



Cisco Interaction Manager Installation Guide

Release 4.1(1)
January 2007

Corporate Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
<http://www.cisco.com>
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100



THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

CCSP, CCVP, the Cisco Square Bridge logo, Follow Me Browsing, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Access Registrar, Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StrataView Plus, TeleRouter, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0502R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

Cisco Interaction Manager Installation Guide
© 2007 Cisco Systems, Inc. All rights reserved.

Contents

Preface	7
About this guide	8
Document conventions	8
Other learning resources	9
Online help	9
Document set.	9
Chapter 1: Installation basics	10
Configuration options	11
Additional partitions and departments	12
Chapter 2: Pre-installation tasks	14
Verifying system requirements	15
Collecting required information	15
Configuring environment variables	15
Verifying SQL Server authentication mode	15
Verifying state of Microsoft Search service	16
Setting up user accounts and permissions.	17
Verifying directory names	17
Creating WebLogic domains	17
Creating a WebLogic domain for primary Application Server.	18
Creating WebLogic domains for secondary Application Servers.	21
Verifying the WebLogic domain	27
Additional requirements for split- and distributed-server configurations	27
Chapter 3: Installation process	28
Installing a single-server configuration	29
Installing a split-server configuration	35

Installing a distributed-server configuration	35
Installing File Server	36
Installing Database	37
Installing primary Application Server	41
Installing secondary Application Servers	47
Installing Web Server	48
Installing Services Server	50
Chapter 4: Post-installation tasks	53
Setting up archives for partition databases	54
Copying license files	54
Verifying configuration of File Server	54
Verifying configuration of Application Servers	55
Applying updates	55
Separating the Web Server from the Application Server	56
Changing Web Server settings	56
Configuring content expiration settings	56
Configuring access for attachments without extensions	57
Changing IIS configuration settings	58
Changing authentication settings for web site	58
Changing security credentials for network directory	60
Starting Cisco Interaction Manager	62
Logging in to the business partition	63
Launching Cisco Interaction Manager from Cisco Agent Desktop Embedded Browser	63
Configuring some important settings	63
Settings that must be configured	64
ESMTP settings	64
Recommended settings	64
Optional settings	65
Uninstalling Cisco Interaction Manager	65
Chapter 5: Additional partitions	67
About partitions	68

Verifying prerequisites	68
Installing a new business partition	69
Chapter 6: Archives	73
About archives	74
Setting up the archive for a partition	74
Chapter 7: SSL for secure connections	77
Installing Microsoft Certificate Services	78
Installing a security certificate	81
Generating a security certificate request	81
Submitting the certificate request	85
Getting the certificate issued	86
Installing the certificate on the Web Server	87
Configuring SSL access	87
Configuring the viewing of attachments	89
Testing SSL access	89
Appendix A: Additional information	90
Best practices for distributed installations	91
Frequently asked questions	92
Starting and stopping components	93
Starting sequence	94
Stopping sequence	94
Starting Services Server and primary Application Server	94
Starting secondary Application Servers	95
Appendix B: Reference sheet	96
Configuration details	97
File Server details	97
Database details	97
Application Server details	99

Cisco Interaction Manager Installation Guide

Web Server details	100
Services Server details	101
Archive details	101

Preface

- ▶ [About this guide](#)
- ▶ [Other learning resources](#)

Welcome to Cisco® Interaction Manager™—multichannel interaction software used by businesses all over the world to build and sustain customer relationships. A comprehensive suite of the industry’s best applications for multichannel customer interaction management, Cisco Interaction Manager is the backbone of many innovative contact center and customer service helpdesk organizations.

About this guide

Cisco Interaction Manager Installation Guide is intended for installation engineers, system administrators, database administrators, and others who are responsible for installing and maintaining Cisco Interaction Manager.

As you need to prepare the installation environment in advance, you should read this guide, *Cisco Interaction Manager System Requirements*, and *Cisco Interaction Manager Release Notes* well before beginning the installation process.

Document conventions

This guide uses the following typographical conventions.


Convention	Indicates
<i>Italic</i>	Emphasis, or the title of a published document.
Bold	The label of an item in the user interface, such as a field, button, or tab.
<code>Monospace</code>	A file name or command. Also, text that must be typed by the user.
<i>Variable</i>	User-specific text, which is supplied by the user.

Other learning resources

Various learning tools are available within the product, as well as on the product CD and our website. You can also request formal end-user or technical training.

Online help

The product includes topic-based as well as context-sensitive help.

Use	To view
 Help button	All topics in <i>Cisco Interaction Manager Help</i> ; the Help button appears in the console toolbar on every screen, as well as on most windows.
F1 keypad button	Context-sensitive information about the item selected on the screen.

Document set

For more information about Cisco Interaction Manager, see the following documents. They can be found in the **Documents** folder on the product CD.

- ▶ *Cisco Interaction Manager System Requirements*
- ▶ Cisco Interaction Manager user's guides

1 Installation basics

- ▶ [Configuration options](#)
- ▶ [Additional partitions and departments](#)

This chapter will help you plan your installation. Use the reference sheet provided in “Appendix B: Reference sheet” on page 96 to record your configuration and installation choices.

Configuration options

This section contains information to help you decide how to configure your installation. An installation has five components:

1. File Server
2. Database
3. Application Server
4. Web Server
5. Services Server

These components can be installed in three types of configuration:

1. **Single server:** All components are installed on a single server.
2. **Split server:** The Database is installed on one server. *All* other components are on a different server
3. **Distributed server:** The Database is installed on one server and other components are distributed over two or more servers. A wide range of options is available for configurations of this type (see the following table for some popular configuration choices).

Type	Server 1	Server 2	Server 3	Server 4	Server 5
Single server	All components				
Split server	Database	Other components			
Distributed server: Option 1	Database File Server	Application Server Web Server Services Server			
Distributed server: Option 2	Database	File Server	Application Server Web Server Services Server		

Type	Server 1	Server 2	Server 3	Server 4	Server 5
Distributed server: Option 3	Database	File Server	Application Server Web Server	Services Server	
Distributed server: Option 4	Database	File Server	Application Server	Web Server	Services Server

Some common distributed configuration options

Additional partitions and departments

As Cisco Interaction Manager is designed for enterprise-wide deployments, a single installation can be used by various independent or semi-independent business units in an organization. You can easily set up the system to mirror the structure of your business.

An installation can have one or more business partitions, which are meant to be used as independent units. While the hardware and software is common for all partitions, system resources and business objects are stored and managed separately for each partition. Partitions are ideal for organizations where business units (or clients, in the case of an outsourced services provider) do not need to share customer, interaction, or product information. For example, a bank, which serves individual retail consumers as well as corporations, might want two partitions as the product offerings and customer service needs for these segments are different. Partitions can also be used for different geographies. The same bank, to continue with our example, might choose to use separate partitions for their US and China businesses because of legal and regulatory needs.

The installation program creates two partitions:

1. The System partition
2. A single-department business partition

You can create additional business partitions by using the installation program (see “Additional partitions” on page 67). Create additional partitions if you want:

- ▶ Complete segregation of data between business units in your enterprise.
- ▶ To serve multiple customers from a single installation.

Each partition can have one or more departments. While partitions do not share system resources or business objects, departments within a partition share system resources and can also share specific business resources. Departments are suited for

organizations where units would like to share system resources and a few business objects such as users.

Additional departments are created in the Administration Console. See *Cisco Interaction Manager Administration Console User's Guide* for more information.

2 Pre-installation tasks

- ▶ [Verifying system requirements](#)
- ▶ [Collecting required information](#)
- ▶ [Configuring environment variables](#)
- ▶ [Verifying SQL Server authentication mode](#)
- ▶ [Verifying state of Microsoft Search service](#)
- ▶ [Setting up user accounts and permissions](#)
- ▶ [Verifying directory names](#)
- ▶ [Creating WebLogic domains](#)
- ▶ [Additional requirements for split- and distributed-server configurations](#)

This chapter describes a number of pre-installation procedures. It is important to perform these procedures carefully and well.

Verifying system requirements

To verify system requirements

- ▶ Verify that your system meets the bandwidth, hardware, and software requirements listed in *Cisco Interaction Manager System Requirements*. This document is available on the application CD. For information on installing the required software, refer to the documentation on the environment CD.

Collecting required information

To collect required information

- ▶ Use the reference sheet provided in Appendix B (page 96) to gather the information that you will need during the installation process.

Configuring environment variables

To configure environment variables

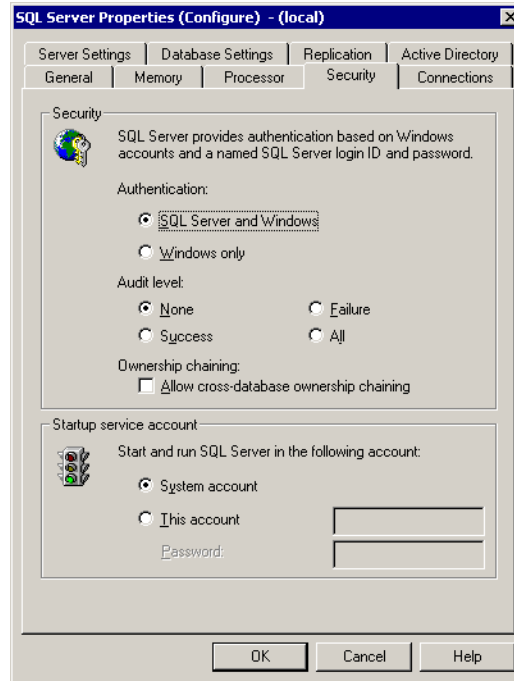
1. Ensure that the JDK path is added to the `path` environment variable. For example, `BEA_Home\JDK142_08`.
2. Set the `TEMP` environment variable to point to some physical location on the system. For example, `C:\temp`.

Verifying SQL Server authentication mode

To verify SQL Server authentication mode

1. Go to **Start > Programs > Microsoft SQL Server > Enterprise Manager**.
2. Browse to **Microsoft SQL Servers > SQL Server Group > *Server_Name***.
3. Right click on the *Server_Name* and select **Properties**.

4. In the SQL Server Properties window, go to the **Security** tab.
5. Verify that the SQL Server authentication mode is set to **SQL Server and Windows**. If authentication is set to **Windows only**, then the application won't be able to connect to the database.



Verify SQL Server authentication

Verifying state of Microsoft Search service

To verify the state of the Microsoft Search service

1. Go to **Start > Programs > Administrative Tools > Services**.
2. Ensure that the Microsoft Search service is running.

This service is required for text searches.

Setting up user accounts and permissions

You will need administrator privileges on the local system to install Cisco Interaction Manager.

To set up user accounts and permissions

1. Create a domain user account for exclusive use by Cisco Interaction Manager.



Caution: Do not change the password of the domain account after Cisco Interaction Manager is installed. The system becomes inaccessible if the password is changed later.

In a single- or split-server installation, a domain account is not mandatory. However, in a distributed installation, a domain user account is required.

2. Add this account to your local administrator group. Use this account to install and configure the system.
3. Verify that the anonymous access user account of the IIS web server or the virtual directory on the web server has permissions to read, write, and execute in *CIM_Home*.
4. Verify that the IIS service is running on a local system account.

Run the system under the local system account in a single- or split-server installation, and under the domain account in a distributed configuration.

Verifying directory names

To verify directory names

- ▶ Ensure that the names of your BEA, WebLogic, and JDK home directories do not contain any spaces.

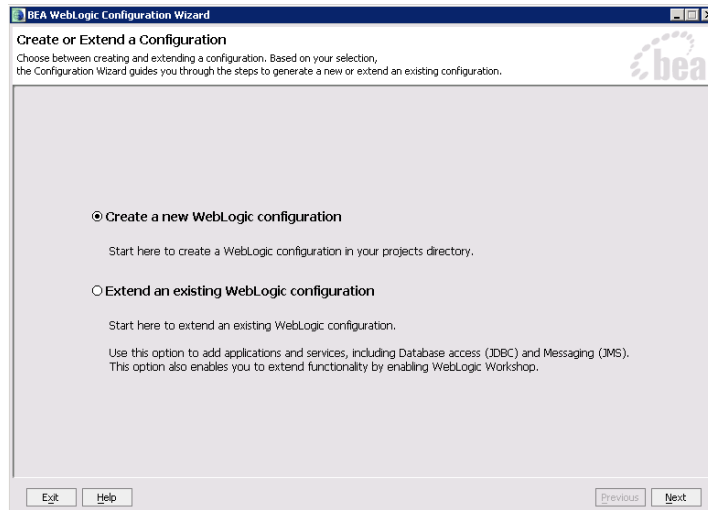
Creating WebLogic domains

You need to create WebLogic domains for each Application Server in your configuration before starting the installation program. The procedures for creating the WebLogic domain for the primary Application Server and that for the secondary Application Server is different.

Creating a WebLogic domain for primary Application Server

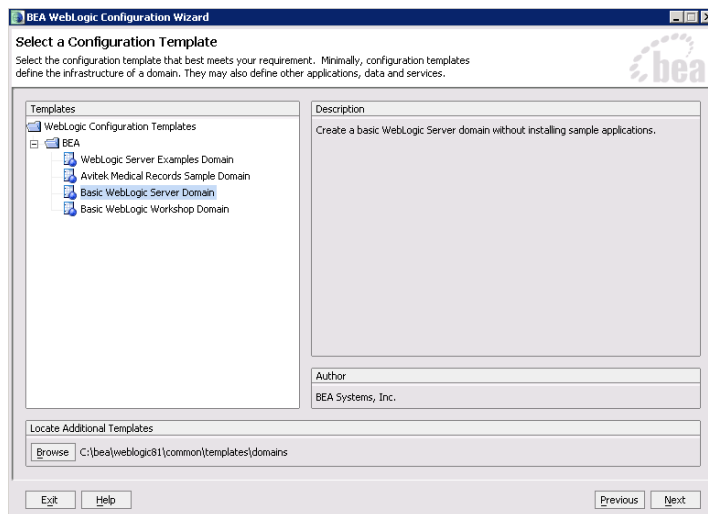
To create the WebLogic domain

1. Go to **Start > Programs > BEA WebLogic Platform 8.1 > Configuration Wizard**.
2. In the Create or Extend a Configuration window, select **Create a new WebLogic configuration**.



