"` to `<Engine ...>`
4. Copy `login-config.xml` from *jboss\_home\server\default\conf* to *jboss\_home\_n\server\all\conf*.
5. Copy the following files from *jboss\_home\server\default\lib* to *jboss\_home\_n\server\all\lib*:
  - `sqljdbc.jar` (MS-SQL)
  - `ojdbc14.jar` (Oracle)

6. Copy the following files of `jboss_home\server\all\farm` to `%JBOSS_HOME_N%\server\all\farm`:
  - `castylesr5.1.1.ear`
  - `IdentityMinder.ear`
7. To create a data source for a relational database User Store, place the data source file under `all/farm` on one cluster node.

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

**Important!** If you are installing a JBoss cluster on an IPv6/IPv4 stack, modify the sample files on each system and replace `jnp://localhost` with `jnp://host-name` used in `run_idm.bat` or `run_idm.sh`. Modify all `jboss.xml` files.

## Configure the JK Connector

### To configure the JK connector

1. Install a JK connector based on these instructions:  
[http://tomcat.apache.org/connectors-doc/generic\\_howto/quick.html](http://tomcat.apache.org/connectors-doc/generic_howto/quick.html)  
**Note:** If you installed SiteMinder, choose one that corresponds to the Web Server on which you installed the SiteMinder Web Agent that will protect Identity Manager resources.
2. Configure JK load balancing as follows:
  - a. Locate `ConnectorConfiguration` in the sample directory appropriate for your Web Server/operation system.
  - b. Use property files in `samples\Cluster\JBoss\ConnectorConfiguration` instead of the files shipped with the `ConnectionConfiguration` sample.

## Start the JBoss Cluster

Once all configuration is complete, start all servers in the correct order.

### To start the servers for JBoss

1. Start one of the SiteMinder Policy Servers that supports Identity Manager.  
**Note:** If you have a Policy Server cluster, only one Policy Server should be running while you create Identity Manager directories, create or modify Identity Manager environments, or change WorkPoint settings.
2. From a command line, navigate to:  
`jboss_home/bin`

3. Enter the following:
  - For Windows:  
`run_idm.bat -c all`
  - For UNIX:  
`./run_idm.sh -c all`
4. If you have already 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 using an application server cluster, check that the installation was successful.

### To verify the clustered installation

1. Start the Identity Manager Management Console as follows:

`http://host_name:port/idmmanage`

#### **host\_name**

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

#### **port**

Defines the application server port.

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



# Chapter 6: 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](#) (see page 51)

[How to Install High Availability Provisioning Components](#) (see page 52)

[Install Provisioning Directories](#) (see page 52)

[Provisioning Servers](#) (see page 56)

[Connector Servers](#) (see page 60)

[Failover for Provisioning Clients](#) (see page 70)

## 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: <ul style="list-style-type: none"><li>■ Standalone installation</li><li>■ Distributed installation</li><li>■ Installation on an application server cluster</li></ul> |
| <b>X</b>     | <b>3. (Optional) Install alternate Provisioning Directories, alternate Provisioning Servers, and connector servers to support failover and load balancing.</b>                                              |
|              | 4. (Optional) Install optional provisioning components as needed.                                                                                                                                           |
|              | 5. (Optional) Protect CA Identity Manager with SiteMinder.                                                                                                                                                  |
|              | 6. (Optional) Install the report server.                                                                                                                                                                    |

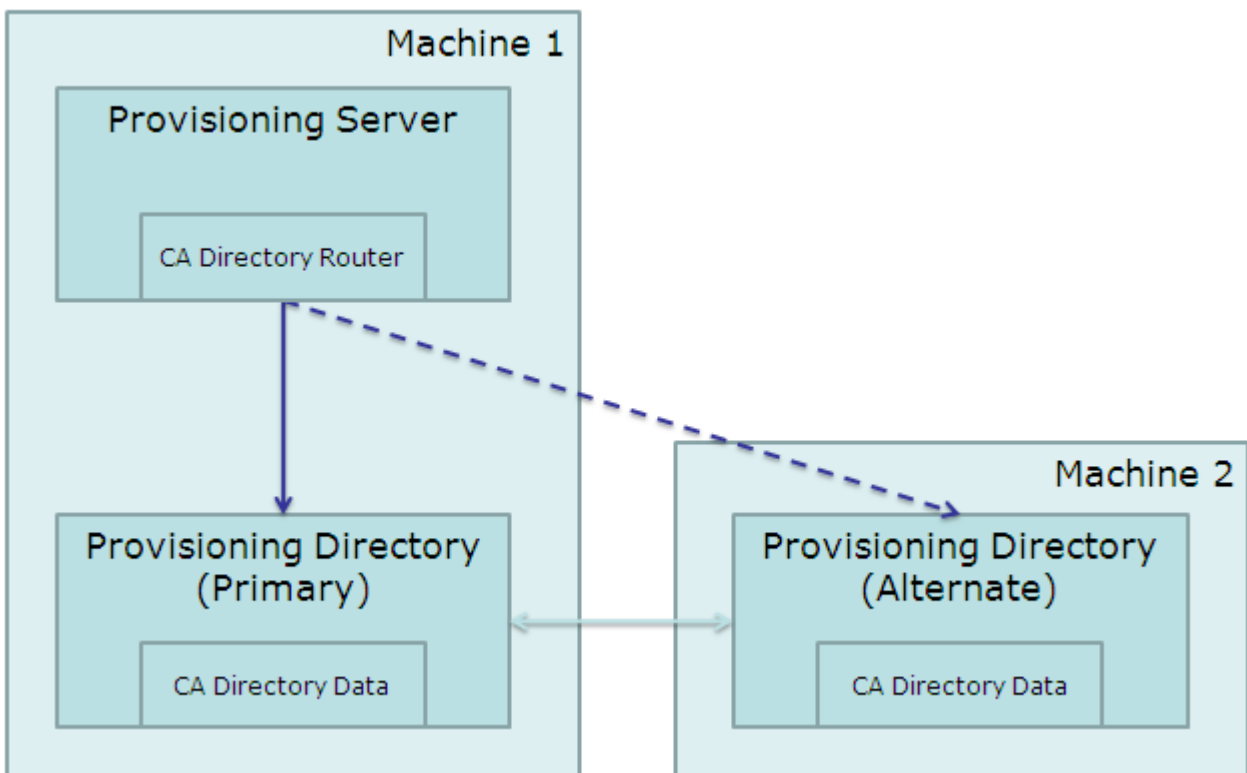
## How to Install High Availability Provisioning Components

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.                                                          |

### Install Provisioning Directories

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



You install alternate Provisioning Directories if they were not configured during the installation.

### To install Provisioning Directories

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*

If you have already installed a primary Provisioning Directory during the installation, you can omit step 1.

2. Perform the [prerequisite configuration](#) (see page 53) for the new Provisioning Directories.
3. [Install one or more alternate Provisioning Directories](#) (see page 54).

## Perform Prerequisite Configuration for New Provisioning Directories

You use the High Availability Configuration command before you use the Provisioning Directory installation program.

### To Perform Prerequisite Configuration for New Provisioning Directories

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 unpacked the install package. For example:

*Unpacked-Install-Package\Provisioning\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 the prompts to provide the hostnames required for each alternate Provisioning Directory that you want to add.

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

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

## Install Alternate Provisioning Directories

Once you have performed the [prerequisite configuration](#) (see page 53) required, you can install alternate Provisioning Directories.

### To install alternate Provisioning Directories

1. Log as a Local Administrator (for Windows) or root (for Solaris) into the system where you plan to install the alternate Provisioning Directory.
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.dxc. If the custom schema files are not copied locally, data replication between the Provisioning Directories will fail.

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.

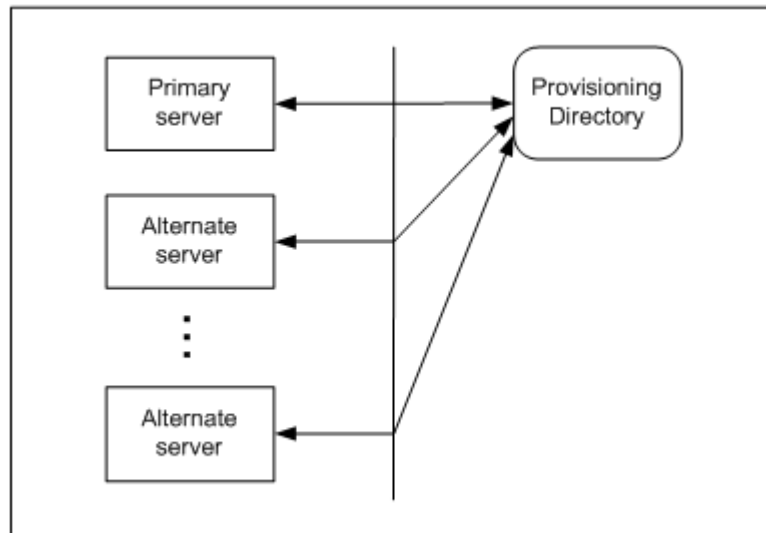
If you are upgrading from a previous release, you may have a significant amount of data to replicate. You should deselect the checkbox if you do not want replication to start at this time. After the installation, you would then need to copy an LDIF data dump or online backup files from an existing Provisioning 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 other alternate Provisioning Directories have a record that replication occurred. If the alternate Provisioning Directory is successfully reinstalled, that data is not replicated again. To avoid this problem, 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.

## 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 goes through a 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, 20392 (for address, SNMP, console and SSLD 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 Servers that can connect to it.

## Install Provisioning Servers

To support failover, you can install primary and alternate Provisioning Servers. If you have already installed a Provisioning Server, you can omit step 1.

### To install Provisioning Servers

1. Install the primary Provisioning Server using the Provisioning Server 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. [Perform prerequisite configuration](#) (see page 58) for the new Provisioning Servers.
3. [Install](#) (see page 59) one or more alternate Provisioning Servers.
4. Enter the alternate Provisioning Server host and port number when you enable provisioning in the Identity Manager Management Console. For details, see the *Configuration Guide*.

## Perform Prerequisite Configuration for New Provisioning Servers

To configure knowledge files, you use the High Availability Configuration command on each system with a Provisioning Directory.