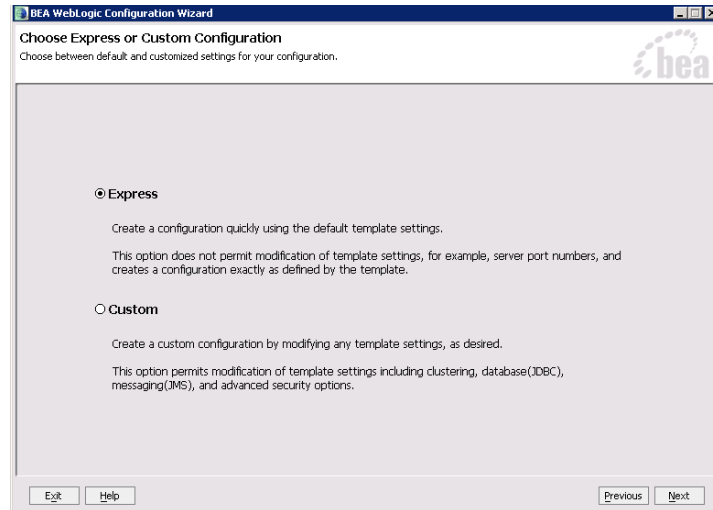
Choose to create a new WebLogic configuration

3. In the Select a Configuration Template window, select **Basic WebLogic Server Domain**.



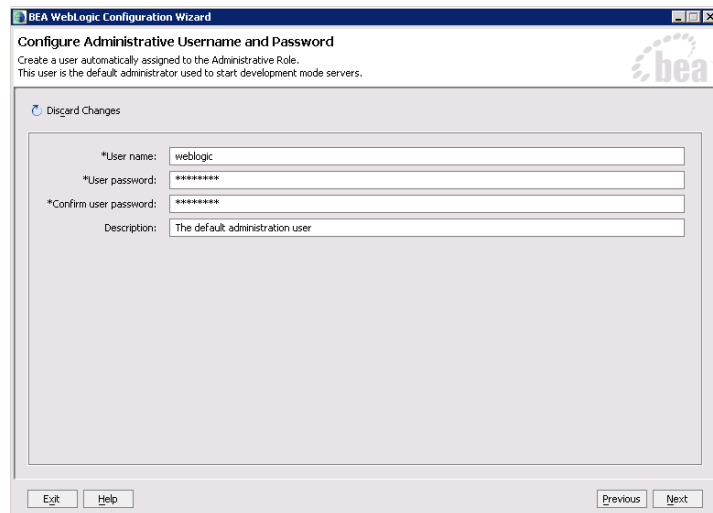
Choose configuration template

4. In the Choose Express or Custom Configuration window, select the **Express** configuration option.



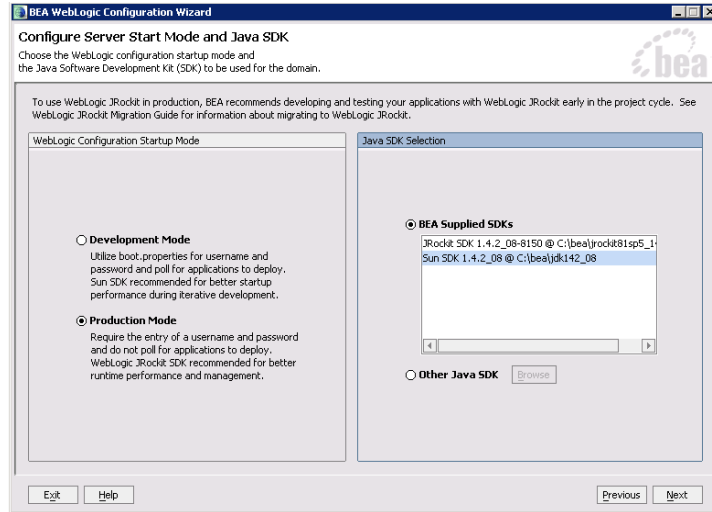
Choose express configuration

5. In the Configure Administrative Username and Password window, configure the user name and password of the WebLogic administrator.



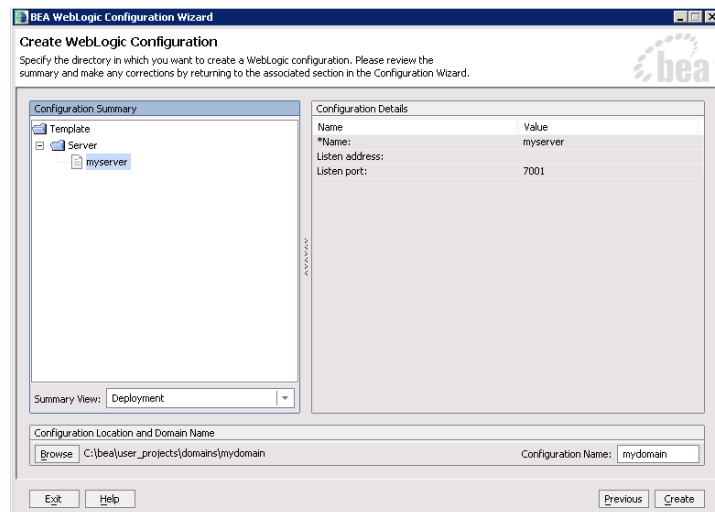
Create administrative user

- In the Configure Server Start Mode and Java SDK window, select the start mode option to be **Production Mode**. And, in the **BEA Supplied SDKs** list, select **Sun SDK 1.4.2_08**.



Configure server start mode and Java SDK

- In the Create WebLogic Configuration window, select **myserver** and click the **Create** button to complete the process of creating the domain.



Create WebLogic configuration

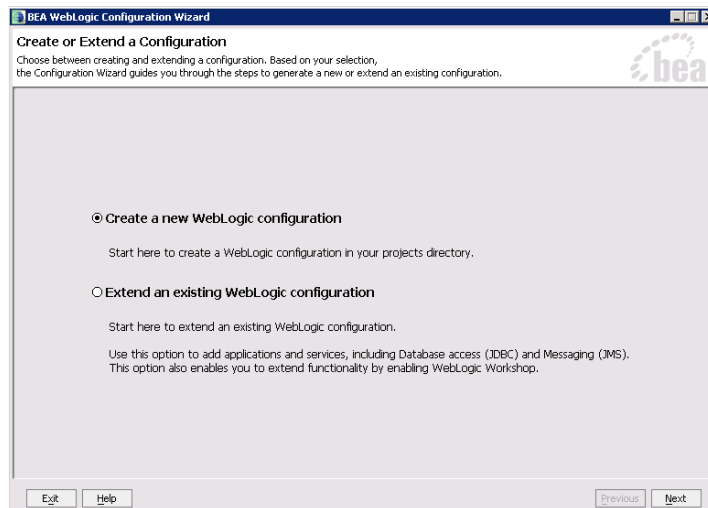
After creating the WebLogic domain, you can verify that it has been created successfully. For details see “Verifying the WebLogic domain” on page 27.

Creating WebLogic domains for secondary Application Servers

Skip this procedure, if you have only one Application Server.

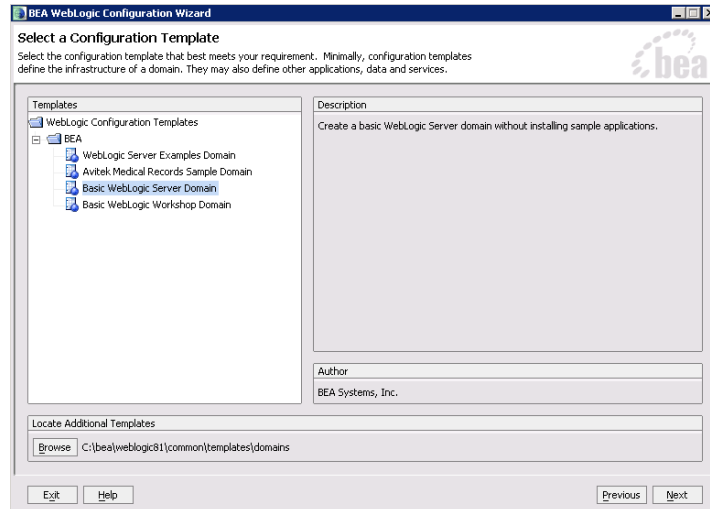
To create the WebLogic domain

1. Go to **Start > Programs > BEA WebLogic Platform 8.1 > Configuration Wizard**.
2. In the Create or Extend a Configuration window, select **Create a new WebLogic configuration**.



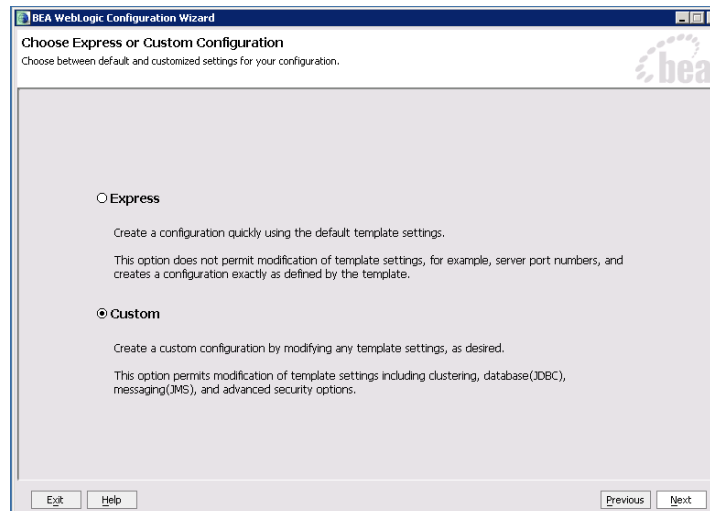
Choose to create a new WebLogic configuration

3. In the Select a Configuration Template window, select **Basic WebLogic Server Domain**.



Choose configuration template

4. In the Choose Express or Custom Configuration window, select the **Custom** configuration option.



Choose custom configuration

5. In the Configure the Administration Server window, provide the name of the server you want to create.



Important: The server name should be different than that of the primary Application Server.

The screenshot shows the 'Configure the Administration Server' window of the BEA WebLogic Configuration Wizard. The window title is 'BEA WebLogic Configuration Wizard'. Below the title bar, it says 'Configure the Administration Server' and provides instructions: 'Enter administration server configurations. Each WebLogic Server domain must have one Administration Server. The Administration Server hosts the Administration Console which is used to perform administrative tasks.' There is a 'Discard Changes' link at the top left. The main area contains several input fields: '*Name:' with the value 'myserver1', 'Listen address:' with a dropdown menu set to 'All Local Addresses', 'Listen port:' with the value '7001', and 'SSL listen port:' with the value 'N/A'. There is an unchecked checkbox for 'SSL enabled:'. At the bottom, there are buttons for 'Exit', 'Help', 'Previous', and 'Next'.

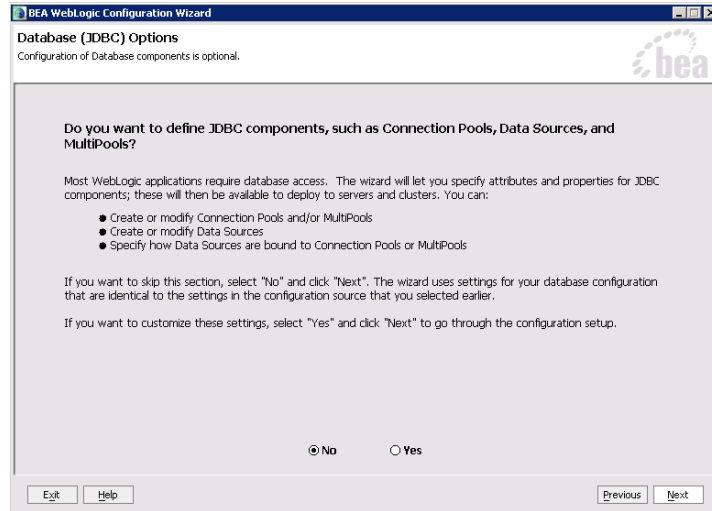
Configure the administration server

6. In the Manage Servers, Clusters, and Machines Options window, select **No**.

The screenshot shows the 'Managed Servers, Clusters, and Machines Options' window of the BEA WebLogic Configuration Wizard. The window title is 'BEA WebLogic Configuration Wizard'. Below the title bar, it says 'Managed Servers, Clusters, and Machines Options' and provides instructions: 'Configuration of Managed Servers, Clusters, and Machines is optional.' There is a 'Discard Changes' link at the top left. The main area contains the following text: 'Do you want to distribute your WebLogic configuration across managed servers, clusters, and physical machines?' followed by a paragraph: 'Your WebLogic configuration minimally requires a single Administration Server on a single machine. You may optionally configure additional resources to be managed by the Administration Server and distribute them across multiple machines. You can:' followed by a bulleted list: '• Add, change or delete managed servers', '• Add, change or delete clusters', '• Group managed servers into clusters, or change the current grouping', and '• Assign servers to machines, or change the current assignment'. Below the list, there are two paragraphs of text explaining the 'No' and 'Yes' options. At the bottom, there are radio buttons for 'No' (which is selected) and 'Yes'. At the bottom of the window, there are buttons for 'Exit', 'Help', 'Previous', and 'Next'.

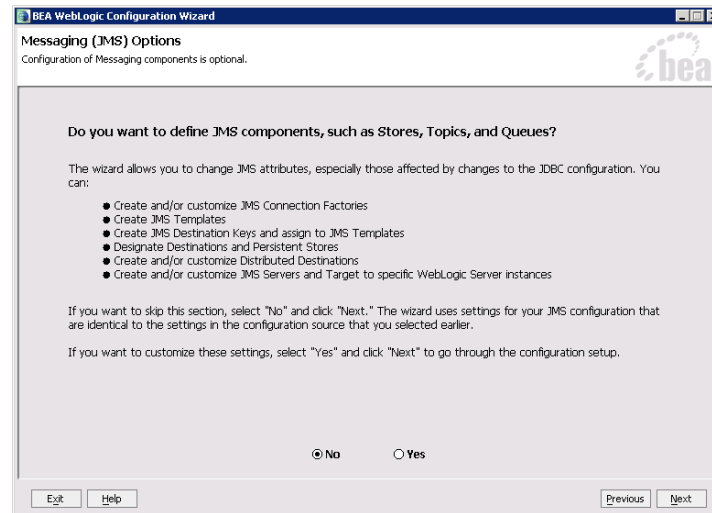
Managed Server, Clusters, and Machines Options window

7. In the Database (JDBC) Options window, select **No**.



Database (JDBC) Options window

8. In the Messaging (JMS) Options window, select **No**.



Messaging (JMS) Options window

9. In the Configure Administrative Username and Password window, configure the user name and password of the WebLogic administrator.

The screenshot shows the 'Configure Administrative Username and Password' window of the BEA WebLogic Configuration Wizard. The window title is 'BEA WebLogic Configuration Wizard' and the subtitle is 'Configure Administrative Username and Password'. Below the subtitle, it says 'Create a user automatically assigned to the Administrative Role. This user is the default administrator used to start development mode servers.' There is a 'Discard Changes' link at the top left. The main area contains four input fields: '*User name:' with the value 'weblogic', '*User password:' with '*****', '*Confirm user password:' with '*****', and 'Description:' with 'The default administration user'. At the bottom, there are radio buttons for 'No' (selected) and 'Yes'. Navigation buttons 'Exit', 'Help', 'Previous', and 'Next' are located at the bottom of the window.

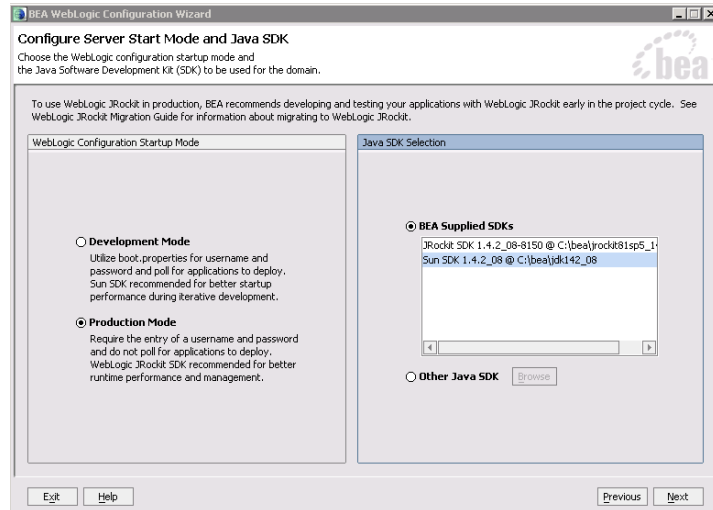
Create administrative user

10. In the Configure Windows Options window, select **No** for both options.

The screenshot shows the 'Configure Windows Options' window of the BEA WebLogic Configuration Wizard. The window title is 'BEA WebLogic Configuration Wizard' and the subtitle is 'Configure Windows Options'. Below the subtitle, it says 'Choose whether or not to add a Windows Start Menu Shortcut and install the server as a Windows service.' There are two panels. The left panel, 'Create Start Menu', has two radio button options: 'Yes' (unselected) with 'Add a shortcut in the Start Menu.' and 'No' (selected) with 'Do not add a shortcut in the Start Menu.' The right panel, 'Install Administrative Server as a Windows Service', has two radio button options: 'Yes' (unselected) with 'I have administrative privileges and want to register my administrative server as a service.' and 'No' (selected) with 'Do not register my administrative server as a service now. See product documentation for post-install registration of a server as a service.' Navigation buttons 'Exit', 'Help', 'Previous', and 'Next' are located at the bottom of the window.

Configure Windows options

- In the Configure Server Start Mode and Java SDK window, select the start mode to be **Production Mode**. And, in the **BEA Supplied SDKs** list, select **Sun SDK 1.4.2_08**.

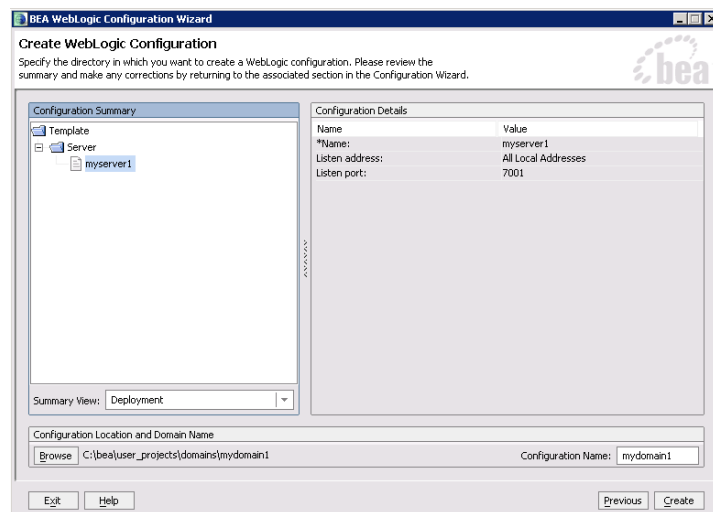


Configure server start mode and Java SDK

- In the Create WebLogic Configuration window, select the administration server you created in Step 5 and click the **Create** button to complete the process of creating a WebLogic domain.



Important: The domain name should be different than that of the primary Application Server.



Create WebLogic configuration

After creating the WebLogic domain, you can verify that it has been created successfully. For details see “Verifying the WebLogic domain” on page 27.

Verifying the WebLogic domain

After creating the WebLogic domain, you can verify that it has been created successfully.

To verify the WebLogic domain

1. Go to *BEA_Home*\user_projects\domains.
2. Verify that there is a folder with the same name that you provided while creating the WebLogic domain.

Additional requirements for split- and distributed-server configurations

Check the following settings

- ▶ Ensure that all the machines are in the same domain.
- ▶ Ensure that all the machines are in the same LAN.
- ▶ Ensure that the system clocks of all the machines are synchronized.

3 Installation process

- ▶ [Installing a single-server configuration](#)
- ▶ [Installing a split-server configuration](#)
- ▶ [Installing a distributed-server configuration](#)

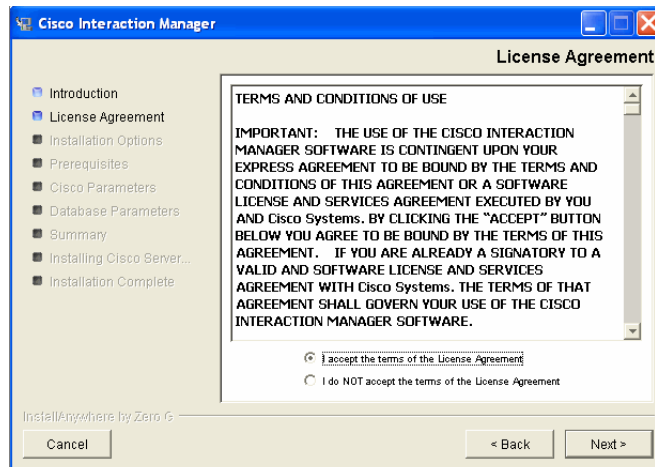
This chapter helps you install the product in the configuration you have chosen (see “Configuration options” on page 11). It describes the process of installing a single-server, split-server, and distributed-server configuration.

Before beginning the installation, ensure that you have complied with all the prerequisites.

Installing a single-server configuration

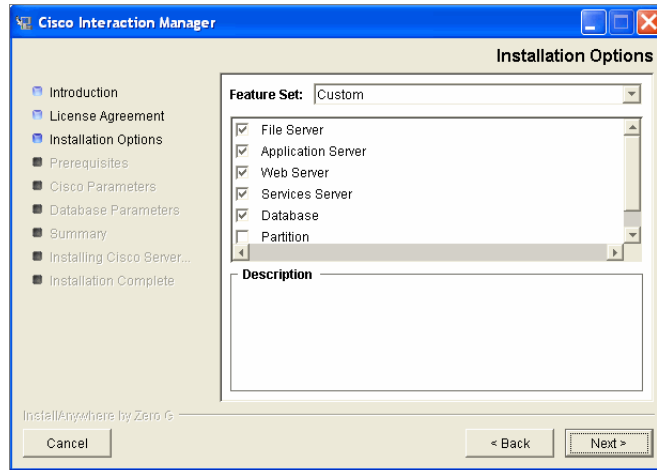
To install a single-server configuration

1. Run `Setup.exe` from the product CD.
2. When the Introduction window appears, read the installation instructions.
3. In the License Agreement window, review the licensing terms and select the **I accept the terms of the License Agreement** option.



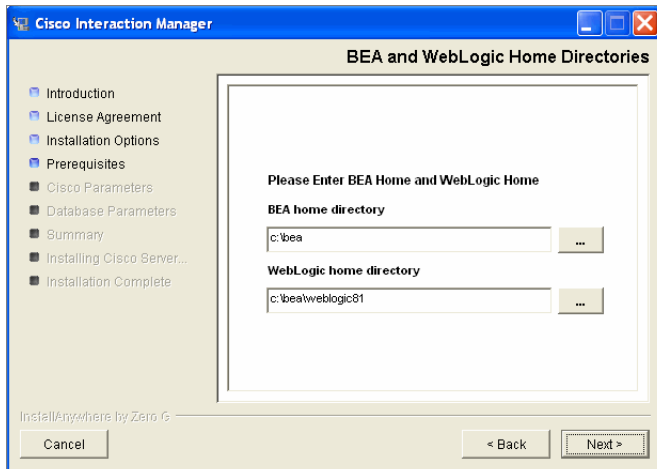
Read and accept the terms of the License Agreement

4. In the Installation Options window, select the following options:
 - File Server
 - Application Server
 - Web Server
 - Services Server
 - Database



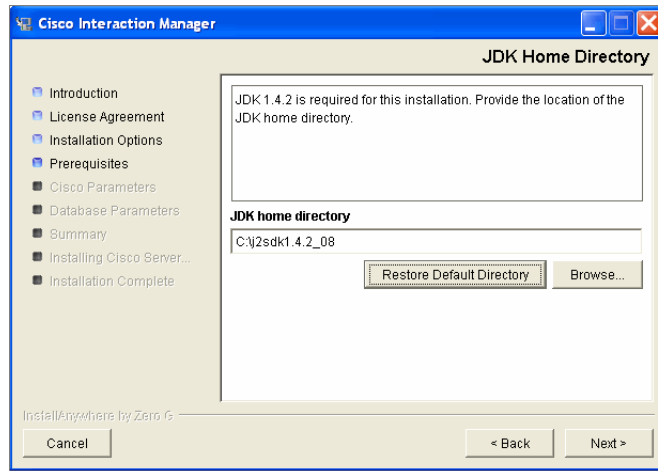
Select installation options

5. Type the path to or browse to the BEA and WebLogic home directories.



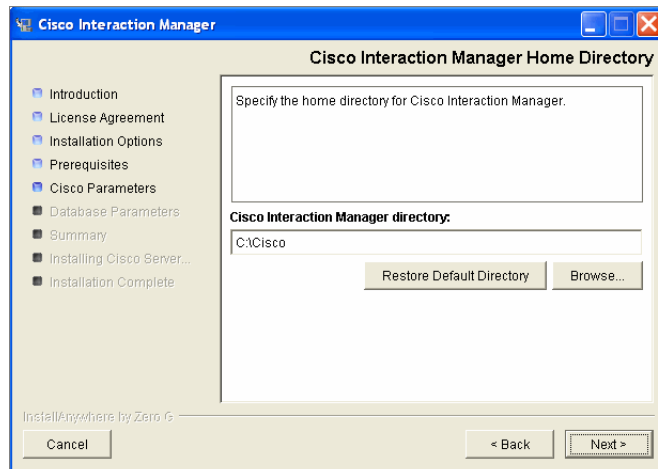
Provide the path to the BEA and WebLogic home directories

6. Type the path to or browse to the JDK home directory.



Provide the path to the JDK home directory

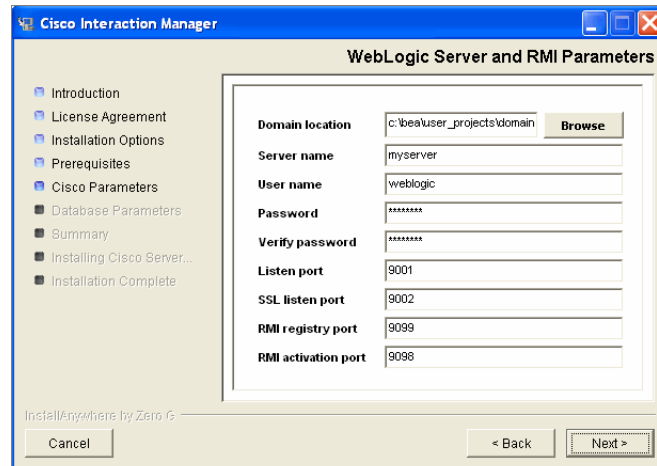
7. Type the path or browse to the folder where you would like to install Cisco Interaction Manager.



Provide a location for the Cisco Interaction Manager home directory

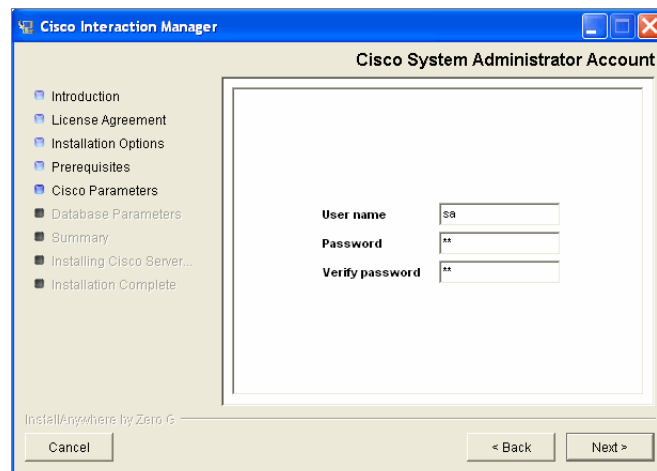
8. In the WebLogic Server and RMI Parameters window, provide the following details.
 - **Domain Location:** Location of the WebLogic domain you configured on page 17.
 - **Server name:** Name of your WebLogic server (page 17). The default name is `myserver`.
 - **User name:** User name of the WebLogic system user (page 17), required to access the WebLogic Server Administration Console.

- **Password:** Password for the WebLogic system user (page 17).
- **Listen port:** Port number of the WebLogic server.
- **SSL listen port:** WebLogic Secure Socket Layer Listen port number.
- **RMI activation port:** Port number used by the RMI Daemon Process.



Provide WebLogic server and RMI parameters

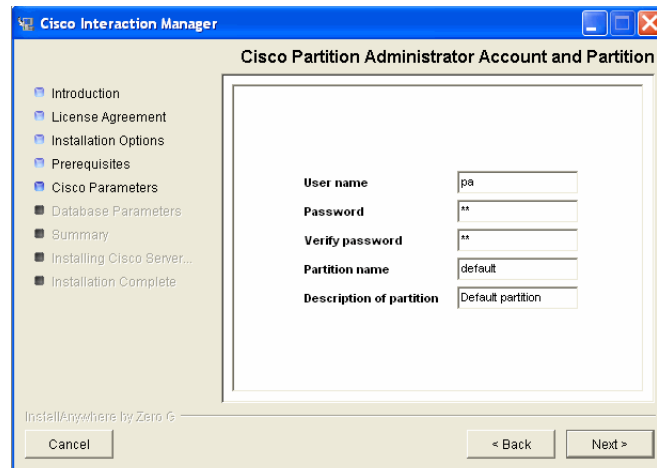
9. In the Cisco System Administrator Account window, type a user name and password for the system administrator.



Create the first system administrator user account

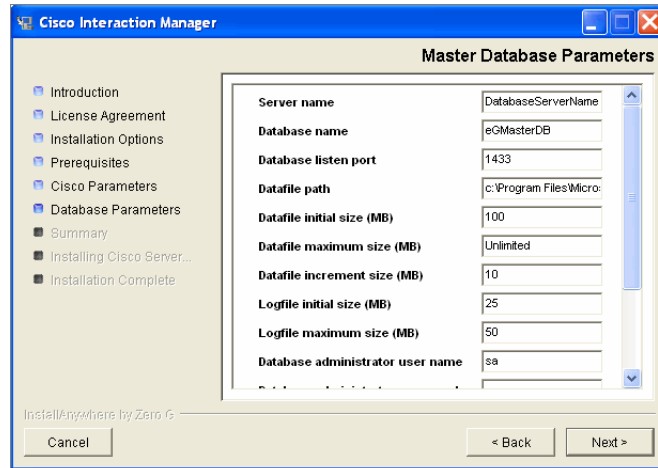
10. In the Cisco Partition Administrator Account and Partition window, provide:
- A user name for the partition administrator.
 - A password for the partition administrator.
 - A name for the partition.

- A description for the partition.



Create the first partition administrator user account and the partition

11. In the Master Database Parameters window, provide the following details about the master database.
 - **Server name:** Name of the local server on which the MSSQL database is to be installed.
 - **Database name:** Name of the master database. The installation program creates the master database with the name you type here.
 - **Database listen port:** MSSQL server port number.
 - **Datafile path:** Path to the data folder on the database server. For example:
MSSQL_Home\MSSQL\Data.
 - **Datafile initial size:** Minimum datafile size for the database.
 - **Datafile maximum size:** Maximum datafile size for the database.
 - **Datafile increment size:** Additional file size limit that will be allocated to a database object after the initial size is full.
 - **Logfile initial size:** Minimum logfile size for log entries.
 - **Logfile maximum size:** Maximum logfile size for log entries.
 - **Database administrator user name:** User name of the database administrator for MSSQL server.
 - **Database administrator password:** Password of the database administrator.
 - **Cisco Database user name:** User name required to connect to the Cisco Interaction Manager master database. The installation program creates the database and its user.
 - **Cisco Database password:** Password for Cisco Interaction Manager master database user.



Provide Master Database parameters

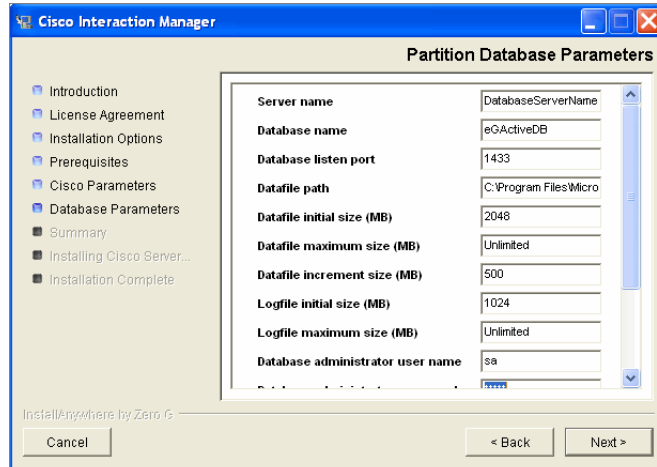
12. In the Partition Database Parameters window, provide the following details.