### To Perform Prerequisite Configuration for New Provisioning Servers

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 unpacked the install package. For example:

```
Unpacked-Install-Package\Provisioning\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 into each system that will host a Provisioning Directory and repeat steps 2 through 4.

## Install Alternate Provisioning Servers

Once you have performed the [prerequisite configuration](#) (see page 58) required, you can install one or more Provisioning Servers.

### To install alternate Provisioning Servers

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.dxc. 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.

## Configure Provisioning Server Failover

For CA Identity Manager 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 Identity Manager directory for your environment. During initialization, CA Identity Manager 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*.

## Provisioning Server Disaster Recovery

To protect against failure of the primary Provisioning Server, you can configure an alternate Provisioning Server. The difference between primary and alternate Provisioning Servers is that the primary server installation populates the Provisioning Directory container entries, default provisioning directory entries, and bootstrapping provisioning administrator entries. Also, uninstalling a primary server removes those entries. Apart from installation and uninstallation, the primary and alternate servers function in the same manner.

To protect a Provisioning Server from disaster, you can reconfigure a primary server as an alternate server. As a result, uninstalling a primary server does not remove Provisioning Directory entries that alternate servers depend on. To convert a primary server to an alternate server or an alternate server to a primary server, use the Identity Manager Provisioning Server installation program.

## 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.

## 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.

## 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 Windows/Solaris; connector Server installed by default respectively on the same Windows/Solaris system.
  - Multiple additional Connector Server instances installed on Windows/Solaris systems, serving as end-point 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.

## Install Connector Servers

Based on the guidelines in this chapter, you make connector servers highly available by installing several instances of Java Connector Servers or C++ Connector Servers, or both.

### To install the Java Connector Server

If you plan to install more than one Java Connector Servers, see the *Java Connector Server Implementation Guide* for additional guidelines. For a single Java Connector Server, follow these steps:

1. Run the following program where you unpacked the install package.

- **Windows:**

*Unpacked-Install-Package\Provisioning\Connector Server\setup.exe*

- **UNIX:**

*Unpacked-Install-Package/Provisioning/ConnectorServer/setup*

2. Complete the instructions in the installer dialog boxes.

### To install the C++ Connector Server

1. Run the following program where you unpacked the install package.

- **Windows:**

*Unpacked-Install-Package\Provisioning\Provisioning Server\setup.exe*

- **UNIX:**

*Unpacked-Install-Package/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](#) (see page 57) applies.

## 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

The C++ Connector Server installed on Solaris can manage only Solaris UNIX ETC and ACC endpoints. For all other Connectors, install the C++ Connector Server on a Windows system and register it with the Provisioning Server installed on Solaris. During installation, specify that this Connector Server is your default C++ Connector Server.

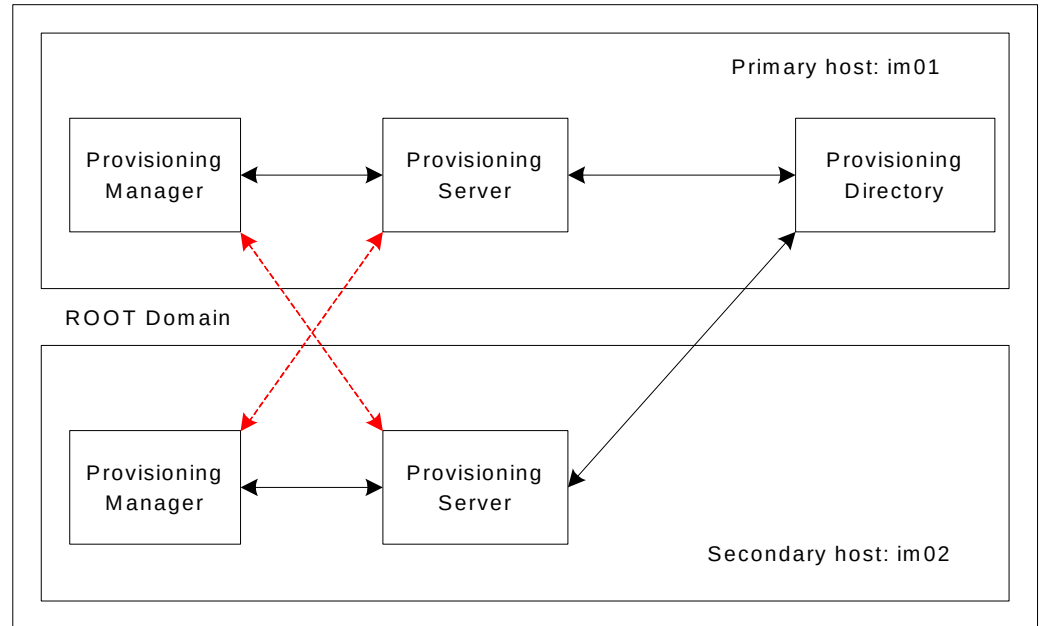
## Failover for Provisioning Clients

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 Identity Manager Server fails, it does not receive Provisioning Server updates. As a result, the Identity Manager User Console does not show provisioning changes. Therefore, you should configure an alternate URL for the Identity Manager Server.

### To enable the client-tier failover for the User Console

1. Launch the Provisioning Manager.
2. Click System, Identity Manager 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.

### To enable the Provisioning Manager failover

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. 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:

### To test Provisioning Manager failover

1. Stop the CA Identity Manager - 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 Identity Manager - Provisioning Server service locally, the traffic flows to the failover domain server. If it does not, check your configuration and try the test again.

# Chapter 7: Optional Provisioning Component Installation

---

This section contains the following topics:

[Installation Status](#) (see page 73)

[Install Optional Provisioning Components](#) (see page 74)

[Provisioning Manager Setup](#) (see page 75)

[Connector Xpress](#) (see page 75)

[Connectors](#) (see page 76)

## 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: <ul style="list-style-type: none"><li>■ Standalone installation</li><li>■ Distributed installation</li><li>■ Installation on an application server cluster</li></ul> |
|              | 3. (Optional) Install alternate Provisioning Directories, alternate Provisioning Servers, and connector servers to support failover and load balancing.                                                     |
| <b>X</b>     | <b>4. (Optional) Install optional provisioning components as needed.</b>                                                                                                                                    |
|              | 5. (Optional) Protect CA Identity Manager with SiteMinder.                                                                                                                                                  |
|              | 6. (Optional) Install the report server.                                                                                                                                                                    |

## Install Optional Provisioning Components

Optional Provisioning Components for CA Identity Manager are in the im-pc-r12.5.zip and include the following:

### **SPML Manager**

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

### **SPML Service**

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

### **Remote Agents**

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

### **Password Sync Agents**

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

### **GINA**

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

### **Vista Credential Provider**

Run the Vista 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.

### **JCS SDK**

Run the JCS SDK installer from the CA Identity Manager 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.

More information exists for these components in the following guides:

- Credential Provider (*Administration Guide*)
- GINA Option for Password Reset/Unlock (*Administration Guide*)

- Password Synchronization Agent (*Administration Guide*)
- Connector Xpress (*Connector Xpress Guide*)
- SPML Service (*Provisioning Reference Guide*)
- Agents for use with connectors (*Connectors Guide*)

## Provisioning Manager Setup

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

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

### To run the Provisioning Manager setup

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

**Note:** You must use the hostname. Entering a localhost for an IP address does not work.

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

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

## Connector Xpress

To create your own connectors, you use Connector Xpress to create connectors without expertise required to use a programming interface.

Connector Xpress is a CA Identity Manager utility for managing dynamic connectors, mapping dynamic connectors to endpoints, and establishing routing rules for endpoints. You can use it to configure dynamic connectors to allow provisioning and management of SQL databases and LDAP directories.

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

## Connectors

The Identity Manager installer installs all connectors by default. However, in some cases, you must 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*.

# Chapter 8: SiteMinder Protection of CA Identity Manager

---

This section contains the following topics:

[Installation Status](#) (see page 77)

[How Resources are Protected](#) (see page 78)

[How to Protect CA Identity Manager with SiteMinder](#) (see page 78)

[Install the SiteMinder Web Agent](#) (see page 79)

[Install the Proxy Plug-In](#) (see page 80)

[Start the Servers for JBoss](#) (see page 81)

[Verify the Web Agent and Connector](#) (see page 81)

[Configure the Policy Store for CA Identity Manager](#) (see page 82)

[SiteMinder High Availability for a JBoss Cluster](#) (see page 89)

## 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: <ul style="list-style-type: none"><li>■ Standalone installation</li><li>■ Distributed installation</li><li>■ Installation on an application server cluster</li></ul> |
|              | 3. (Optional) Install alternate Provisioning Directories, alternate Provisioning Servers, and connector servers to support failover and load balancing.                                                     |
|              | 4. (Optional) Install optional provisioning components as needed.                                                                                                                                           |
| <b>X</b>     | <b>5. (Optional) Protect CA Identity Manager with SiteMinder.</b>                                                                                                                                           |
|              | 6. (Optional) Install the report server.                                                                                                                                                                    |

## How Resources are Protected

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

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

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

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

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

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

## How to Protect CA Identity Manager with SiteMinder

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

|  <b>Step</b>               |
|---------------------------------------------------------------------------------------------------------------|
| 1. Be sure you have installed the Identity Manager Extensions for SiteMinder on the SiteMinder Policy Server. |
| 2. Install and configure a SiteMinder Web Agent to protect CA Identity Manager resources.                     |
| 3. Install the plug-in the Web Server uses to forward requests to the application server.                     |
| 4. Verify that the plug-in is successfully forwarding requests to the application server.                     |
| 5. Configure the SiteMinder Policy Store for use with CA Identity Manager.                                    |

**Step**

6. Configure SiteMinder high availability for CA Identity Manager.

## Install the SiteMinder Web Agent

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

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

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

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

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

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

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

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

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

To verify the Web Agent, confirm the following:

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

## Install the Proxy Plug-In

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

To forward these requests, install and configure a JK Connector on the system where the SiteMinder Web Agent installed. See the following Jakarta Project web site for more information about the JK Connector:

<http://tomcat.apache.org/tomcat-4.1-doc/config/jk.html>

The Identity Manager Administrative Tools include sample configuration files that you can use to configure the JK Connector. See the readme.txt file in the directory where the sample configuration files are located for instructions.

The following table describes the location of these files:

| Platform                               | Location                                                                                                             |
|----------------------------------------|----------------------------------------------------------------------------------------------------------------------|
| IIS Web server on a Windows system     | C:\Program Files\CA\Identity Manager\IAM Suite\Identity Manager\samples\ConnectorConfiguration\windows\IIS_JBoss     |
| iPlanet Web server on a Solaris system | C:\Program Files\CA\Identity Manager\IAM Suite\Identity Manager\samples\ConnectorConfiguration\solaris\Iplanet_JBoss |

| Platform                              | Location                                                                                                            |
|---------------------------------------|---------------------------------------------------------------------------------------------------------------------|
| Apache Web server on a Solaris system | C:\Program Files\CA\Identity Manager\IAM Suite\Identity Manager\samples\ConnectorConfiguration\solaris\Apache_JBoss |

## Start the Servers for JBoss

Once all configuration is complete, start all servers in the correct order.

### To start the servers for JBoss

1. Start one of the SiteMinder Policy Servers that supports CA Identity Manager.  
**Note:** If you have a Policy Server cluster, only one Policy Server should be running while you create Identity Manager directories, create or modify Identity Manager environments, or change WorkPoint settings.
2. From a command line, navigate to:  
`jboss_home/bin`
3. Enter the following:
  - For Windows:  
`run_idm.bat -c all`
  - For UNIX:  
`./run_idm.sh -c all`
4. Start the Web Server where you installed the SiteMinder Web Agent and the application server proxy plug-in.

## Verify the Web Agent and Connector

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

In a browser, enter the following URL:

`http://web_server/idm/ui/ping.jsp`

For example:

`http://MyServer.MyCompany.com/idm/ui/ping.jsp`

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

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