Important: Partition Database should be created on the same database server as Master Database.

- **Server name:** Name of the local server on which your MSSQL database is installed.
- **Database name:** Name of the partition database. The installation program creates a database with the name you type here.
- **Database listen port:** MSSQL server port number.
- **Datafile path:** Path to the Data folder on the database server. For example:
MSSQL_Home\MSSQL\Data.
- **Datafile initial size:** Minimum datafile size for the database.
- **Datafile maximum size:** Maximum datafile size for the database.
- **Datafile increment size:** Additional file size limit that will be allocated to a database object after the initial size is full.
- **Logfile initial size:** Minimum logfile size for log entries.
- **Logfile maximum size:** Maximum logfile size for log entries.
- **Database administrator user name:** User name of the database administrator for MSSQL server.
- **Database administrator password:** Password of the database administrator.
- **Cisco Database user name:** User name required to connect to the Cisco Interaction Manager database. The installation program creates the database and its user.

- **Cisco Database password:** Password for Cisco Interaction Manager database user.



Provide Partition Database parameters

13. Review the information displayed in the Summary window, and click **Install**.
14. In the Installation Complete window, click **Finish** to complete the installation process.

Installing a split-server configuration

To install a split-server configuration

- ▶ Follow all the steps in “To install a single-server configuration” on page 29. In Steps 11 and 12 make sure you give the following values.
 - Server name: Give the name of the remote server on which you want to install the Partition and Master Databases.

Installing a distributed-server configuration

In the procedure described here, each component is installed separately on a dedicated machine.



Important: Refer to the sheet on page 96 for details that you are asked to provide during the installation.

Make sure you install the components in the following order.

1. File Server
2. Database
3. Application Server
4. Web Server
5. Services Server

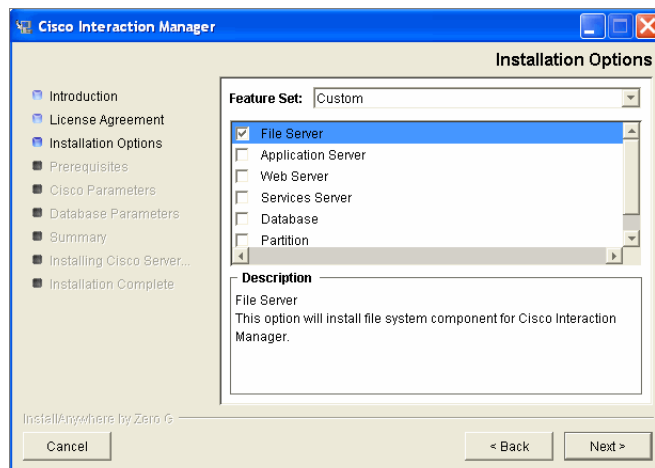
Installing File Server



Important: Run the installation program from the File Server desktop.

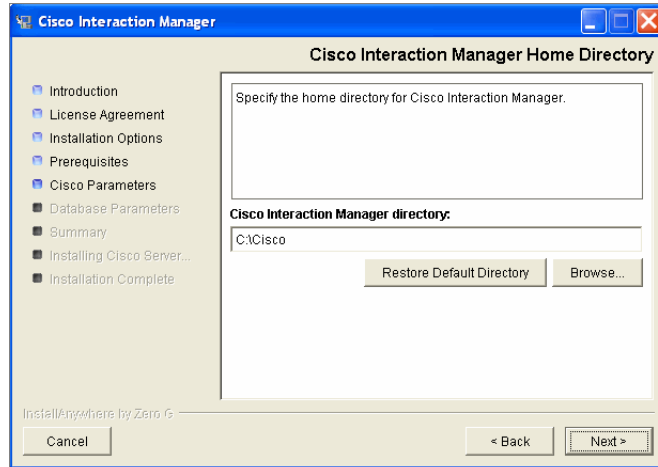
To install the File Server

1. Follow Steps 1–3 in “To install a single-server configuration” on page 29.
2. In the Installation Options window, select the **File Server** option.



Installation Options window

3. Type the path or browse to the folder where you would like to install the File Server.



Cisco Interaction Manager Home Directory window

4. Review the information displayed in the Summary window, and click **Install**.
5. In the Install Complete window, click the **Finish** button to complete the installation process.

Installing Database

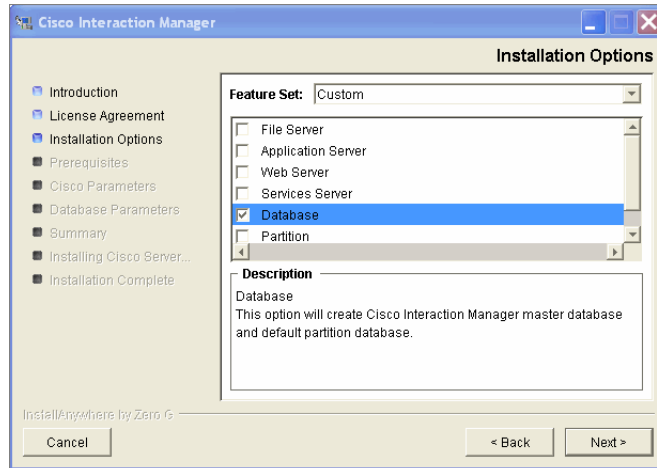


Important: Ensure that MSSQL Server, MS Search Service, and MSSQL Server Agent Service are running. If you are planning a distributed installation, verify that all machines are in the same domain and LAN, and their clocks are synchronized.

This section describes the process of installing Cisco Interaction Manager master database and the default partition database.

To install the Database

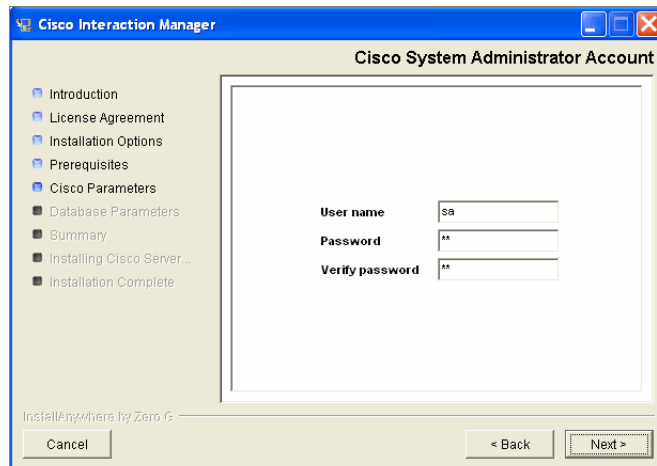
1. Follow Steps 1–3 in “To install a single-server configuration” on page 29.
2. In the Installation Options window, select the **Database** option.



Installation Options window

Cisco Interaction Manager has two distinct areas: the system area and the partition (or business) area. An administrator type user is created for each area during the installation. In the next two windows, you will be asked for user names and passwords for these two users:

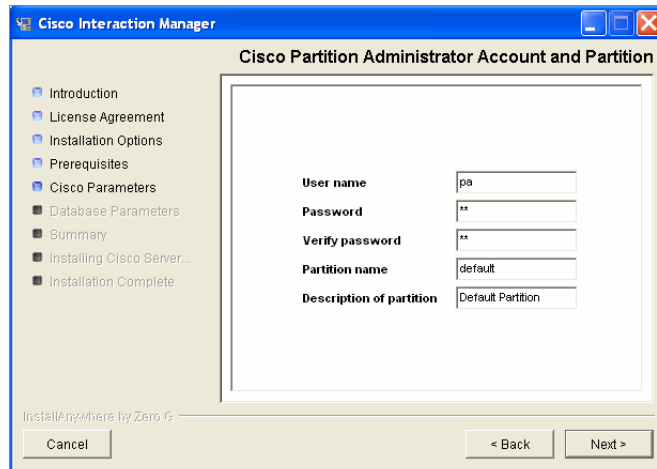
- ▶ System Administrator
 - ▶ Partition Administrator
3. Type a user name and password for the system administrator.



Cisco System Administrator Account window

4. In the Cisco Partition Administrator Account and Partition window, provide the following details.
- Type a user name for the partition administrator.

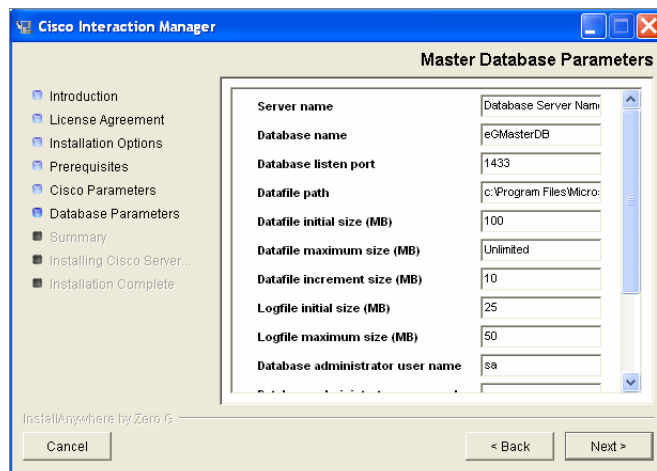
- Type a password for the partition administrator.
- Provide a name for the partition. This name will be part of the URL that users will use to log in to Cisco Interaction Manager:
`http://CIM/Partition_Name`. Make sure that the name does not contain any spaces.
- Provide a description for the partition.



Cisco Partition Administrator Account and Partition window

5. In the Master Database Parameters window provide the following details.
 - Server name: Name of the local or remote server on which you want to install MSSQL database.
 - Database name: Name of the master database. The installation program creates a database with the name you type here.
 - Database listener port: MSSQL server port number.
 - Datafile path: Path to the Data folder on the database server. For example, `MSSQL_Home\MSSQL\Data`.
 - Datafile initial size (MB): Minimum datafile size for the database.
 - Datafile maximum size (MB): Maximum datafile size for the database.
 - Datafile increment size (MB): Additional file size limit that will be allocated to a database object after the initial size is full.
 - Logfile initial size (MB): Minimum logfile size for log entries.
 - Logfile maximum size (MB): Maximum logfile size for log entries.
 - Database administrator user name: User name of the database administrator for MSSQL Server.
 - Database administrator password: Password of the database administrator.

- Cisco Database user name: User name required for connecting to the Cisco Interaction Manager master database. The installation program creates the database and its user.
- Cisco Database password: Password for the Cisco Interaction Manager master database user.



Type master database parameters

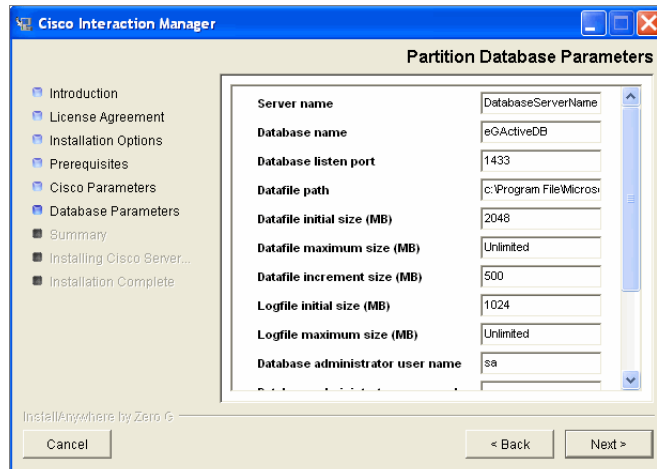
6. In the Partition Database Parameters window, provide the following details.



Important: Partition database should be created on the same database server as the master database.

- Server name: Name of the local or remote server on which your MSSQL database is installed.
- Database name: Name of the partition database. The installation program creates a database with the name you type here.
- Database listener port: MSSQL server port number.
- Datafile path: Path to the Data folder on the database server. For example, *MSSQL_Home\MSSQL\Data*.
- Datafile initial size (MB): Minimum datafile size for the database.
- Datafile maximum size (MB): Maximum datafile size for the database.
- Datafile increment size (MB): Additional file size limit that will be allocated to a database object after the initial size is full.
- Logfile initial size (MB): Minimum logfile size for log entries.
- Logfile maximum size (MB): Maximum logfile size for log entries.
- Database administrator user name: User name of the database administrator for MSSQL Server.

- Database administrator password: Password of the database administrator.
- Cisco Database user name: User name required for connecting to the Cisco Interaction Manager database. The installation program creates the database and its user.
- Cisco Database password: Password for the Cisco Interaction Manager database user.



Type partition database parameters

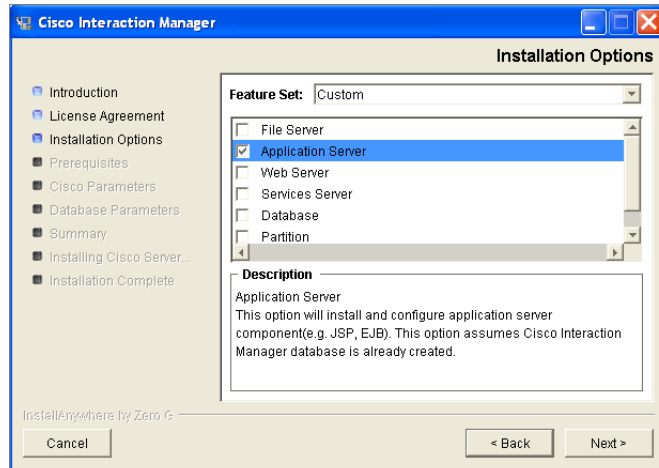
7. Review the information displayed in the Summary window, and click **Install**.
8. In the Install Complete window, click the **Finish** button to complete the installation process.

Installing primary Application Server

In this section, we describe the process of creating the Application Server.

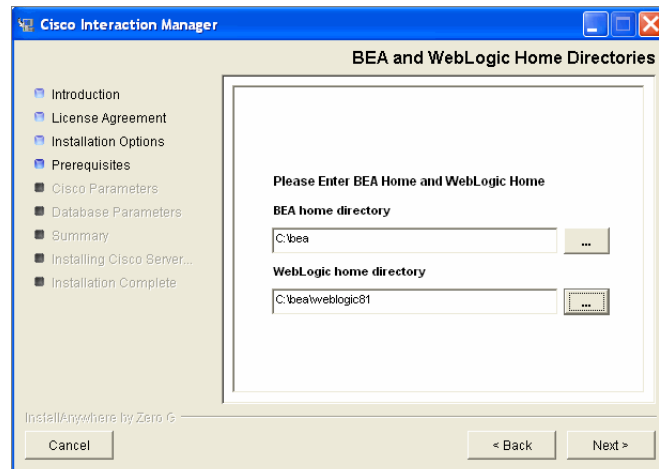
To install the Application Server

1. Follow Steps 1–3 in “To install a single-server configuration” on page 29.
2. In the Installation Options window, select the **Application Server** option.



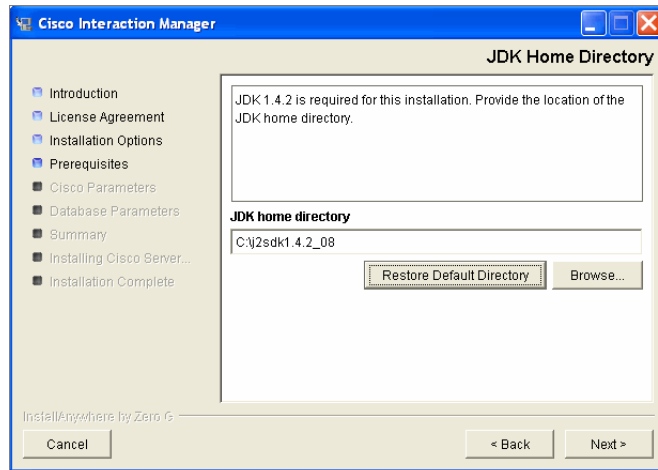
Installation Options window

3. Type the path or browse to the BEA and WebLogic home directories.



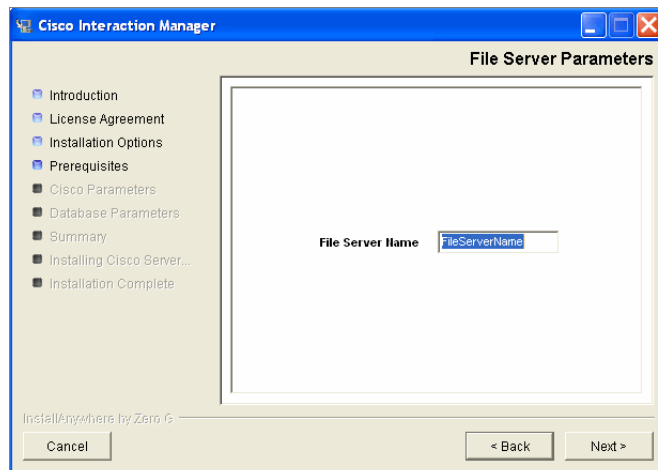
BEA and WebLogic Home Directories window

4. Type the path to or browse to the JDK home directory.



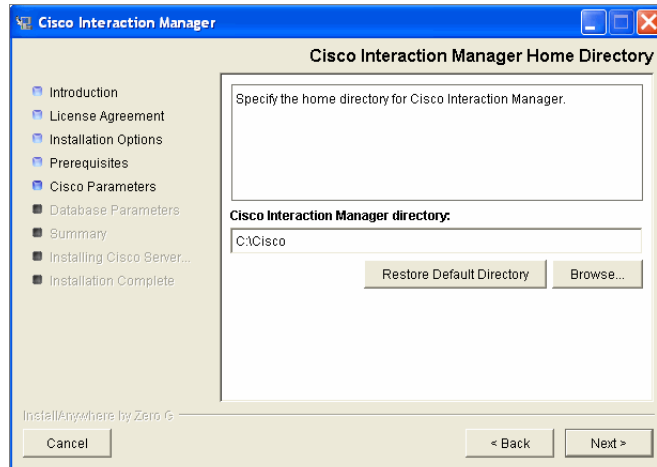
JDK Home Directory window

5. Type the name of the File Server.



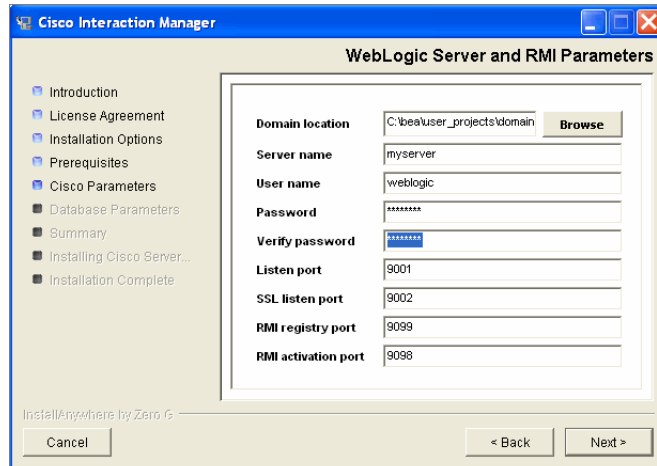
File Server Parameters window

6. Type the path to or browse to the folder where you would like to install Cisco Interaction Manager Application Server.



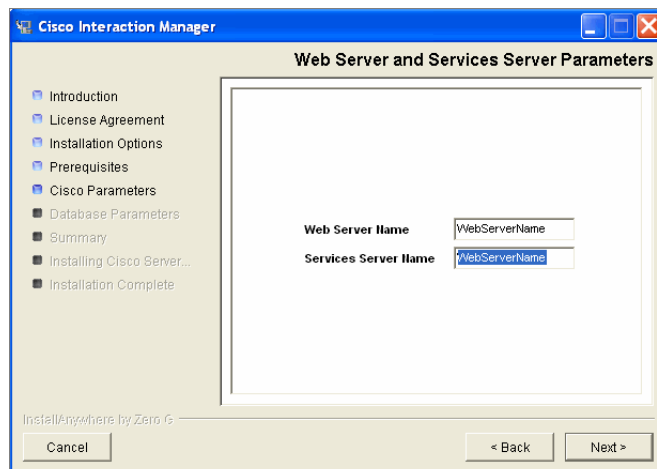
Cisco Interaction Manager Home Directory window

7. In the WebLogic Server and RMI Parameters window, provide the following details.
 - Domain location: Location of the WebLogic domain you configured on page 17.
 - Server name: Name of your WebLogic server (page 17). The default name is myserver.
 - User name: User name of the WebLogic system user (page 17), required to access the WebLogic Server Administration Console.
 - Password: Password for the WebLogic system user (page 17).
 - Listen port: Port number of the WebLogic server.
 - SSL listen port: WebLogic Secure Socket Layer Listen port number.
 - RMI registry port: Port number used by the RMI registry naming service.
 - RMI activation port: Port number used by the RMI Daemon Process.



WebLogic Server and RMI Parameters window

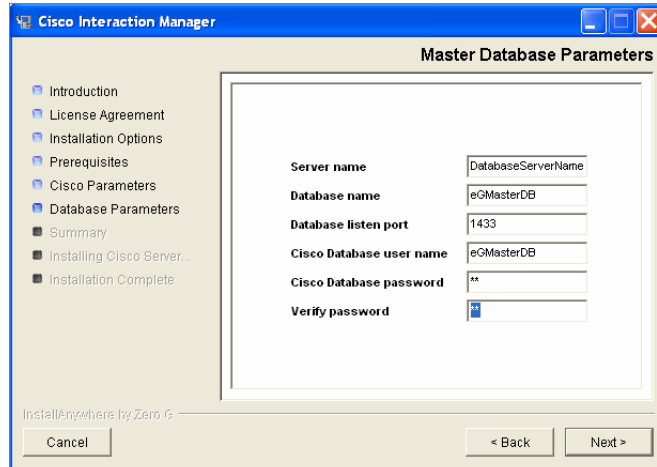
8. In the Web Server and Services Server Parameters window, type the Web Server and Services Server names.



Web Server and Services Server Parameters window

9. In the Master Database Parameters window, provide the following details.
 - Server name: Name of the local or remote server on which your MSSQL database is installed.
 - Database name: Name of the master database.
 - Database listen port: MSSQL server port number.
 - Cisco Database user name: User name for the Cisco Interaction Manager master database.

10. Cisco Database password: Password for the Cisco Interaction Manager master database user.



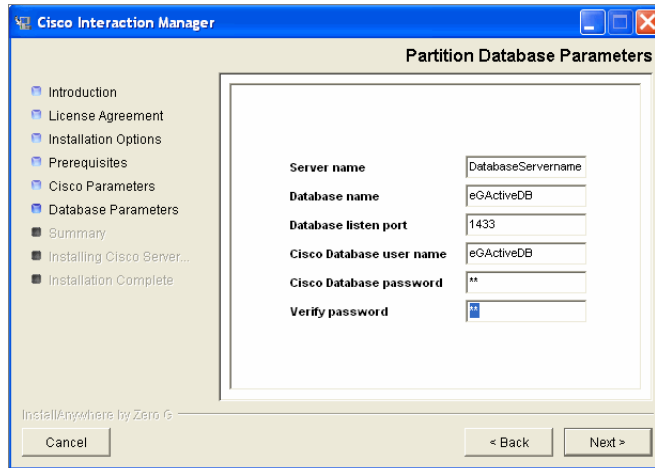
Master Database Parameters window

11. In the Partition Database Parameters window, provide the following details.



Important: Partition database should be created on the same database server as the master database.

- Server name: Name of the local or remote server on which your MSSQL database is installed.
- Database name: Name of the partition database.
- Database listen port: MSSQL server port number.
- Cisco Database user name: User name of the Cisco Interaction Manager database.
- Cisco Database password: Password for the Cisco Interaction Manager database user.



Partition Database Parameters window

12. Review the information displayed in the Summary window, and click **Install**.
13. In the Installation Complete window, click **Finish** to complete the installation process.

Installing secondary Application Servers

You can install secondary Application Servers, following the steps detailed in this section. You will need to create a new WebLogic domain on a different server because the secondary server cannot share the WebLogic domain or server of the primary Application and Web Servers.

Backing up web.xml file



Important: Before installing the secondary Application Server, make sure you take a backup of the web.xml file.

To take a backup of the web.xml file

1. On the File Server browse to the Cisco Interaction Manager home directory.
2. Then browse to the web-inf > web.xml file.
3. Rename web.xml to web.xml.org.

Installing Server

To install a secondary Application Server

1. First, create a WebLogic domain. For details see “Creating WebLogic domains” on page 17.



Important: WebLogic domain name and server name should be different than those of the primary Application Server.

2. Then, follow the steps from page 41. In step 10 on page 45 make sure you give the following values.
 - Domain location: The domain location should be different than the one given for the primary Application Server.
 - Server name: The server name should be different than the one given for the primary Application Server.
 - Listen port: The port number should be the same as the one given for the primary Application Server.

Restoring web.xml file



Important: After installing the secondary Application Server, make sure you restore the web.xml file.

To restore the web.xml file

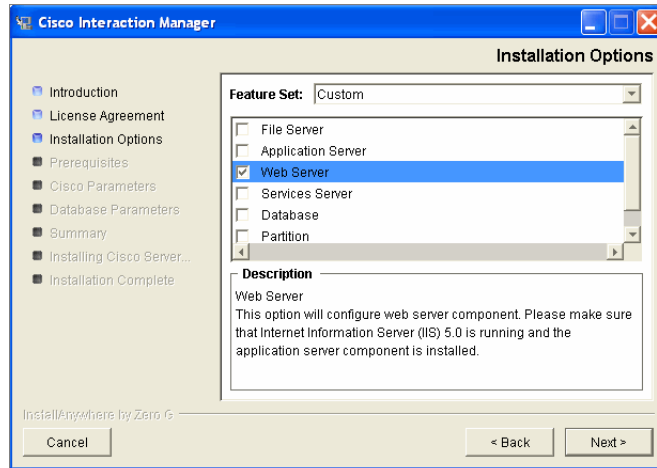
1. On the File Server browse to the Cisco Interaction Manager home directory.
2. Then browse to the web-inf > web.xml.org file.
3. Rename web.xml.org to web.xml, and restart the Cisco Interaction Manager application.

Installing Web Server

In this section, we describe the process of creating the Web Server.

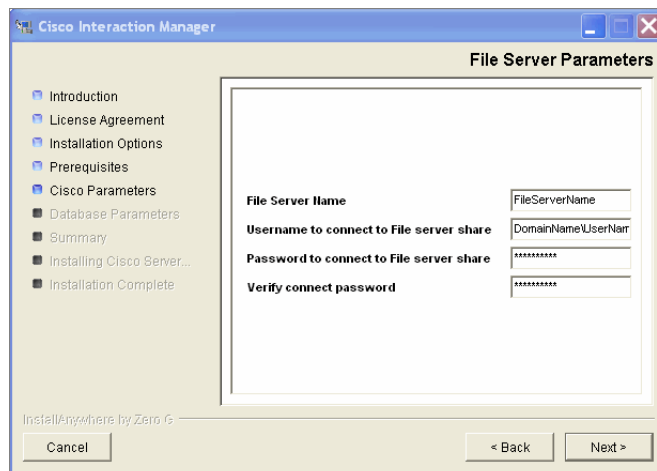
To install the Web Server

1. Follow Steps 1–3 in “To install a single-server configuration” on page 29.
2. In the Installation Options window, select the **Web Server** option.



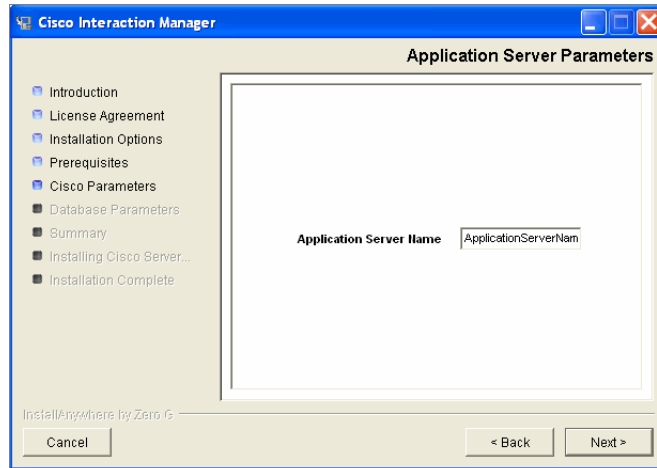
Installation Options window

3. In the File Server Parameters window, provide the following details.
 - File Server name: Name of the File Server.
 - User name to connect to File server share: Type the user name to connect to the File Server share. The user name is the domain name of the user account created exclusively for Cisco Interaction Manager.
 - Password to connect to File server share: Password for the user.



File Server Parameters window

4. In the Application Server Parameters window, type the name of the Application Server name for which you want to configure the Web Server.



Application Server Parameters window

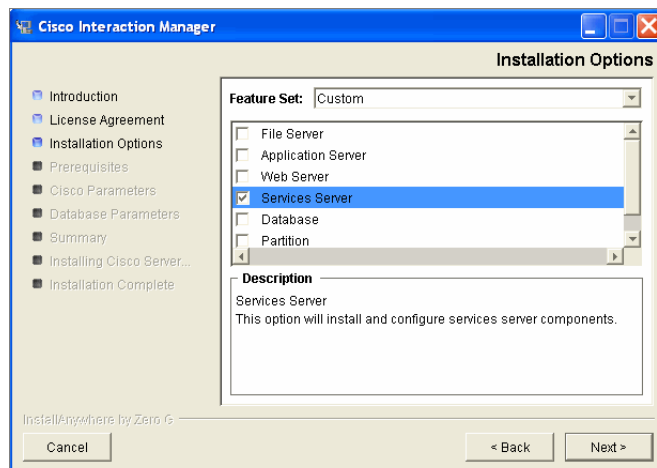
5. Review the information displayed in the Summary window, and click **Install**.
6. In the Installation Complete window, click **Finish** to complete the installation process.

Installing Services Server

In this section, we describe the process of creating the Services Server.

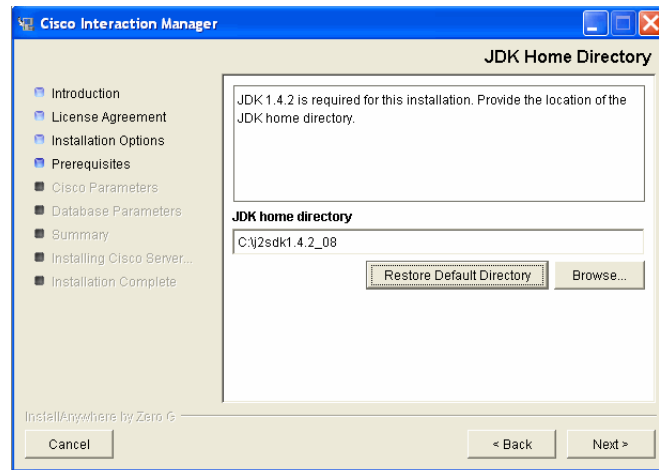
To install the Services Server

1. Follow Steps 1–3 in “To install a single-server configuration” on page 29.
2. In the Installation Options window, select the **Services Server** option.