```
SM_AUTHTYPE = Not Protected
SM_DOMAIN = domain
SMTRANSACTIONID = system-generated_id
```

For example:

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

## Configure the Policy Store for CA Identity Manager

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

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

## Configure a Relational Database

### To configure a relational database policy store

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

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

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

- **SQL:** C:\Program Files\CA\Identity Manager\IAM Suite\Identity Manager\tools\policystore-schemas\MicrosoftSQLServer\ims8\_mssql\_ps.sql
- **Oracle:**  
/opt/CA/IdentityManager/IAM\_Suite/Identity\_Manager/tools/policystore-schemas/OracleRDBMS/ims8\_oracle\_ps.sql

The preceding are default installation locations. The location for your installation may be different.

## Configure Sun Java Systems Directory Server or IBM Directory Server

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

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

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

2. Add the appropriate LDIF schema file from the following table to the directory. The default Windows location for the LDIF files is C:\Program Files\CA\Identity Manager\IAM Suite\Identity Manager\tools\policystore-schemas.

Adding the following schema files for your directory:

- **IBM Directory Server:**

IBMDirectoryServer\V3.identityminder8

- **Sun Java Systems Directory Server (iPlanet):**

SunJavaSystemDirectoryServer\sundirectory\_ims8.ldif

## Configure Microsoft Active Directory

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

### To configure an Active Directory policy store

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

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

2. Modify the activedirectory\_ims8.ldif schema file as follows:

- a. In a text editor, open the activedirectory\_ims8.ldif file. The default Windows location is:

C:\Program Files\CA\Identity Manager\IAM Suite\Identity Manager\tools\polycystore-schemas\MicrosoftActiveDirectory

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

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

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

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

## Configure Microsoft ADAM

To configure a Microsoft ADAM policy store, you apply the adam\_ims8.ldif script.

### To configure a Microsoft ADAM policy store

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

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

2. Modify the adam\_ims8.ldif schema file as follows:

- a. In a text editor, open the adam\_ims8.ldif\ldif file. The default Windows location is:

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

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

For example, if the guid string is

CN={39BC711D-7F27-4311-B6C0-68FDEE2917B8}, then replace every

cn={guid} reference with

CN={39BC711D-7F27-4311-B6C0-68FDEE2917B8}.

- c. Save the file.

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

## Configure CA Directory Server

### To configure a CA Directory policy store

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

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

2. Copy etrust\_ims8.dxc to *dxserver\_home*\config\schema

where *dxserver\_home* is the directory where CA Directory is installed. The default source location for this file on Windows is C:\Program Files\CA\Identity Manager\IAM Suite\Identity Manager\tools\policystore-schemas\eTrustDirectory.

3. Create a custom schema configuration file as follows:
  - a. Copy the `dxserver_home\config\schema\default.dxc` to `dxserver_home\config\schema\company_name-schema.dxc`.
  - b. Edit the `dxserver_home\config\schema\company_name-schema.dxc` file by adding the following lines to the bottom of the file:

```
# Identity Manager Schema
source "etrust_ims8.dxc";
```
4. Edit the `dxserver_home\bin\schema.txt` file by adding the contents of `etrust_ims_schema.txt` to the end of the file. The default source location for this file on Windows is `C:\Program Files\CA\Identity Manager\IAM Suite\Identity Manager\tools\policystore-schemas\etrustDirectory`.
5. Create a custom limits configuration file as follows:
  - a. Copy the `dxserver_home\config\limits\default.dxc` to `dxserver_home\config\limits\company_name-limits.dxc`.
  - b. Increase the default size limit to 5000 in the `dxserver_home\config\limits\company_name-limits.dxc` file as follows:

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

**Note:** If you upgrade CA Directory, the `limits.dxc` file is overwritten, therefore you must reset `max-op-size` to 5000 after the upgrade is completed.
6. Edit the `dxserver_home\config\servers\dsa_name.dxi` as follows:

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

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

where `dsa_name` is the name of the DSA using the customized configuration files.
7. Run the `dxsyntax` command.

This utility reports any errors with the directory configuration. If this utility runs with no errors, continue to Step 8.
8. Stop and restart the DSA as the `dsa` user to make the schema changes take effect, as follows:

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

## Configure Novell eDirectory Server

To configure an Novell eDirectory Server policy store, you apply the novell\_ims8.ldif script.

### To configure an Novell eDirectory policy store

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

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

2. Find the DN of the NCPServer for your Novell eDirectory Server by entering the following information in a command window on the system where the Policy Server is installed:

```
ldapsearch -h hostname -p port -b container -s sub  
-D admin_login -w password objectClass=ncpServer dn
```

For example:

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

3. Open the novell\_ims8.ldif file.
4. Replace every NCPServer variable with the value you found in Step 2.

The default location for novell\_ims8.ldif on Windows is:

C:\Program Files\CA\Identity Manager\IAM Suite\Identity  
Manager\tools\policystore-schemas\NovelleDirectory

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

5. Update the eDirectory Server with the novell\_ims8.ldif file.  
See the Novell eDirectory documentation for instructions.

## Configure Oracle Internet Directory (OID)

### To configure an Oracle Internet Directory policy store

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

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

2. Update the Oracle Internet Directory Server with the oracleoid\_ims8.ldif file. The default installation location for this file on Windows is:

C:\Program Files\CA\Identity Manager\IAM Suite\Identity Manager\polycystore-schemas\OracleOID\

See the Oracle Internet Directory documentation for instructions.

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

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

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

The LdapPolicy key is located in:

HKEY\_LOCAL\_MACHINE\SOFTWARE\Netegrity\SiteMinder\CurrentVersion\Ds\

## Verify the Policy Store

To verify the policy store, confirm the following:

- Your Policy Server log does not contain a section of warnings that begins with the following:

\*\*\* IMS NO SCHEMA BEGIN

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

This warning appears only if you have installed the Extensions for the SiteMinder Policy Server, but you have not extended the Policy Store schema.

- The CA Identity Manager objects exist in the policy store database or directory. The CA Identity Manager objects begin with an ims prefix.

## SiteMinder High Availability for a JBoss Cluster

If you have created a SiteMinder Policy Server cluster, you can configure a JBoss cluster to use it for load balancing and failover.

### To configure SiteMinder high availability for a JBoss cluster

1. Edit the ra.xml file in this location:  
*jboss\_home/server/default/IdentityMinder.ear/policyserver\_rar/META-INF*
2. Modify these items, which are explained in the sections that follow:
  - Connection settings for the Policy Server
  - The number of Policy Servers
  - The selection of load balancing or failover for the cluster.
3. Repeat these steps for each Identity Manager server in the cluster.
4. Restart the JBoss server for changes to take effect.

### Modify Policy Server Connection Settings

The Policy Server connection information should reflect the primary server for the production environment. This information consists of the ConnectionURL, the user name and password for the SiteMinder Admin account, and the name and shared secret for the Agent.

In the following example, the values to edit appear in CAPITAL LETTERS.

```
<config-property>
    <config-property-name>ConnectionURL</config-property-name>
    <config-property-type>java.lang.String</config-property-type>
    <config-property-value>DEVELOPMENT.SEVERCOMPANY.COM,VALUE,VALUE,VALUE</config-
        property-value>
</config-property>

<config-property>
    <config-property-name>UserName</config-property-name>
    <config-property-type>java.lang.String</config-property-type>
    <config-property-value>SITEMINDER-ADMIN-NAME</config-property-
        value>
</config-property>

<config-property>
    <config-property-name>AdminSecret</config-property-name>
    <config-property-type>java.lang.String</config-property-type>
    <config-property-value>ENCRYPTED-PASSWORD</config-
        property-value>
</config-property>
```

```
<config-property>
  <config-property-name>AgentName</config-property-name>
  <config-property-type>java.lang.String</config-property-type>
  <config-property-value>DEVELOPMENT-AGENT-NAME</config-property-
    value>
</config-property>

<config-property>
  <config-property-name>AgentSecret</config-property-name>
  <config-property-type>java.lang.String</config-property-type>
  <config-property-value>ENCRYPTED-AGENT-SECRET</config-
    property-value>
</config-property>
```

**Note:** For the values that require encrypted text, use the Identity Manager password tool. For more information, see the *Configuration Guide*.

## Add More Policy Servers

To add more Policy Servers to the CA Identity Manager installation instance, edit the FailoverServers entry in the ra.xml file.

**Note:** Include the primary Policy Server and all failover servers in the FailoverServers entry.

For each Policy Server, enter an IP address followed by port numbers for authentication, authorization, and accounting services. Use a semi-colon to separate entries as shown here:

```
<config-property>
  <config-property-name>FailoverServers</config-property-name>
  <config-property-type>java.lang.String</config-property-type>
  <config-property-value>
    172.123.123.123,44441,44442,44443;172.123.123.124,33331,
    33332,33333
  </config-property-value>
</config-property>
```

## Select Load Balancing or Fail Over

The default behavior of CA Identity Manager is to use round-robin load balancing using the servers identified by the ConnectionURL and FailoverServers. Load balancing occurs if you leave FailOver set to false.

To select failover, set FailOver to true:

```
<config-property>
  <config-property-name>FailOver</config-property-name>
  <config-property-type>java.lang.String</config-property-type>
  <config-property-value>true</config-property-value>
</config-property>
```



# Chapter 9: Report Server Installation

---

This section contains the following topics:

[Installation Status](#) (see page 93)

[Reporting Architecture](#) (see page 94)

[Reporting Considerations](#) (see page 95)

[Hardware Requirements](#) (see page 95)

[How to Install the Report Server](#) (see page 96)

[How to Uninstall Reporting](#) (see page 103)

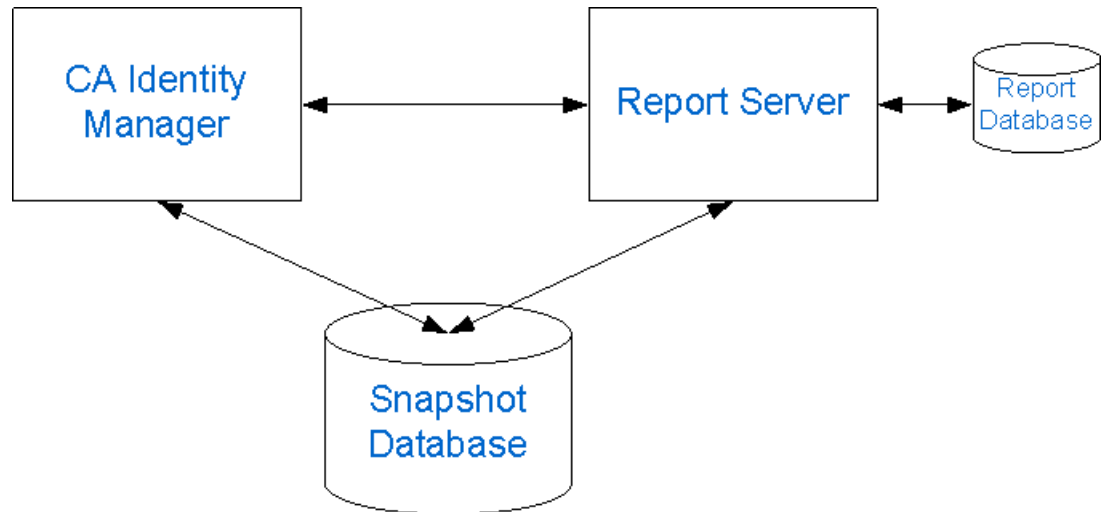
## Installation Status

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: <ul style="list-style-type: none"><li>■ Standalone installation</li><li>■ Distributed installation</li><li>■ Installation on an application server cluster</li></ul> |
|              | 3. (Optional) Install alternate Provisioning Directories, alternate Provisioning Servers, and connector servers to support failover and load balancing.                                                     |
|              | 4. (Optional) Install optional provisioning components as needed.                                                                                                                                           |
|              | 5. (Optional) Protect CA Identity Manager with SiteMinder.                                                                                                                                                  |
| <b>X</b>     | <b>6. (Optional) Install the report server.</b>                                                                                                                                                             |

## Reporting Architecture

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



**Note:** The Snapshot Database in the previous graphic could also be the Audit Database or Workflow Database.

### Report Server

Also known as CA Business Intelligence. This is the engine behind the generation of reports for CA Identity Manager. It communicates directly with CA Identity Manager and the Snapshot Database.

### Report Database

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

### CA Identity Manager

CA Identity Manager allows you to export CA Identity Manager object data to the Report Database.

### Snapshot Database

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

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

## 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 machine to which you are installing the Report Server, port conflicts may occur. If you experience port conflicts after installing the Report 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 following requirements must be met for the Report Server to install and run correctly in the following environments:

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

**Windows**

- Processor: P3, 700 MHz
- Physical Memory: 2 GB is recommended
- Disk Space: 9 GB for Business Objects and 1.5 GB for Performance Management
- Drives: CDRom

### Solaris 8, 9

- Processor: SPARC v8plus
- Physical Memory: 2 GB is recommended
- Disk Space: 9 GB for Business Objects

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

## How to Install the Report Server

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

|  Step |
|----------------------------------------------------------------------------------------|
| 1. Review the report pre-installation checklist.                                       |
| 2. Gather reporting information.                                                       |
| 3. Install the Report Server (CA Business Intelligence)                                |
| 4. Run the Registry Script.                                                            |
| 5. Copy the JDBC JAR files.                                                            |
| 6. Run the command line to deploy the default reports.                                 |

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

## Reports Pre-Installation Checklist

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

- Be sure that the Windows or UNIX system to which you are installing the report server meets the minimum system requirements.
- Be sure that you are using a supported version of MS SQL Server or Oracle database for the Report Database.

- Create a database instance to be used as the Report Database.
  - If you are using MS SQL Server, create a data source name (DSN) that the report server uses to communicate with the Report Database.
  - If you are using Oracle, create a transparent network substrate (TNS) that the report server uses to communicate with the Report Database.
- If you create a new database instance for the Snapshot Database, run the following scripts on the new database:
  - MS SQL: C:\Program Files\CA\Identity Manager\IAM Suite\Identity Manager\tools\imreexport\db\sqlserver\ims\_mssql\_report.sql
  - Oracle: C:\Program Files\CA\Identity Manager\IAM Suite\Identity Manager\tools\imreexport\db\oracle\ims\_oracle\_report.sql
- (UNIX) Set the following parameters:
  - ORACLE\_HOME: the path to the Oracle root directory.
  - LD\_LIBRARY\_PATH: \$ORACLE\_HOME/lib32:\$ORACLE\_HOME/lib
  - 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/j2sdk1.4.2\_08
  - PATH:  
\$LD\_LIBRARY\_PATH:\$JAVA\_HOME:\$JAVA\_HOME/bin:\$ORACLE\_HOME/bin:\$PATH
  - LC\_ALL: en\_US.UTF-8
- (UNIX) Be sure that you have access to a non-root user account. You cannot use a root account to install the report server.

## 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 into the Business Objects Infoview console.                           |               |
| DSN Name               | Identify the name of the DSN that the Report Server uses to communicate with the Report Database. |               |
| TNS Name               | The name of the TNS that the Report Server uses to                                                |               |

| Field Name                       | Description                                                                                                                                                                                                                                                                                                                     | Your Response |
|----------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------|
|                                  | communicate with the Report Database.<br><b>Note:</b> This information is needed only if you are using Oracle.                                                                                                                                                                                                                  |               |
| Database Name                    | Identify the Report Database name.<br><b>Note:</b> This information is needed only if you are using MS SQL.                                                                                                                                                                                                                     |               |
| User Name                        | Identify the username for the Report Database.                                                                                                                                                                                                                                                                                  |               |
| Password                         | Identify the administrative password credentials for the Report Database.                                                                                                                                                                                                                                                       |               |
| 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.<br><b>Note:</b> If you are installing the Report Server on the same system as the CA Identity Manager, ensure that the Tomcat connection port does not conflict with the port number you specified for the application server URL when installing the CA Identity Manager. |               |

**Note:** Oracle and MS SQL are supported for the Report Database.

## 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, as well as a UNIX console.

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

The Report Server is powered by Business Objects Enterprise XI.

**Note:** CA Identity Manager supports the latest version of Business Objects XI. For more information on upgrading the Report Server, see the *Upgrade Guide*.

### Run the Windows Installer

Install the Report Server using the Windows installation wizard (ca-iamreportserver-12.5-win32.exe) found on the Report Server media.

**Note:** The Report Server is available for download on the [CA Support site](#), under CA Identity Manager product downloads.

#### To install the Report Server

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 Custom install during installation. This lets you select either Oracle or MS SQL as your Report Database.
  - If you are installing the Report Server on the same system as CA Identity Manager, ensure that the Tomcat connection port does not conflict with the port number you specified for the application server URL when installing CA Identity Manager.
5. Review the installation settings and click Install.  
The Report Server is installed.

## Run the UNIX Installer

Install the Report Server using the UNIX installation wizard (ca-iamreportserver-12.5-sol.bin) found on the Report Server media.

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

```
chmod+x ca-iamreportserver-12.5-sol.bin
```

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

### To install the Report Server

1. Exit all applications.
2. Download the Report Server and untar it.
3. **Note:** The Report Server is available for download on the [CA Support site](#), under CA Identity Manager product downloads.
4. Open a command window and navigate to where the install program is located.
5. Enter the following command:

```
sh./ca-iamreportserver-12.5-sol.bin
```

The installation wizard starts.

6. Use the gathered reporting information to install the report server.

Choosing a Typical install installs Tomcat and use MySQL as the Report Database by default. A Custom install will allow you to select another type of database for your Report Database.

Note the following:

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

## Run the Registry Script

In order for CA Identity Manager to dynamically change data sources for reports in the Report Server, run the mergeConnection.reg script. The default Windows location for this script is: C:\Program Files\CA\Identity Manager\IAM Suite\Identity Manager\tools\ReportServerTools.

## Copy the JDBC JAR Files

### To copy the jdbc JAR files

1. Navigate to the C:\Program Files\CA\Identity Manager\IAM Suite\Identity Manager\lib\jdbcdrivers folder on the CA Identity Manager media.
2. Copy one of the following JAR files to *report\_server\_home/common/3.5/java/lib*:
  - **SQL:** sqljdbc.jar
  - **Oracle:** ojdbc14.jar
3. In *report\_server\_home/common/3.5/java*, open the CRConfig.xml file.
4. Add the location of the jdbc JAR files to the Classpath. For example, if you are using an MS SQL database, your Classpath would look like the following:  