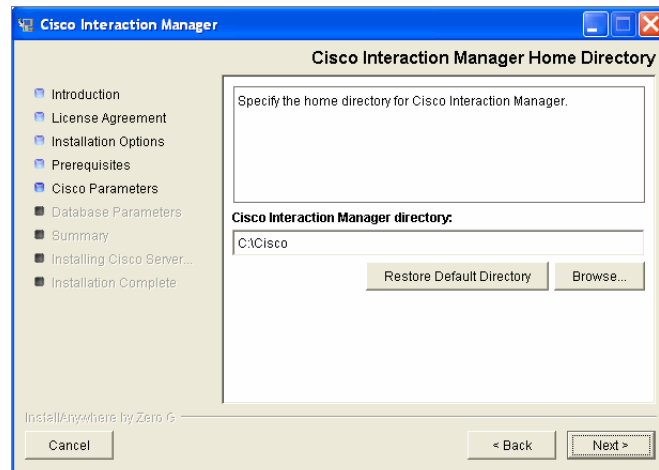
Installation Options window

3. Type the path or browse to the JDK home directory.



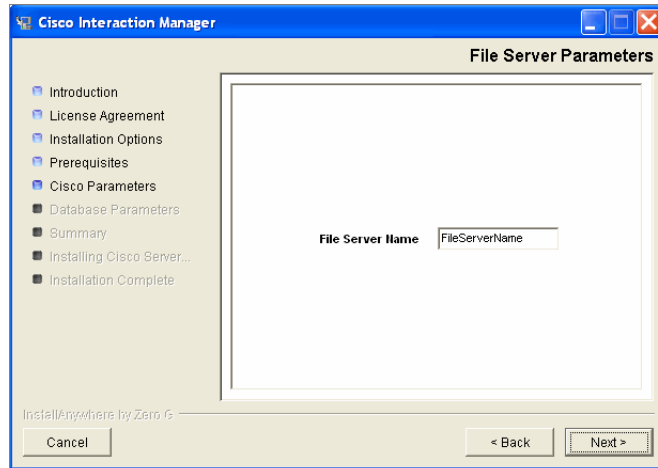
JDK Home Directory window

4. Type the path to or browse to the folder where you would like to install the Services Server.



Cisco Interaction Manager Home Directory window

5. Type the name of the File Server.



File Server Parameters window

6. Review the information displayed in the Summary window, and click **Install**.
7. In the Installation Complete window, click **Finish** to complete the installation process.
8. Go to “Post-installation tasks” on page 53, and perform the post-installation procedures described there. If you need to install an additional partition before that, go to “Additional partitions” on page 67.

4 Post-installation tasks

- ▶ [Setting up archives for partition databases](#)
- ▶ [Copying license files](#)
- ▶ [Verifying configuration of File Server](#)
- ▶ [Verifying configuration of Application Servers](#)
- ▶ [Applying updates](#)
- ▶ [Separating the Web Server from the Application Server](#)
- ▶ [Changing Web Server settings](#)
- ▶ [Changing IIS configuration settings](#)
- ▶ [Starting Cisco Interaction Manager](#)
- ▶ [Configuring some important settings](#)
- ▶ [Uninstalling Cisco Interaction Manager](#)

This chapter guides you through the tasks to be performed after installing the system. It also describe the process of uninstalling Cisco Interaction Manager.

Setting up archives for partition databases

It is important to set up an archive for each partition database to keep the size of the database manageable and to avoid performance issues that could appear later.

See “Setting up the archive for a partition” on page 74 for details of the installation procedure.

Copying license files

To copy the license files

- ▶ For each partition, copy the license files provided by Cisco to the following location: *CIM_Home\config\license*.

Verifying configuration of File Server

During the configuration of File Server, in some cases, installer is not able to generate web.xml file properly. To confirm that the file has been generated properly, check the following.

To verify the configuration of File Server

1. On the File Server browse, to the Cisco home directory. In the web-inf folder, locate the following two files.
 - web.xml
 - weblogic.xml
2. In addition to these two files, if there is an additional file, *web_weblogic.xml*, then delete the *web.xml* file and rename *web_weblogic.xml* file to *web.xml*.

Verifying configuration of Application Servers

On the Application Server, you need to check the `weblogic.jar` and BEA licence files.

You need to perform the following steps on the primary Application Server and all the secondary Application Servers.

To verify the configuration of Application Server

1. Go to the location `BEA_Home\weblogic81\server\lib\` and locate the following two files.
 - `weblogic.jar_orig`
 - `weblogic.jar`
2. If the file `weblogic.jar_orig` doesn't exist, then rename the file `weblogic.jar` to `weblogic.jar_orig`.
3. Now, from the location, `PL_Home\lib\ext\platform\`, copy the file `weblogic.jar` and paste it at the location, `BEA_Home\weblogic81\server\lib`.
4. Next, go to the location `BEA_Home`, and open the file `license.bea`.

This file should have the following two entries:

```
expiration="never"
```

```
type="ISV"
```

5. If these entries do not exist, then copy the file `license_isv.bea` from the location, `CIM_Home\config\` and paste it at location, `BEA_Home`.
6. Go the DOS prompt from the `BEA_Home` location, and run the following command.

```
UpdateLicense.cmd license_isv.bea
```

Applying updates

To apply the updates

1. Verify that Cisco Interaction Manager is stopped.
2. Open the `Updates` folder in the Application CD.
3. Apply all the updates based on instructions in the accompanying `ReadMe` file.

Separating the Web Server from the Application Server

To separate the Web Server from the Application Server you need to add the IP address of the Web Server in the Master and Active databases.

To verify the IP address

- ▶ You can verify the IP address by running the following query on the master and active databases.

```
SELECT SETTING_ACT_VAL FROM EGPL_PREF_GLOBALSETTINGS  
WHERE SETTING_NAME = 'Common.messaging.applethost'
```

To change the IP address

Table name: EGPL_PREF_GLOBALSETTINGS

Setting name: Common.messaging.applethost

- ▶ Set the SETTING_ACT_VAL to IP address of the Web Server.

Changing Web Server settings

Configuring content expiration settings

As part of the post-install procedure, you can configure the content expiration of cache pages in your Web Server. By doing so, the browser compares the current date with the expiration date that you have set to determine whether to display a cached page, or request an updated page from the server. We recommend you set the expiration to 365 days for optimum performance.



Important: You must set this option for all partitions, including the System Partition.

To configure content expiration

1. Go to **Start > Programs > Administrative Tools > Internet Services Manager**.
2. In the **Default Web Site** node, right-click **System** and select the **Properties** option.

3. In the System Properties window, go to the **HTTP Headers** section. Select the **Enable Content Expiration** option. Select the Expire after option and enter **365** in the text box. By default it is calculated in days. Click **OK**.

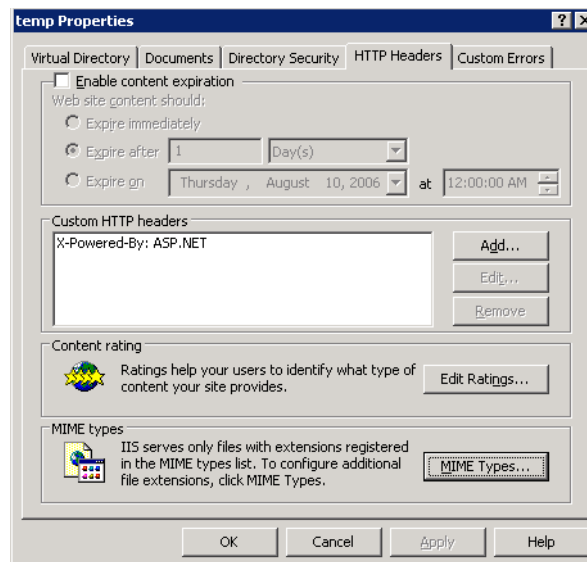
Configuring access for attachments without extensions

To allow access to attachments that have no extension, you need to configure following changes from the IIS Manager.

To configure access for attachments without extensions

1. Open the Internet Information Services (IIS) Manager.
2. In the **Default Web Site** directory select the **temp** virtual directory.
3. Right click the **temp** virtual directory and select **Properties**.

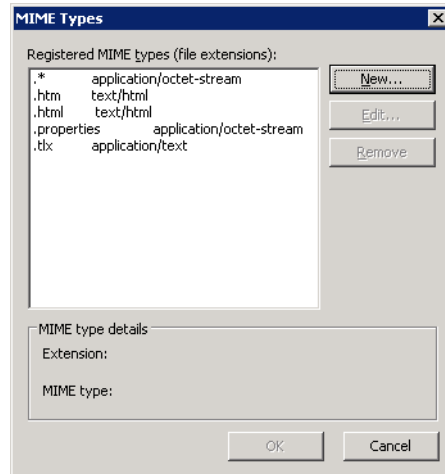
The temp Properties window opens.



temp Properties window

4. In the temp Properties window go to the **HTTP Headers** tab and click the **MIME types** button.

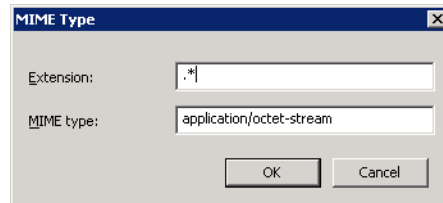
The MIME Types window appears.



MIME Types window

5. In the MIME Types window click the **New** button.

The MIME Type window appears.



MIME Type window

6. In the MIME Type window provide the following details and click the **OK** button.
 - **Extension:** Type the extension as `.*`.
 - **MIME type:** Type the MIME type as `application/octet-stream`.
7. In the temp Properties window, click the **Apply** button.

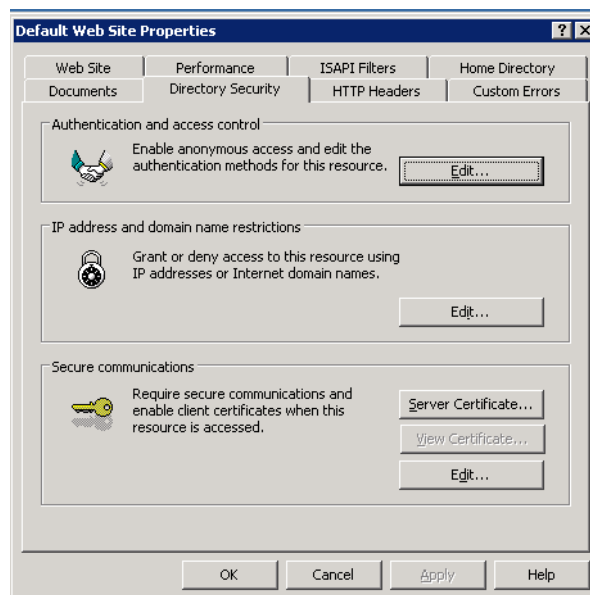
Changing IIS configuration settings

Changing authentication settings for web site

You need to change the authentication settings for the web site only when the Application Server and Web Server are configured on two different machines.

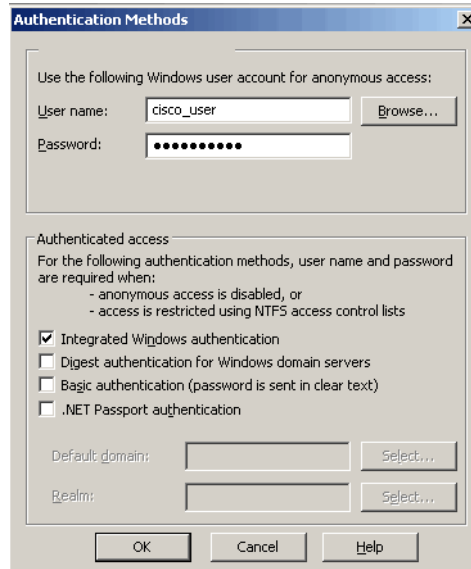
To change web site authentication settings

1. Go to **Start > Programs > Administration Tools > Internet Information Services (IIS) Manager**.
2. Browse to **Web Sites > Default Web Site**.
3. Right click on **Default Web Site** and select **Properties**.
4. In the Default Web Site Properties window go to **Directory Security** tab.



Default Web Site Properties window

5. In the **Authentication and access control** section click the **Edit** button.
6. In the Authentication Details window change the authentication details from internet user account to domain user account.



Authentication Methods window

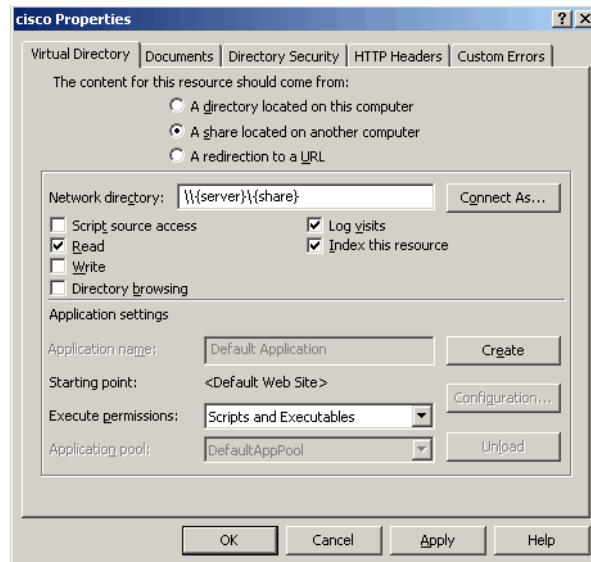
7. Click the **OK** button to close the window.

Changing security credentials for network directory

You need to change the network directory security for each Cisco Interaction Manager virtual directory. These steps are required when Application Server and Web Server are configured on the same machine, and the File Server is configured on a different machine. You need to follow these steps for each partition.

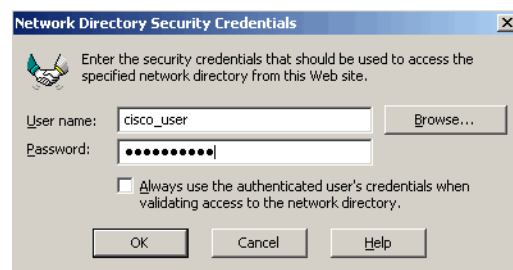
To change the network directory security settings

1. Go to **Start > Programs > Administration Tools > Internet Information Services (IIS) Manager**.
2. Browse to **Web Sites > Default Web Site**.
3. Right click on the Cisco virtual directory and select **Properties**.
4. In the virtual directory properties window go to **Virtual Directories** tab.



Cisco Properties window

5. In the section **The content for this resource should Come from:** select the option **A share located on another computer.**
6. Provide the **Network directory** name and click the **Connect As** button.
7. In the Network Directory Security Credentials window, clear the option **Always use the authenticated user's credentials when validating access to the network directory** and provide the user name and password of the domain user.



Network Directory Security Credentials window

8. Click **OK** to close the window.
- Repeat these steps for all the Cisco Interaction Manager virtual directories.

Starting Cisco Interaction Manager

To start Cisco Interaction Manager after completing the installation process

1. Carry out the following tasks for security reasons:
 - a. On the Web Server, remove execute permission from the virtual directory `temp`.
 - b. On the Application Server in a distributed installation, remove permissions to everyone from the `cisco` share.
 - c. Give full control to the domain user account that you had created earlier for Cisco Interaction Manager services.
2. If Cisco Interaction Manager is installed as a Windows service, change logon parameters for the domain user on both the Application and Services Servers:
 - a. Go to **Start > Settings > Control Panel > Administrative Tools > Services**.
 - b. In the Services window, locate the Cisco Interaction Manager service and double-click it.
 - c. In the Properties window, under the **Log On** tab, change the logon parameters to the domain user.
 - d. Start the services using the domain user account.
3. Remove the extension mapping for the `temp` virtual directory created by the installation program:
 - a. Go to **Start > Settings > Control Panel > Administrative Tools > Internet Information Services**.
 - b. Under **Default Web Site**, browse to the `temp` directory. Right-click to open its Properties window.
 - c. Click the **Create** button.
 - d. Click the **Configuration...** button.
 - e. Remove mapping for the following extensions, if they exist: `.jsp` and `.asp`. Click **OK**.
 - f. Now, click the **Remove** button. Click **OK**.
 - g. Restart IIS.
4. In the NT Services panel, start Cisco Service to start all Cisco Interaction Manager services.