```
<Classpath>C:\report_server_home\common\3.5\java\lib\sqljdbc.jar;...</Classpath>
```
5. Save the file.
6. Restart the Report Server as follows:
  - a. Go to Start, Program Files, CA, Report Server, Central Configuration Manager.  
The Central Configuration Manager opens.
  - b. Select all services and click Restart.

## Deploy Default Reports

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

### To deploy the default reports

1. Unzip the importbiarfilestool.zip file on the machine where the Report Server is installed. This default Windows location for this tools is:  
C:\Program Files\CA\Identity Manager\IAM Suite\Identity Manager\tools\BIARTool

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

2. Be sure that the JAVA\_HOME variable is set correctly, and that you have JDK1.5 installed.

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

importMBIARFiles.bat

Provide the following information needed to import the default reports:

- Report Server Root Folder—location of the business objects install folder, for example, E:\Program Files\CA\SC\CommonReporting\BusinessObjects Enterprise 11.5
- Reporting Database Type—1=MSSQL, 2=Oracle  
**Note:** This is the database that the Report Server (CA Business Intelligence) uses to store its own data.
- Reporting Database User—user created for the Report Database
- Reporting Database Password—password for the user created in Report Database
- Reporting Database DSN Name—the ODBC DSN name created
- Reporting Database Name—the Report Database name
- Reporting Server Administrator Name—The default is Administrator. If you have a different administrator name, provide it here.
- Reporting System Password—reporting administrator's password entered during the installation
- BIAR File Location—provide the correct location. The default installation location on Windows is:
  - C:\Program Files\CA\Identity Manager\IAM Suite\Identity Manager\tools\imexport\ReportDefinitions\IM Standard Reports\Ms-SQL\_Reports\ms-sql\_reports.biar
  - C:\Program Files\CA\Identity Manager\IAM Suite\Identity Manager\tools\imexport\ReportDefinitions\IM Standard Reports\Oracle Reports\oracle\_reports.biar

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

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

## Verify the Reporting Installation

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

- In the Central Configuration Manager, ensure that all services are running.
- Be sure that your Report Database is running.

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

## How to Uninstall Reporting

Complete the following procedures to uninstall the Report Server:

1. Uninstall the Report Server.
2. Remove leftover items.

### Uninstall the Report Server from Windows

You uninstall the Report Server when it is no longer required on the system.

#### To uninstall the Report Server

1. Click Start, Settings, Control Panel.  
The Control Panel opens.
2. Double-click Add/Remove Programs.  
A list of currently installed programs appears.
3. Select Report Server, and click Change/Remove  
A wizard to uninstall the Report Server starts.
4. Follow the instructions and prompts in the wizard.  
**Note:** If the system displays a remove shared file message, click No to All.
5. If requested, reboot the system.  
The Report Server is uninstalled.

### Uninstall the Report Server from UNIX

You uninstall the Report Server when it is no longer necessary on the system.

#### To uninstall the Report Server on UNIX

1. Navigate to the Report Server home directory in a console window.

2. Run the following command:

```
./iam-report-server-uninstall.sh
```

The uninstallation program appears.

3. Press Enter.

A status indicator shows the Report Server is being uninstalled and prompts successful completion.

## Remove Leftover Items

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

### Remove Windows Items

#### **To remove leftover Report Server items after removing a Report Server from a Windows system**

1. Navigate to *report\_server\_home*\IAM Report Server.

##### ***report\_server\_home***

Specifies the Report Server installation path.

2. Open the BusinessObjects Enterprise 11.5 folder, and delete the following folders:
  - Data
  - Developer\_Help
  - java
  - Logging
  - Samples
  - Web Content
  - Web Services
  - win32x86
3. Return to the Report Server folder.
4. Open the common folder.

5. Open the 3.5 folder, and delete the following folders:
  - crystalreportviewers115
  - java
6. Return to the Report Server folder, and delete the following folders:
  - log
  - OLAP Intelligence 11.5
  - stylesheets

You have completed removing leftover items.

## Remove UNIX Items

### **To remove leftover Report Server items after uninstalling a Report Server from a UNIX system**

1. Navigate to the following location from a command prompt:  
/opt/CA/SharedComponents
2. Delete the following folders:
  - CommonReporting
  - iamreportserver

You have completed removing leftover items.



# Chapter 10: Uninstallation and Reinstallation

---

This section contains the following topics:

[How to Uninstall CA Identity Manager](#) (see page 107)

[Remove CA Identity Manager Objects with the Management Console](#) (see page 108)

[Remove the CA Identity Manager Schema from the Policy Store](#) (see page 108)

[Uninstall CA Identity Manager Software Components](#) (see page 110)

[Remove CA Identity Manager from JBoss](#) (see page 110)

[Reinstall CA Identity Manager](#) (see page 111)

## How to Uninstall CA Identity Manager

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

The following checklist describes the steps to uninstall CA Identity Manager:

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

## Remove CA Identity Manager Objects with the Management Console

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

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

## Remove the CA Identity Manager Schema from the Policy Store

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

### Remove the CA Identity Manager schema from a SQL Policy Store

On systems where you installed the CA Identity Manager Extensions for SiteMinder, remove the CA Identity Manager 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\polycystore-schemas\mssql\ims8_mssql_ps_delete.sql`
- Oracle:  
`/opt/CA/IdentityManager/IAM_Suite/Identity_Manager/tools/polycystore-schemas/oracle/ims8_oracle_ps_delete.sql`

## Remove the CA Identity Manager 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.

### To remove the CA Identity Manager schema from an LDAP policy store

1. Complete one of the following:

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

**Note:** There are no other steps required to remove the schema from an IBM Directory Server. Continue with Uninstall CA Identity Manager 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 Identity Manager 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               | <code>novell\novell-delete-ims8.ldif</code>                                       |
| Oracle Internet Directory (OID) | <code>oracle-internet-directory\oracle-internet-directory-delete-ims8.ldif</code> |

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

## Uninstall CA Identity Manager Software Components

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

### To uninstall CA Identity Manager software components on Windows

1. Install a 32-bit JRE or JDK, which is required for the uninstallation program to run.
2. Go to Start, Control Panel, Add/Remove Programs and select CA Identity Manager.
3. Select CA Identity Manager.
4. Click Change/Remove.

All non-provisioning components will be uninstalled.

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

### To uninstall CA Identity Manager software components on UNIX

1. Navigate to the following location:  
`/opt/CA/Identity_Manager/install_config_info/im-uninstall/uninstall`
2. Run the following script:  

```
sh im-uninstall.sh
```

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

## Remove CA Identity Manager from JBoss

After you uninstall CA Identity Manager, there are no additional steps required in the JBoss application server.

To remove the JBoss application server, delete the directory where you installed JBoss.

## Reinstall CA Identity Manager

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

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



# Appendix A: Unattended Installation

---

This section contains the following topics:

[How to Run an Unattended Installation](#) (see page 113)

[Modify the Configuration File](#) (see page 113)

[Configuration File Format](#) (see page 119)

## How to Run an Unattended Installation

### To run the installer in the unattended installation mode

1. Modify the im-installer.properties file.
2. Run the following command:
  - **Windows:**  
`ca-im-12.0-sp02-win32.exe -f im-installer.properties -i silent`
  - **UNIX:**  
`./ca-im-12.0-sp02-sol.bin -f im-installer.properties -i silent`

## Modify the Configuration File

To enable an unattended CA Identity Manager 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 Identity Manager 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_DISPATCH_NAME | Enter 'New Installation' if this is a fresh install. For upgrades, this will be blank.                                                                                                                                                                                                                                                                                                                    |
| DEFAULT_COMPONENTS                 | <p>Enter one or more components:</p> <ul style="list-style-type: none"> <li>■ Server - Identity Manager Server</li> <li>■ Exten - Extensions to the Policy Server</li> <li>■ Admin - Identity Manager Administrative Tools</li> <li>■ Provision - Provisioning Server</li> <li>■ Directory - Provisioning Directory</li> </ul> <p>To install more than one component, separate components by a comma.</p> |
| DEFAULT_INSTALL_FOLDER             | Enter the directory in which to install the Identity Manager Server.                                                                                                                                                                                                                                                                                                                                      |
| DEFAULT_GENERIC_USERNAME           | Generic login information for CA Identity Manager components that are installed.                                                                                                                                                                                                                                                                                                                          |
| DEFAULT_GENERIC_PASSWORD           | Generic password information for CA Identity Manager 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.

## Identity Manager Server

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

| Parameter                             | Instructions                                                                                                              |
|---------------------------------------|---------------------------------------------------------------------------------------------------------------------------|
| DEFAULT_APP_SERVER                    | Enter, Weblogic, WebSphere, or JBoss                                                                                      |
| DEFAULT_APP_SERVER_URL                | Enter full URL of the application server hosting CA Identity Manager, including the port.                                 |
| DEFAULT_JAVA_HOME                     | Path to JRE or JDK for CA Identity Manager.                                                                               |
| <b>Additional Database Parameters</b> |                                                                                                                           |
| DEFAULT_DB_HOST                       | Enter the hostname of the system hosting the CA Identity Manager database.                                                |
| DEFAULT_DB_PORT                       | Enter the port of the system hosting the CA Identity Manager database.                                                    |
| DEFAULT_DB_NAME                       | Enter the name of the CA Identity Manager database.                                                                       |
| DEFAULT_DB_USER                       | Enter the administrative username for the CA Identity Manager database.                                                   |
| DEFAULT_DB_PASSWORD                   | Enter the password for the administrative user of the CA Identity Manager database.                                       |
| DEFAULT_DB_TYPE                       | Enter the type of database used for the CA Identity Manager database.                                                     |
| <b>Additional JBoss Parameter</b>     |                                                                                                                           |
| DEFAULT_JBOSS_FOLDER                  | Enter the full pathname of the directory where you installed the JBoss application server.<br>For example, C:\jboss-4.2.3 |
| <b>Additional WebLogic Parameters</b> |                                                                                                                           |
| DEFAULT_BINARY_FOLDER                 | Enter the full directory path of the directory where you installed WebLogic. For example: C:\bea\weblogic92\              |

| Parameter             | Instructions                                                                                        |
|-----------------------|-----------------------------------------------------------------------------------------------------|
| DEFAULT_DOMAIN_FOLDER | Enter the full path and directory name for the WebLogic domain you created for CA Identity Manager. |
| DEFAULT_SERVER_NAME   | Enter the name of the WebLogic server instance you created for use with CA Identity Manager.        |
| 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 Identity Manager Tools for WebSphere. |
| DEFAULT_WAS_NODE         | Enter the name of the node in which the application server is located.                                |
| DEFAULT_WAS_SERVER       | Enter the name of the system on which the application server is running.                              |
| DEFAULT_WAS_CELL         | Enter the name of the cell in which the application server is located.                                |
| WAS_PROFILE              | (WebSphere 6) Enter the location of the WebSphere profile files.                                      |
| DEFAULT_WAS_CLUSTER      | (WebSphere 6) Enter the cluster name for the WebSphere cluster.                                       |

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

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

| Parameter     | Instruction                                            |
|---------------|--------------------------------------------------------|
|               | 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. |

| Parameter              | Instruction                                                                    |
|------------------------|--------------------------------------------------------------------------------|
| 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 Identity Manager installation directory, for example, C:\Program Files\CA\CA Identity Manager\install\_config\_info\.

The following is an example of the im-installer.properties file created during a CA Identity Manager installation:

```
#####
### Silent input properties file for the IMR12.5 installer ##
#####

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

# 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
DEFAULT_INSTALL_FOLDER=

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

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

#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=

#Identity Manager Application Server information
# App Server
# Valid values: JBoss, Weblogic9, WebLogic10, WebSphere6
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=