Logging in to the business partition

The System partition as well as the first business partition are created during the installation.

To log in to the business partition

1. Type the URL `http://Web_Server/Partition_Virtual_Directory` in your browser, where *Web_Server* is your Web Server and *Partition_Virtual_Directory* is the virtual directory created for this partition.

During the installation, you are prompted to provide the virtual site name in the Partition Administrator Account and Partition window.

2. In the Login window, type the user name and password you had set up for the partition administrator in the Partition Administrator Login Parameters window during the installation. Click the **Log In** button.

Launching Cisco Interaction Manager from Cisco Agent Desktop Embedded Browser

This release of Cisco Interaction Manager can be used with two browsers:

- ▶ Microsoft Internet Explorer
- ▶ Cisco Agent Desktop

See CAD documentation for details about configuring a new task button in CAD to launch Cisco Interaction Manager using a URL. The URL is `http://Web_Server/Partition_Virtual_Directory`.

Make sure that Cisco Interaction Manager is configured to run in its own browser tab, uninterrupted by other browser applications.

Configuring some important settings

Settings allow you to configure various aspects of Cisco Interaction Manager. Some settings are configured at the partition level, while others have to be set up for each department.

In this section, we describe certain settings that should be configured soon after installation. These settings are of three types:

1. Mandatory settings that must be configured.
2. Settings related to using ESMTP protocol, which must be configured if you are using ESMTP protocol for exception and spam emails and notifications.

3. Important non-mandatory settings that you should configure before using Cisco Interaction Manager.

Settings that must be configured

Make sure you configure the following settings for each partition.

At the partition level

- ▶ Default SMTP server
- ▶ Notifications mail SMTP Server
- ▶ Notifications mail redirection from address
- ▶ Notifications mail redirection to address

At the department level

Configure the following setting for each department.

- ▶ Default From address for alarm

ESMTP settings

Configure these partition-level settings only if you use ESMTP protocol for exception and spam emails and notifications.

- ▶ Exception mails SMTP user name
- ▶ Exception mails SMTP password
- ▶ SPAM mails SMTP user name
- ▶ SPAM mails SMTP password
- ▶ Notification mails SMTP user name
- ▶ Notification mails SMTP password

Recommended settings

Although these settings are not required it is recommended that you configure them to your business needs.

At the partition level

- ▶ Exception email SMTP

- ▶ Exception mail redirection to address
- ▶ Exception mail redirection from address
- ▶ SPAM mail SMTP Server
- ▶ SPAM mail redirection from address
- ▶ SPAM mail redirection to address
- ▶ Customer departmentalization

At the department level

- ▶ Business calendar time zone

Optional settings

Although it is not mandatory to change these settings, you are likely to feel the need to configure them for your business.

At the partition level

- ▶ Expiry time for auto pushback
- ▶ Inactive time out
- ▶ Deletion time out

Uninstalling Cisco Interaction Manager

To uninstall Cisco Interaction Manager

1. Go to **Start > Settings > Control Panel**.
2. Double-click **Add/Remove Programs**.
3. From the list of currently installed programs, select **Cisco Interaction Manager** and click **Remove**. Follow the instructions to uninstall Cisco Interaction Manager.

By default, the program does not uninstall the following:

- Database
- Storage folder on the file system.

This ensures that your critical data is never lost.

4. Go to the SQL Enterprise Manager and delete the database manually, if required.



Additional partitions

- ▶ [About partitions](#)
- ▶ [Verifying prerequisites](#)
- ▶ [Installing a new business partition](#)

The System partition and the first business partition are installed by default. You can create additional business partitions with the installation program. This chapter describes the procedure for installing and configuring a new business partition.

About partitions

As Cisco Interaction Manager is designed for enterprise-wide deployments, a single installation can be used by various independent or semi-independent business units in an organization. You can easily set up Cisco Interaction Manager to mirror the structure of your business.

An Cisco Interaction Manager installation can have one or more business partitions, which are meant to be used as independent units. While the hardware and software is common for all partitions, system resources and business objects are stored and managed separately for each partition. Partitions are ideal for organizations where business units (or clients, in the case of an outsourced services provider) do not need to share customer, interaction, or product information.

The installation program creates the System partition and a single-department business partition. You can create additional business partitions by using the installation program. Create additional partitions if you:

- ▶ Want complete segregation of data between business units in your enterprise.
- ▶ Are an outsourcing or application service provider, and want to serve multiple customers from a single installation.

Verifying prerequisites

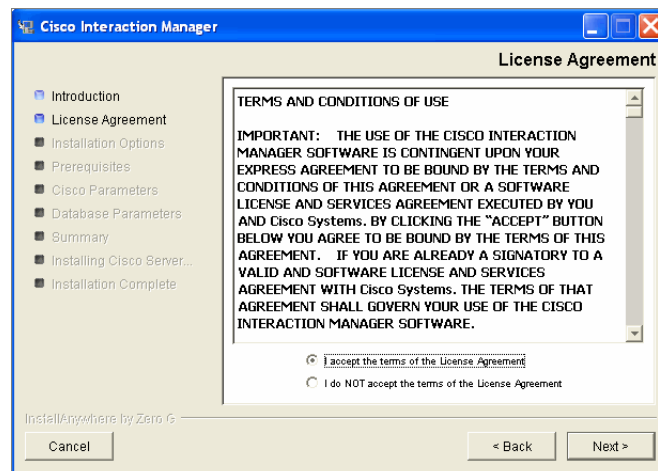
Complete the following tasks before beginning to install an additional partition.

1. Ensure that WebLogic and RMID services for the first partition are running before installing the new partition.
2. Ensure that the application is installed properly.
3. Ensure that Cisco Interaction Manager is installed and running for the default partition.

Installing a new business partition

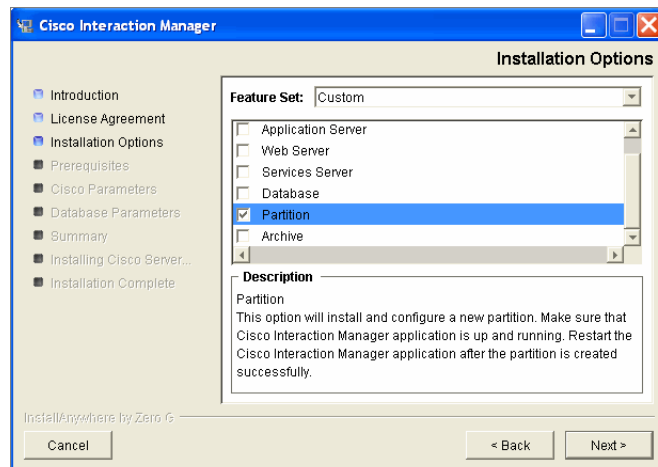
To create a new business partition

1. On the File Server, run `Setup.exe` from the Application CD.
2. In the Introduction window read the installation instructions.
3. Review the license agreement and select the **I accept the terms of the License Agreement** option.



License Agreement window

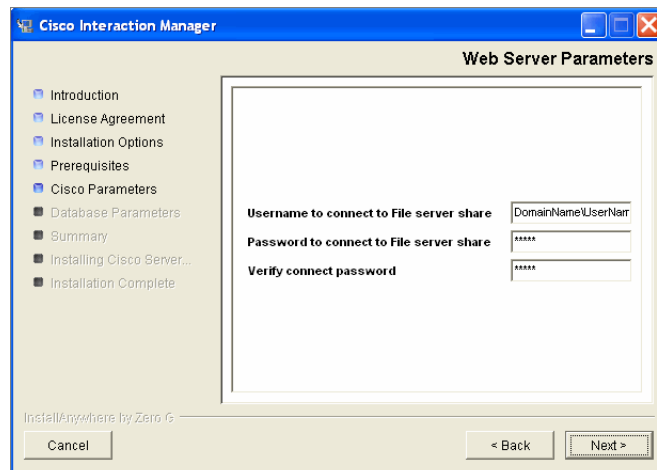
4. In the Installation Options window, select the **Partition** option.



Installation Options window

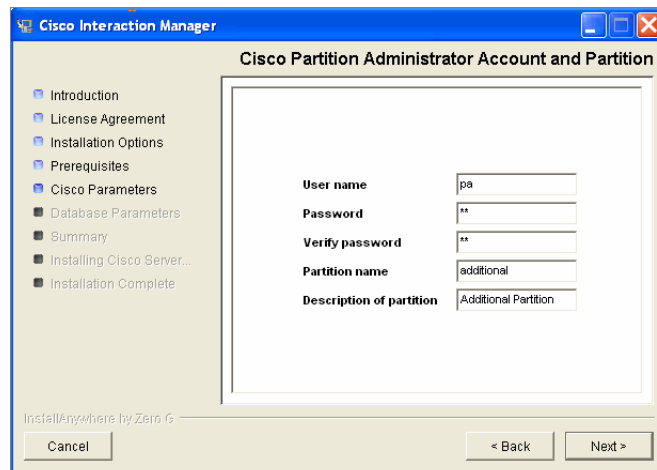
5. In the Web Server Parameters window, provide the following information.

- User name to connect to File server share: Type the user name to connect to File Server share. The user name is the domain name of the user account created exclusively for Cisco Interaction Manager. For details, see “Setting up user accounts and permissions” on page 17.
- Password to connect to File server share: Type the password to connect to File Server share.



Web Server Parameters window

6. In the Partition Administrator Account and Partition window provide the following details.
 - a. Type a user name for the Partition Administrator.
 - b. Type a password for the Partition Administrator.
 - c. Provide a name for the partition. This name will be part of the URL that users will use to log in to Cisco Interaction Manager:
http://CIM_Home/Partition_Name Make sure that the name does not contain any spaces.
 - d. Provide a description for the partition.



Partition Administrator Account and Partition window

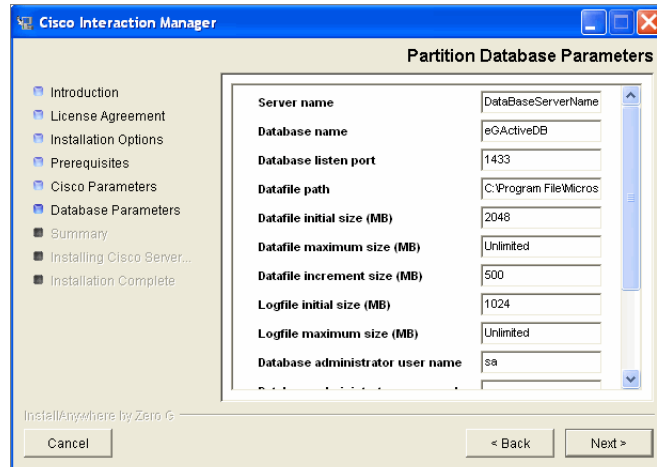
7. In the Partition Database Parameters window provide the following details.



Important: Partition database should be created on the same database server as the master database.

- Server name: Name of the local or remote server on which your MSSQL database is installed.
- Database name: Name of the master database. The installation program creates a database with the name you type here.
- Database listener port: MSSQL server port number.
- Datafile path: Path to the `Data` folder on the database server. For example, `MSSQL_Home\MSSQL\Data`.
- Datafile initial size (MB): Minimum datafile size for the database.
- Datafile maximum size (MB): Maximum datafile size for the database.
- Datafile increment size (MB): Additional file size limit that will be allocated to a database object after the initial size is full.
- Logfile initial size (MB): Minimum logfile size for log entries.
- Logfile maximum size (MB): Maximum logfile size for log entries.
- Database administrator user name: User name of the database administrator for MSSQL Server.
- Database administrator password: Password of the database administrator.
- Cisco Database user name: User name required for connecting to the Cisco Interaction Manager database. The installation program creates the database and its user.

- Cisco Database password: Password for the Cisco Interaction Manager database user.



Type partition database parameters

8. Review the information displayed in the Summary window, and click **Install**.
9. In the Install Complete window, click **Finish** to complete the installation process.

6 Archives

- ▶ [About archives](#)
- ▶ [Setting up the archive for a partition](#)

About archives

Data is stored in the active database. With time, the size of the data usually increases to a point where it begins to affect the performance of the system. Hence, it is important that data that is not in use anymore is stored somewhere other than the active database.

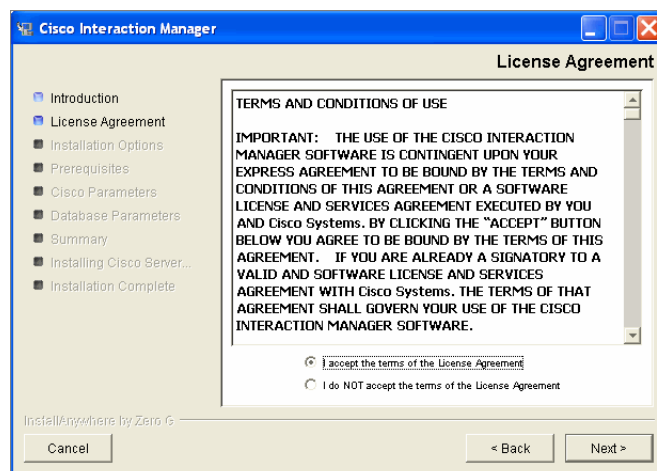
Archiving is a systematic process which moves the data from the active database to the archive database. Periodic archiving helps to keep the size of the active database within prescribed levels, thereby improving the performance of the system.

Archives can be set up for all partitions except the system partition. The application's installation program helps you install archives. You can install them while installing the application or creating a new partition. You can also choose them later—in that case, make sure that the File Server is properly installed.

Setting up the archive for a partition

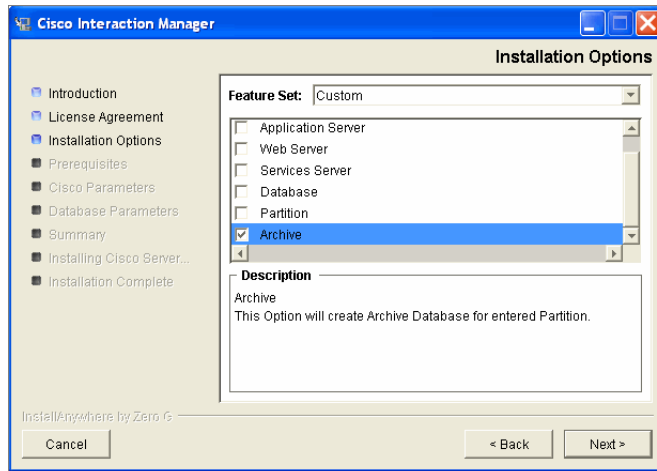
To set up the archive

1. On the File Server, run `Setup.exe` from the Application CD.
2. In the Introduction window read the installation instructions.
3. Review the license agreement and select the **I accept the terms of the License Agreement** option.