#Weblogic info
DEFAULT_BINARY_FOLDER=
DEFAULT_DOMAIN_FOLDER=
DEFAULT_SERVER_NAME=

#For Weblogic 9 & 10 only:
DEFAULT_BEA_CLUSTER=

#WebSphere info
DEFAULT_WEBSPHERE_FOLDER=

#WAS_NODE Value: $WAS_HOME$\installedApps\$WAS_NODE$ or
$WAS_HOME$\config\cells\$WAS_CELL$\nodes\$WAS_NODE$. 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: $WEBSPHERE_HOME$\profiles\$WAS_PROFILE$
WAS_PROFILE=

#WAS_CLUSTER Value: $WAS_HOME$\config\cells\$WAS_CELL$\clusters\$WAS_CLUSTER$
DEFAULT_WAS_CLUSTER=

#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=
# 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=

#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=
#DEFAULT_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 Persistence
```

```
DEFAULT_MIGRATE_TP=
```

# Appendix B: 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](#) (see page 123)

[Log files on UNIX](#) (see page 124)

## Log Files on Windows

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

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

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

C:\Program Files\CA\Identity Manager\install\_config\_info

On a 64-bit windows system, the default location is:

C:\Program Files (x86)\CA\Identity Manager\install\_config\_info

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

### **Example:**

C:\Documents and Settings\user\Local Settings\Temp\imps\_server\_install.log

## Log files on UNIX

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

`/opt/CA/IdentityManager/`

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

`/opt/CA/IdentityManager/install_config_info`

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

# Appendix C: Database Creation

---

This section contains the following topics:

- [How to Create a Database Instance](#) (see page 125)
- [Create an MS SQL Server Database Instance](#) (see page 126)
- [Create an Oracle Database Instance](#) (see page 126)
- [Edit the Data Source](#) (see page 127)
- [Run the SQL Scripts](#) (see page 128)

## How to Create a Database Instance

CA Identity Manager requires a relational database to store objects and data for auditing, snapshots (reporting), workflow, and task persistence. When installing CA Identity Manager, all of the database schemas are created automatically when the application server is started.

Also, for scalability purposes, you may want to create a separate database to replace any one of the existing database schemas initially created by CA Identity Manager during installation.

You can create a new database instance for the following:

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

Perform the following steps to create a new database.

1. Create a new MS SQL Server or Oracle database instance for CA Identity Manager.
2. Edit the data source.
3. (Optional) Run the SQL scripts.

**Important!** The Windows default locations for CA Identity Manager database schema files are the following:

- Workflow: [run the CreateDatabase script](#) (see page 129)
- 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\imexport\tools\db
- Archive (task persistence archive): C:\Program Files\CA\Identity Manager\IAM Suite\Identity Manager\tools\db

## Create an MS SQL Server Database Instance

### To create an MS SQL Server Database Instance

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

**Note:** The user must have at least select, insert, update, and delete permissions for all of the tables created by the .sql script for creating the database, and must be able to execute all of the stored procedures (if applicable) defined in these scripts.

For example, the user must have these permissions on the tables defined in 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 or Windows on the Security tab of the SQL Server Properties dialog for the server where the database is installed.

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

## Create an Oracle Database Instance

### To create an Oracle Database Instance

1. Create a new tablespace.
2. Create a new user.

3. Grant the 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.

## Edit the Data Source

### To edit the data source

1. In a text editor, open the appropriate data source descriptor located in the *jboss\_home/server/default/deploy* directory. Choose from the following:
  - Task Persistence: `imtaskpersistencedb-ds.xml`
  - Workflow: `imworkflowdb-ds.xml`
  - Auditing: `imauditdb-ds.xml`
  - Object Store: `objectstore-ds.xml`
  - Snapshots: `reportsnapshot-ds.xml`
  - Archive: `imarchivedb-ds.xml`
2. Change the `JndiName` in the data source descriptor according to the following:
  - Task Persistence: `jdbc/idm`
  - Workflow: `jdbc/WPDS`

- Auditing: auditDbDataSource
  - Object Store: jdbc/objectstore
  - Snapshots: jdbc/reportsnapshot
  - Archive: jdbc/archive
3. Change the DatabaseName, User, and Password in the data source descriptor to the appropriate values for the new database.

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

## Run the SQL Scripts

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

These scripts are installed with the Identity Manager Administrative Tools.

### To run the SQL scripts

1. Do one of the following:
  - MS SQL Server: Open the Query Analyzer tool and select the script you need.
  - Oracle: Open the SQL prompt for the script you need.
2. Select one of the following scripts (shown with the default Windows locations) depending on what the database was created for:
  - Task Persistence:
    - MS SQL: C:\Program Files\CA\Identity Manager\IAM Suite\Identity Manager\tools\db\taskpersistence\sqlserver\idm\_db\_sqlserver.sql
    - Oracle: C:\Program Files\CA\Identity Manager\IAM Suite\Identity Manager\tools\db\taskpersistence\oracle9i\idm\_db\_oracle.sql
  - Workflow: Run the CreateDatabase script outlined in the next section.
  - Auditing:
    - MS SQL: C:\Program Files\CA\Identity Manager\IAM Suite\Identity Manager\tools\db\auditing\sqlserver\ims\_mssql\_logs.sql
    - Oracle: C:\Program Files\CA\Identity Manager\IAM Suite\Identity Manager\tools\db\auditing\oracle\ims\_oracle\_logs.sql

- Snapshots:

- MS SQL: C:\Program Files\CA\Identity Manager\IAM Suite\Identity Manager\tools\imrexpert\db\sqlserver\ims\_mssql\_report.sql
- Oracle: C:\Program Files\CA\Identity Manager\IAM Suite\Identity Manager\tools\imrexpert\db\oracle\ims\_oracle\_report.sql

3. Run the script file.

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

## Run the CreateDatabase Script for Workflow

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

### To run the CreateDatabase script

1. Add the path to the sqljdbc.jar to the DB\_CLASSPATH attribute in the CreateDatabase.bat or .sh script before you run it.
2. From a command prompt, run CreateDatabase.bat or sh. The default installation location for Windows for this script is C:\Program Files\CA\Identity Manager\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.jdbc.sqlserver.SQLServerDriver

**SQL Server 2005:** com.microsoft.sqlserver.jdbc.SQLServerDriver

- For the JDBC URL, enter:

**Oracle:** jdbc:oracle:thin:@*wf\_db\_system*:1521:*wf\_oracle\_SID*

**SQL Server:** jdbc:microsoft:sqlserver://*wf\_db\_system*:1433;  
databaseName=*wf\_db\_name*

**SQL Server 2005:** 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.

# Appendix D: CA Identity Manager as a Windows Service

---

This section contains the following topics:

[How to Configure Identity Manager as a Windows Service](#) (see page 131)

[Install the Java Service Wrapper Files](#) (see page 131)

[Configure the Java Service Wrapper](#) (see page 132)

[Install the Windows Service](#) (see page 135)

[Example of a wrapper.conf File](#) (see page 136)

## How to Configure Identity Manager as a Windows Service

CA Identity Manager has the capability to automatically start with its underlying operating system. We recommend the Java Service Wrapper method to run JBoss Application Server as a Windows Service.

Perform the following steps to configure JBoss to run as a Windows Service:

1. [Install the Java Service Wrapper Files](#) (see page 131).
2. [Configure the Java Service Wrapper](#) (see page 132).
3. [Install the Windows Service](#) (see page 135).

## Install the Java Service Wrapper Files

Four files are required to use the Java Service Wrapper and three additional files are provided to launch JBoss manually and install or uninstall the Windows Service.

1. [Download](#) the Java Service Wrapper.
2. Copy the following files into the JBoss **bin** directory:
  - *wrapper\_home\bin\wrapper.exe*—the Java Service Wrapper executable
  - *wrapper\_home\src\bin\App.bat.in*—the batch file to run JBoss in a console
  - *wrapper\_home\src\bin\InstallApp-NT.bat.in*—the batch file to install the Windows Service
  - *wrapper\_home\src\bin\UninstallApp-NT.bat.in*—the batch file to uninstall the Windows Service

*wrapper\_home* is the location where you installed the Java Service Wrapper.

3. Rename the three batch files from Step 1 as follows:
  - *jboss\_home\bin\CAIdentityManager.bat*
  - *jboss\_home\bin\InstallCAIdentityManagerService.bat*
  - *jboss\_home\bin\UninstallCAIdentityManagerService.bat*
4. Copy the following files into the JBoss **lib** directory:
  - *wrapper\_home\lib\wrapper.dll*—native library required by the Java Service Wrapper
  - *wrapper\_home\lib\wrapper.jar*—Java Service Wrapper classes
5. Create the following directory:  
*jboss\_home\conf*
6. Copy the following files into this **conf** directory:  
*wrapper\_home\src\conf\wrapper.conf.in*—the Java Service Wrapper configuration
7. Rename the file as follows:  
*jboss\_home\conf\wrapper.conf*

## Configure the Java Service Wrapper

The libraries, classes, and parameters for CA Identity Manager must be configured in the Java Service Wrapper configuration file:

*jboss\_home\conf\wrapper.conf*

**Note:** Property values that are paths to directories or files should *not* be enclosed in quotation marks. Forward (/) or back-slashes (\) can be used as a path separator.

## Local Environment Variables

Several local environment variables will be created in order to simplify later configuration and to prevent the default ability of the Java Service Wrapper to use the %PATH% from the environment. Careful inspection of the run-idm.bat file will reveal that the %PATH% is carefully constructed in order to eliminate any SiteMinder library version conflicts. These variables are not system-wide and will only be available for the JVM created by the Java Service Wrapper. Some system-wide environment variables are used in the creation of these local variables.

Add the following properties to the beginning of wrapper.conf before any other properties:

- set.JAVA\_HOME=[JAVA\_HOME from run-idm.bat]

**Example:** set.JAVA\_HOME=C:\CA\j2sdk1.4.2\_14

- set.NETE\_SPS\_PATH=[resolved NETE\_SPS\_PATH from run-idm.bat]

**Example:** set.NETE\_SPS\_PATH=C:\CA\eTrust  
SiteMinder\agentframework\bin

- set.IM\_EAR=../server/default/deploy/IdentityMinder.ear

- set.SYSTEM\_PATH=%SystemRoot%\SYSTEM32;%SystemRoot%;%SystemRoot%\SYSTEM32\WBEM

- set.PATH=%IGW\_LOC%;%NETE\_SPS\_PATH%;%NETE\_PS\_PATH%;%IM\_EAR%/library;%SYSTEM\_PATH%

## Java Executable

During the CA Identity Manager installation, a java SDK was selected and was used to set the JAVA\_HOME variable at the top of *jboss\_home*\bin\run-idm.bat. The local environment variable for this location is used in the following property:

wrapper.java.command=%JAVA\_HOME%\bin\java

## Java Classpath

Create all java classpath entries populated in *jboss\_home*\bin\run.bat. Also, include the Java Service Wrapper classes in the classpath that are used within the JVM. That list is as follows, taking advantage of local environment variables created previously:

- wrapper.java.classpath.1=../lib/wrapper.jar
- wrapper.java.classpath.2=%JAVA\_HOME%\lib\tools.jar
- wrapper.java.classpath.3=../run.jar

### Java Library Path

Add the required libraries for JBoss to the library path and the environment path that were created previously:

- `wrapper.java.library.path.1=../lib`
- `wrapper.java.library.path.2=../server/default/lib`
- `wrapper.java.library.path.3=%PATH%`

### Java Arguments

Create the Java arguments that are populated in *jboss\_home\bin\run-idm.bat* and *jboss\_home\bin\run.bat*. That list is as follows, taking advantage of local environment variables created previously and excluding memory settings that will be configured separately:

- `wrapper.java.additional.1=-server`
- `wrapper.java.additional.2=-Dprogram.name=run.bat`
- `wrapper.java.additional.4=-Djava.security.policy=.\workpoint_client.policy`
- `wrapper.java.additional.5=-XX:MaxPermSize=128m`

### Java Memory Sizes

Set the JVM memory settings as follows:

- `wrapper.java.initmemory=256`
- `wrapper.java.maxmemory=512`

### Main Class

Specify the main class that the Java Service Wrapper should be called as follows:

`wrapper.app.parameter.1=org.jboss.Main`

### Java Service Wrapper Logging

The location of the log file for the Java Service Wrapper will default to *jboss\_home/logs/wrapper.log*. Settings can be changed as described in the *wrapper.conf* file.

### Windows Service Names

Specify the names to be used for the Windows Service as follows:

- `wrapper.ntservice.name=CAIdentityManager`
- `wrapper.ntservice.displayname=CA Identity Manager`
- `wrapper.ntservice.description=CA Identity Manager`

## Install the Windows Service

### To install the windows service

1. Run the following batch file to test the configuration:

`CAIdentityManager.bat`

If CA Identity Manager starts in a console, continue on to Step 2.

2. Close the CA Identity Manager console.
3. Run the following batch file to install the Windows Service:

`InstallCAIdentityManagerService.bat`

## Example of a wrapper.conf File

A complete and working wrapper.conf file is provided here for reference:

```
#####  
# Wrapper Properties  
#####  
# Local Environment Variables  
set.JAVA_HOME=C:\CA\j2sdk1.4.2_14  
set.NETE_SPS_ROOT=C:\CA\Trust SiteMinder  
set.NETE_SPS_PATH=%NETE_SPS_ROOT%\agentframework\bin  
set.IM_EAR=../server/default/deploy/IdentityMinder.ear  
set.SYSTEM_PATH=%SystemRoot%\SYSTEM32;%SystemRoot%\%SystemRoot%\SYSTEM32\WBEM  
set.PATH=%IGW_LOC%;%NETE_SPS_PATH%;%NETE_PS_PATH%;  
%IM_EAR%\library;%SYSTEM_PATH%  
  
# Java Application  
wrapper.java.command=%JAVA_HOME%\bin\java  
  
# Java Main class. This class must implement the WrapperListener interface  
# or guarantee that the WrapperManager class is initialized. Helper  
# classes are provided to do this for you. See the Integration section  
# of the documentation for details.  
wrapper.java.mainclass=org.tanukisoftware.wrapper.WrapperSimpleApp  
  
# Java Classpath (include wrapper.jar) Add class path elements as  
# needed starting from 1  
wrapper.java.classpath.1=../lib/wrapper.jar  
wrapper.java.classpath.2=%JAVA_HOME%\lib\tools.jar  
wrapper.java.classpath.3=../run.jar  
  
# Java Library Path (location of Wrapper.DLL or libwrapper.so)  
wrapper.java.library.path.1=../lib  
wrapper.java.library.path.2=../server/default/lib  
wrapper.java.library.path.3=%PATH%  
  
# Java Additional Parameters  
wrapper.java.additional.1=-server  
wrapper.java.additional.2=-Dprogram.name=run.bat  
wrapper.java.additional.4=-Djava.security.policy=../workpoint_client.policy  
wrapper.java.additional.5=-XX:MaxPermSize=128m  
  
# Initial Java Heap Size (in MB)  
wrapper.java.initmemory=256  
  
# Maximum Java Heap Size (in MB)  
wrapper.java.maxmemory=512
```

---

```
# Application parameters. Add parameters as needed starting from 1
wrapper.app.parameter.1=org.jboss.Main

#####
# Wrapper Logging Properties
#####
# Format of output for the console. (See docs for formats)
wrapper.console.format=PM

# Log Level for console output. (See docs for log levels)
wrapper.console.loglevel=INFO

# Log file to use for wrapper output logging.
wrapper.logfile=./logs/wrapper.log

# Format of output for the log file. (See docs for formats)
wrapper.logfile.format=LPTM

# Log Level for log file output. (See docs for log levels)
wrapper.logfile.loglevel=DEBUG

# Maximum size that the log file will be allowed to grow to before
# the log is rolled. Size is specified in bytes. The default value
# of 0, disables log rolling. May abbreviate with the 'k' (kb) or
# 'm' (mb) suffix. For example: 10m = 10 megabytes.
wrapper.logfile.maxsize=10m

# Maximum number of rolled log files which will be allowed before old
# files are deleted. The default value of 0 implies no limit.
wrapper.logfile.maxfiles=5

# Log Level for sys/event log output. (See docs for log levels)
wrapper.syslog.loglevel=NONE

#####
# Wrapper Windows Properties
#####
# Title to use when running as a console
wrapper.console.title=CAIdentityManager

#####
# Wrapper Windows NT/2000/XP Service Properties
#####
# WARNING - Do not modify any of these properties when an application
# using this configuration file has been installed as a service.
# Please uninstall the service before modifying this section. The
# service can then be reinstalled.
```

---

```
# Name of the service
wrapper.ntservice.name=CAIdentityManager

# Display name of the service
wrapper.ntservice.displayname=CA Identity Manager

# Description of the service
wrapper.ntservice.description=CA Identity Manager

# Service dependencies. Add dependencies as needed starting from 1
wrapper.ntservice.dependency.1=

# Mode in which the service is installed. AUTO_START or
# DEMAND_START
wrapper.ntservice.starttype=AUTO_START

# Allow the service to interact with the desktop.
wrapper.ntservice.interactive=false
```

# Appendix E: Windows Services Started by CA Identity Manager

---

The following are the services started on Windows when you install and start all components of CA Identity Manager:

- CA Directory impd-co
- CA Directory impd-inc
- CA Directory impd-notify
- CA Directory impd-router
- CA Directory SSL Daemon – impd
- CA Identity Manager Connector Server (C++)
- CA Identity Manager Connector Server (Java)
- CA Identity Manager 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.



# Appendix F: Installation Worksheet

---

Use the following worksheets to collect information about your system before installing CA Identity Manager. If you are running the CA Identity Manager installer on an IPv6 system, ensure that you provide hostnames (and not IP addresses) in the installer screens.

This section contains the following topics:

[JBoss Information](#) (see page 141)

[Provisioning Information](#) (see page 142)

[Provisioning Components Passwords](#) (see page 142)

[Database Information](#) (see page 143)

[SiteMinder Information](#) (see page 144)

[Reporting Information](#) (see page 145)

## JBoss Information

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

| Field Name              | Description                                                                                                                                  | Your Response |
|-------------------------|----------------------------------------------------------------------------------------------------------------------------------------------|---------------|
| JBoss Folder            | The location of the application server home directory. The path should <i>not</i> contain spaces.                                            |               |
| App Server URL and port | The application URL and port number of the system that will host the Identity Manager Server (system that will host the application server). |               |

## Provisioning Information

### Provisioning Directory Information

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

| Field Name                           | Description                                                                                                                                  | Your Response |
|--------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------|---------------|
| Provisioning Directory Hostname      | The hostname of the Provisioning Directory system.<br><br>You need the hostnames for the primary and any alternate Provisioning Directories. |               |
| Port                                 | The port number of the Provisioning Directory system.                                                                                        |               |
| Provisioning Server Hostname         | The hostname names of each Provisioning Server.<br><br>You need the hostnames for the primary and any alternate Provisioning Servers.        |               |
| Provisioning Directory Shared Secret | The special password for the Provisioning Directory. Use the same password for the primary and any alternate Provisioning Directories.       |               |

## Provisioning Components Passwords

Record the following passwords you need during the Provisioning Server and C++ Server installation.

| Field Name           | Description                                 | Your Response |
|----------------------|---------------------------------------------|---------------|
| Provisioning Server  | A password for this Server.                 |               |
| C++ Connector Server | A password needed for this server. Each C++ |               |

| Field Name             | Description                                                                                                                                                                                                      | Your Response |
|------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------|
|                        | Connector Server can have a unique password.                                                                                                                                                                     |               |
| Provisioning Directory | A password used by Provisioning Server to connect to Provisioning Directory.<br><br>For an alternate Provisioning Server, enter the Provisioning Directory password created for the primary Provisioning Server. |               |

## Database Information

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

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

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

## SiteMinder Information

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

| Field Name                        | Description                                                                                                         | Your Response |
|-----------------------------------|---------------------------------------------------------------------------------------------------------------------|---------------|
| Policy Server Host Name           | The hostname of the SiteMinder Policy Server.                                                                       |               |
| SiteMinder Administrator Name     | The administrator username for the SiteMinder Policy Server.                                                        |               |
| SiteMinder Administrator Password | The administrator user password for the SiteMinder Policy Server.                                                   |               |
| SiteMinder Folder (Solaris Only)  | The location of SiteMinder on the system with a SiteMinder Policy Server installed.                                 |               |
| SiteMinder Agent Name             | The AgentName in the ra.xml file under "IdentityMinder.ear\policyserver.rar\META-INF.<br>Enter it in cipher text.   |               |
| SiteMinder Shared Secret          | The AgentSecret in the ra.xml file under "IdentityMinder.ear\policyserver.rar\META-INF.<br>Enter it in cipher text. |               |

## 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 into the Business Objects Infoview console.                                                                                                                                 |               |
| DSN Name                         | Identify the name of the DSN that the Report Server uses to communicate with the Report Database.                                                                                                       |               |
| TNS Name                         | The name of the TNS that the Report Server uses to communicate with the Report Database.<br><b>Note:</b> This information is needed only if you are using Oracle.                                       |               |
| Database Name                    | Identify the Report Database name.<br><b>Note:</b> This information is needed only if you are using MS SQL.                                                                                             |               |
| User Name                        | Identify the username for the Report Database.                                                                                                                                                          |               |
| Password                         | Identify the administrative password credentials for the Report Database.                                                                                                                               |               |
| 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.<br><b>Note:</b> If you are installing the Report Server on the same system as the CA Identity Manager, ensure that the Tomcat connection port does |               |

| Field Name | Description                                                                                                             | Your Response |
|------------|-------------------------------------------------------------------------------------------------------------------------|---------------|
|            | not conflict with the port number you specified for the application server URL when installing the CA Identity Manager. |               |

**Note:** Oracle and MS SQL are supported for the Report Database.

# Appendix G: Installation Checklists

---

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

This section contains the following topics:

[How to Install Prerequisite Components](#) (see page 147)

[How to Perform a Standalone Installation](#) (see page 147)

[How to Perform a Distributed Installation](#) (see page 148)

[How to Install CA Identity Manager on a JBoss Cluster](#) (see page 148)

[How to Install High Availability Provisioning Components](#) (see page 149)

[How to Protect CA Identity Manager with SiteMinder](#) (see page 149)

[How to Install the Report Server](#) (see page 150)

[How to Uninstall CA Identity Manager](#) (see page 150)

## How to Install Prerequisite Components

To install the prerequisite hardware and software for CA Identity Manager:

|  Step       |
|------------------------------------------------------------------------------------------------|
| 1. Install the CA Identity Manager bookshelf.                                                  |
| 2. Make your system meet the hardware and software requirements.                               |
| 3. Set up the application server as required.                                                  |
| 4. Record the information you will need to supply during the CA Identity Manager installation. |

## How to Perform a Standalone Installation

Use the following checklist to perform a standalone installation of CA Identity Manager:

|  Step |
|------------------------------------------------------------------------------------------|
| 1. Install the components of CA Identity Manager on one system.                          |



---

**Step**

---

2. Configure support for IPv6 if required.
  3. Verify the Identity Manager Server starts.
- 

## How to Perform a Distributed Installation

Use the following checklist to perform a distributed installation of CA Identity Manager:



---

**Step**

---

1. Install CA Identity Manager on the systems required.
  2. Configure support for IPv6 if required.
  3. Verify that the Identity Manager Server starts.
- 

## How to Install CA Identity Manager on a JBoss Cluster

The following procedures describe how to set up multiple JBoss application servers with the same Identity Manager application on each server. In this type of cluster, each JBoss application server acts independently of the other application servers.



---

**Step**

---

1. [Test the Default Multicast Address](#) (see page 42)
  2. [Create the First Cluster Node](#) (see page 43)
  3. [Add Cluster Nodes](#) (see page 47)
-

## 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.                                                          |

## How to Protect CA Identity Manager with SiteMinder

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

|  Step                        |
|---------------------------------------------------------------------------------------------------------------|
| 1. Be sure you have installed the Identity Manager Extensions for SiteMinder on the SiteMinder Policy Server. |
| 2. Install and configure a SiteMinder Web Agent to protect CA Identity Manager resources.                     |
| 3. Install the plug-in the Web Server uses to forward requests to the application server.                     |
| 4. Verify that the plug-in is successfully forwarding requests to the application server.                     |
| 5. Configure the SiteMinder Policy Store for use with CA Identity Manager.                                    |
| 6. Configure SiteMinder high availability for CA Identity Manager.                                            |

## How to Install the Report Server

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

| ✓ | Step                                                    |
|---|---------------------------------------------------------|
|   | 1. Review the report pre-installation checklist.        |
|   | 2. Gather reporting information.                        |
|   | 3. Install the Report Server (CA Business Intelligence) |
|   | 4. Run the Registry Script.                             |
|   | 5. Copy the JDBC JAR files.                             |
|   | 6. Run the command line to deploy the default reports.  |

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

## How to Uninstall CA Identity Manager

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

The following checklist describes the steps to uninstall CA Identity Manager:

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



**Step**

---

5. Remove CA Identity Manager configuration information from the application server.

---



# Index

---

## (

(Optional) Configure a Policy Server • 25

## A

Add Cluster Nodes • 47

Add More Policy Servers • 90

## B

Basic Installation • 12

## C

C++ Connector Server on Solaris • 70

CA Identity Manager as a Windows Service • 131

CA Identity Manager Components • 31

CA Product References • iii

Check for Cumulative Releases • 24

Check Hardware Requirements • 21

Check Software Requirements • 23

Collect Information for the Installer • 26

Configuration File Format • 119

Configure a Relational Database • 83

Configure CA Directory Server • 85

Configure Connector Servers • 65

Configure IPv6 Support • 34, 38

Configure Microsoft Active Directory • 83

Configure Microsoft ADAM • 85

Configure Novell eDirectory Server • 87

Configure Oracle Internet Directory (OID) • 88

Configure Provisioning Server Failover • 59

Configure Sun Java Systems Directory Server or IBM Directory Server • 83

Configure the Java Service Wrapper • 133

Configure the JK Connector • 48

Configure the Policy Store for CA Identity Manager • 82

Connector Server Framework • 60

Connector Servers • 60

Connector Xpress • 75

Connectors • 76

Contact CA • iii

Copy the JDBC JAR Files • 101

Create a Database • 24

Create a FIPS 140-2 Encryption Key • 24

Create an MS SQL Server Database Instance • 126

Create an Oracle Database Instance • 126

Create the First Cluster Node • 43

csfconfig Command • 65

csfconfig Command Examples • 70

## D

Database Creation • 125

Database Information • 28, 143

Deploy Default Reports • 101

Distributed Installation • 35

Distributed versus Clustered Installation • 36

## E

Edit the Data Source • 127

Enable Provisioning Manager Failover • 72

Enable User Console Failover • 71

Example of a wrapper.conf File • 136

Extensions for SiteMinder • 117

## F

Failover for Provisioning Clients • 70

## H

Hardware Requirements • 95

High Availability Installation • 16

High Availability Provisioning Installation • 51

How Resources are Protected • 78

How to Configure Identity Manager as a Windows Service • 131

How to Create a Database Instance • 125

How to Install CA Identity Manager on a JBoss Cluster • 42, 148

How to Install High Availability Provisioning Components • 52, 149

How to Install Prerequisite Components • 20, 147

How to Install the Report Server • 96, 150

How to Perform a Distributed Installation • 36, 148

How to Perform a Standalone Installation • 32, 147

How to Protect CA Identity Manager with SiteMinder • 78, 149

---

How to Run an Unattended Installation • 113  
How to Uninstall CA Identity Manager • 107, 150  
How to Uninstall Reporting • 103

## I

Identity Manager Server • 115  
Identity Manager Server Architecture • 16  
Initial Choices • 114  
Install Additional Components • 39  
Install All Components on One System • 32  
Install Alternate Provisioning Directories • 54  
Install Alternate Provisioning Servers • 59  
Install Connector Servers • 64  
Install Optional Provisioning Components • 74  
Install Provisioning Directories • 52  
Install Provisioning Servers • 57  
Install the CA Identity Manager Bookshelf • 20  
Install the CA Report Server • 98  
Install the Java Service Wrapper Files • 132  
Install the Proxy Plug-In • 80  
Install the SiteMinder Web Agent • 79  
Install the Windows Service • 135  
Installation Checklists • 147  
Installation Log Files • 123  
Installation on a JBoss Cluster • 41  
Installation on UNIX and Console Mode • 18  
Installation Overview • 11  
Installation Status • 19, 31, 35, 41, 51, 73, 77, 93  
Installation with a SiteMinder Policy Server • 14  
Installation Worksheet • 18, 141

## J

JBoss Application Server • 26  
JBoss Information • 26, 141

## L

Load-Balancing and Failover • 62  
Log files on UNIX • 124  
Log Files on Windows • 123

## M

Meet System Requirements • 21  
Modify Policy Server Connection Settings • 89  
Modify the Configuration File • 113  
Multi-Platform Installations • 63

## O

Optional Provisioning Component Installation • 73  
Overall Installation Process • 18

## P

Perform a Distributed Installation • 37  
Perform Prerequisite Configuration for New Provisioning Directories • 53  
Perform Prerequisite Configuration for New Provisioning Servers • 58  
Prerequisite Knowledge • 20  
Product Prerequisites • 19  
Provisioning Components • 117  
Provisioning Components Architecture • 17  
Provisioning Components Passwords • 27, 142  
Provisioning Information • 27, 141  
Provisioning Manager Setup • 75  
Provisioning Server Disaster Recovery • 60  
Provisioning Servers • 56

## R

Reinstall CA Identity Manager • 111  
Reliability and Scalability • 63  
Remove CA Identity Manager from JBoss • 111  
Remove CA Identity Manager Objects with the Management Console • 108  
Remove Leftover Items • 104  
Remove the CA Identity Manager schema from a SQL Policy Store • 108  
Remove the CA Identity Manager schema from an LDAP Policy Store • 109  
Remove the CA Identity Manager Schema from the Policy Store • 108  
Remove UNIX Items • 105  
Remove Windows Items • 104  
Report Server Installation • 93  
Reporting Architecture • 94  
Reporting Considerations • 95  
Reporting Information • 97, 144  
Reports Pre-Installation Checklist • 96  
Router DSA for the Provisioning Server • 57  
Run the CreateDatabase Script for Workflow • 129  
Run the Registry Script • 100  
Run the SQL Scripts • 128  
Run the UNIX Installer • 99  
Run the Windows Installer • 99

---

## S

- Sample CA Identity Manager Installations • 11
- Select Load Balancing or Fail Over • 91
- SiteMinder High Availability for a JBoss Cluster • 89
- SiteMinder Information • 29, 143
- SiteMinder Protection of CA Identity Manager • 77
- Standalone Installation • 31
- Start the JBoss Cluster • 49
- Start the Servers for JBoss • 81

## T

- Test the Default Multicast Address • 42
- Test the Provisioning Manager Failover • 72

## U

- Unattended Installation • 113
- Uninstall CA Identity Manager Software Components • 110
- Uninstall the Report Server from UNIX • 103
- Uninstall the Report Server from Windows • 103
- Uninstallation and Reinstallation • 107

## V

- Verify the Clustered Installation • 49
- Verify the Identity Manager Server Starts • 34, 39
- Verify the Policy Store • 88
- Verify the Reporting Installation • 103
- Verify the Web Agent and Connector • 82

## W

- Windows Services Started by CA Identity Manager • 139