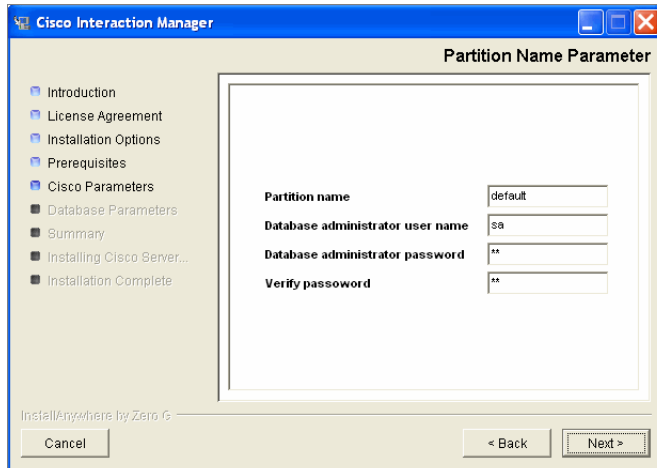
License Agreement window

4. In the Installation Options window, select the **Archive** option.



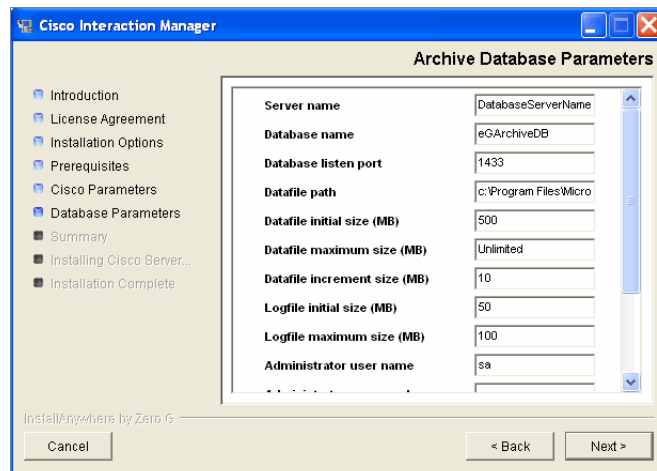
Installation Options window

5. In the Partition Name Parameter window provide the following details.
 - Partition name: Name of the partition for which you want to create the archive database.
 - Database administrator user name: User name of the partition database administrator for MSSQL server.
 - Database administrator password: Password of the partition database administrator.



Partition Name Parameter window

6. In the Archive Database Parameters window provide the following details:
 - Server name: Name of the local or remote MSSQL database server on which your archive database will be installed.
 - Database name: Name of the archive database. The installation program creates a database with the name you type here.
 - Database listener port: MSSQL server port number.
 - Datafile path: Path to the `Data` folder on the database server. For example, `MSSQL_Home\MSSQL\Data`.
 - Datafile initial size (MB): Minimum datafile size for the database.
 - Datafile maximum size (MB): Maximum datafile size for the database.
 - Datafile increment size (MB): Additional file size limit that will be allocated to a database object after the initial size is full.
 - Logfile initial size (MB): Minimum logfile size for log entries.
 - Logfile maximum size (MB): Maximum logfile size for log entries.
 - Administrator user name: The user name of the archive database administrator for MSSQL Server.
 - Administrator password: Password of the archive database administrator.
 - Cisco Database user name: User name required for connecting to the archive database.
 - Cisco Database password: Password for the archive database user.



Archive Database Parameters window

7. Review the information displayed in the **Summary** window, and click **Install**.
8. In the Install Complete window, click **Finish** to complete the installation process.

7

SSL for secure connections

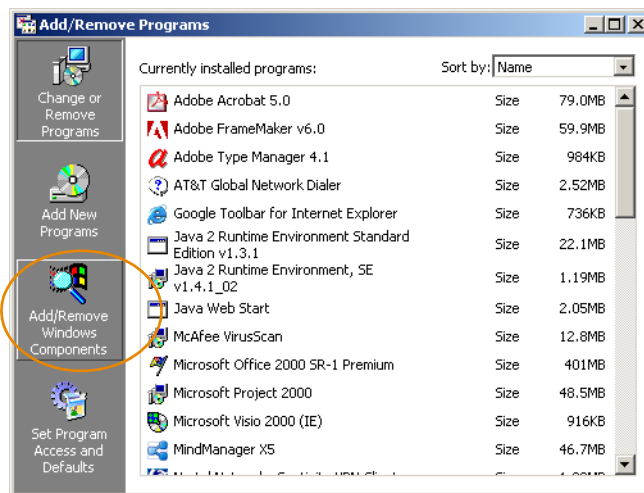
- ▶ [Installing Microsoft Certificate Services](#)
- ▶ [Installing a security certificate](#)
- ▶ [Configuring SSL access](#)
- ▶ [Configuring the viewing of attachments](#)
- ▶ [Testing SSL access](#)

Secure Sockets Layer (SSL) is widely used to create a secure communication channel between web browsers and servers. You can set up SSL for more secure connections to your Cisco Interaction Manager installation by following the procedures described in this chapter.

Installing Microsoft Certificate Services

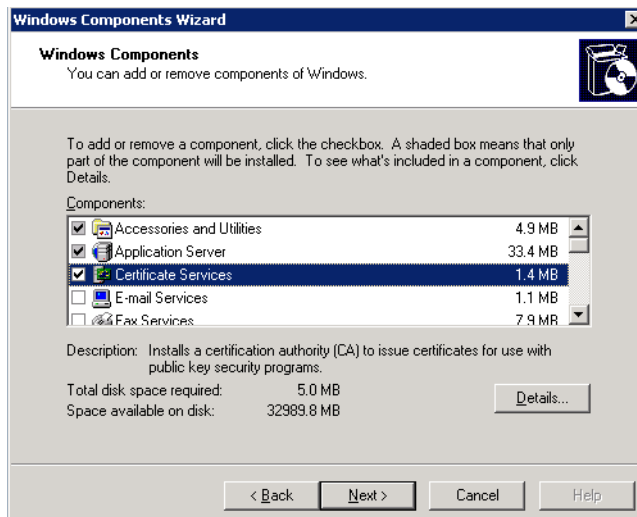
To install Microsoft Certificate Services

1. Go to **Start > Settings > Control Panel**.
2. Double-click **Add/Remove Programs**.
3. In the Add/Remove Programs window, click the **Add/Remove Windows Components** button.



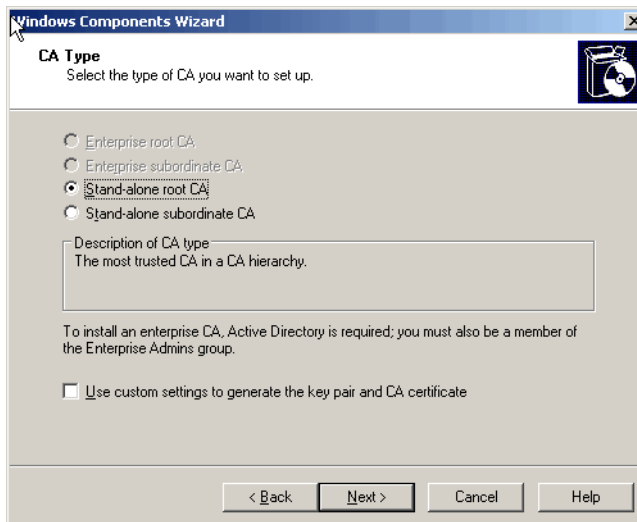
Click the Add/Remove Components button on the Add/Remove Programs window

4. In the Windows Components window, select the **Certificate Services** option. Click **Yes**, and then **Next**.



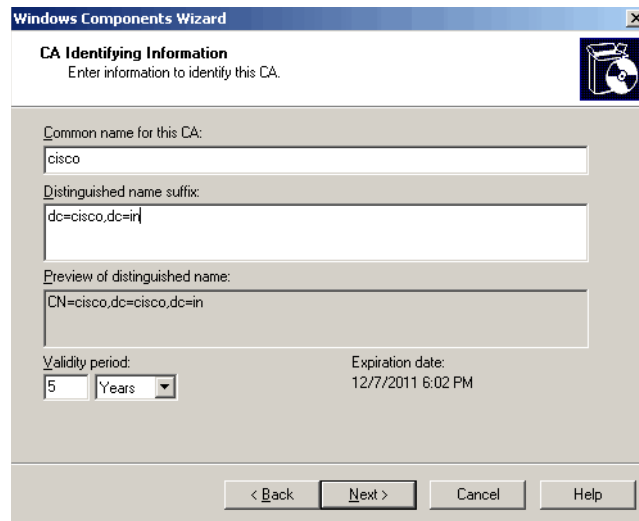
Windows Components window

5. In the CA type window select the **Standalone Root CA** option. Click **Next**.



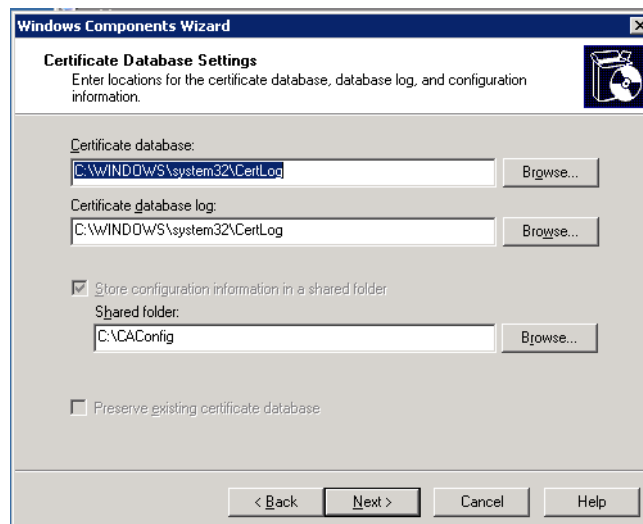
CA Type window

6. In the CA Identifying Information window, provide the details of the CA certificate.



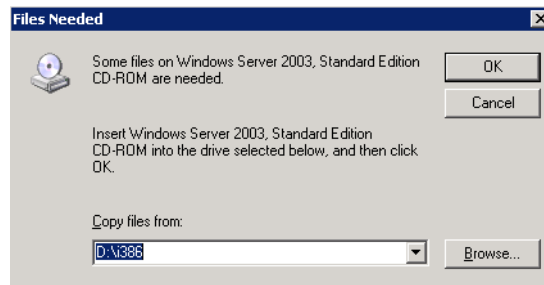
Provide CA identification information

7. In the Certificate Database Settings window, provide the location of the certificate database, database log, and configuration information and click **Next**.



Configure certificate database settings

8. Stop the IIS if it is running.
9. Insert your Windows 2003 CD when prompted, and then click **OK**.



Files Needed window

10. Click **Finish** to complete the installation.

Installing a security certificate

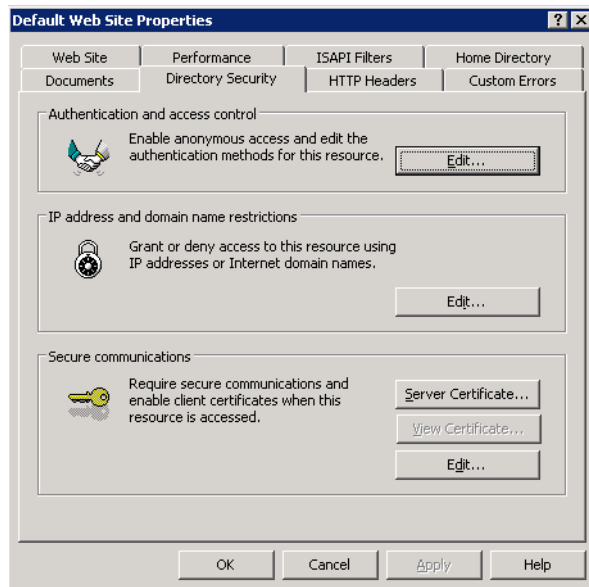
This section contains the procedures for that you must perform to acquire a certificate request.

Generating a security certificate request

This procedure creates a new certificate request, which is then sent to a Certificate Authority (CA) for processing. If successful, the CA will send you back a file containing a validated certificate.

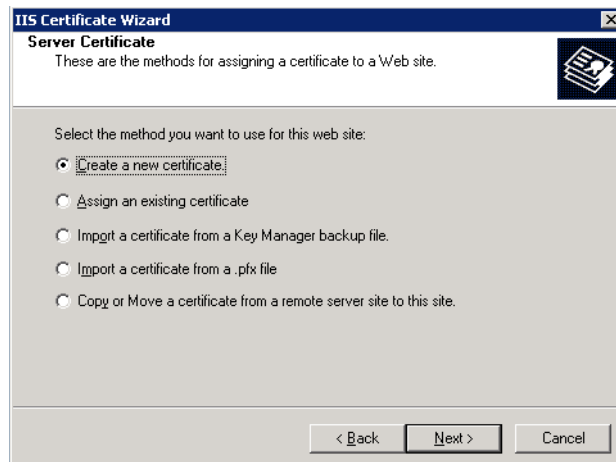
To generate a certificate request

1. Start the IIS Microsoft Management Console (MMC) snap-in.
2. Right-click **Default Web Site**, and then click **Properties**.
3. Click the **Directory Security** tab.



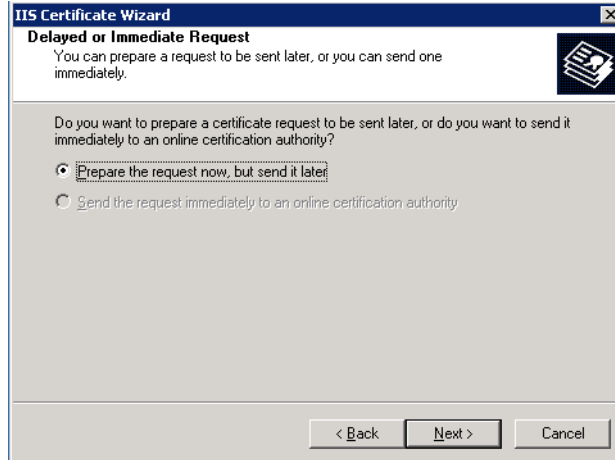
Default Web Site Properties window

4. Under **Secure communications**, click the **Server Certificate** button to launch the Web Server Certificate Wizard.
5. On the Welcome to the web Server Certificate Wizard window Click the **Next** button.
6. In the Server Certificate window select **Create a New Certificate**. Click the **Next** button.



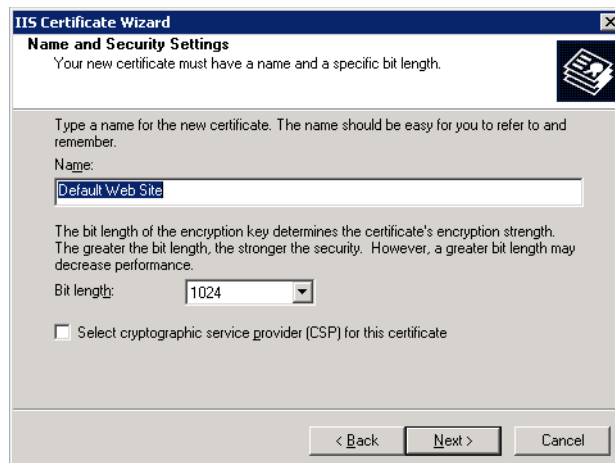
Server Certificate window

7. In the Delayed or Immediate Request window, select the **Prepare the request now, but send it later** option and click **Next**.



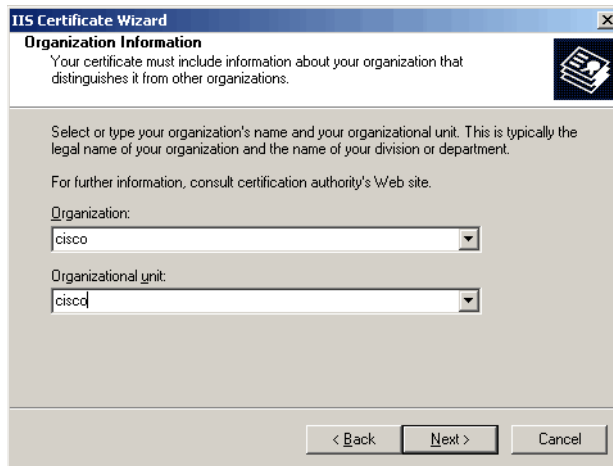
Delayed or Immediate Request window

8. In the Name and Security Settings window, type a descriptive name for the certificate in the **Name** field, type a bit length for the key in the **Bit length** field, and then click **Next**. The wizard uses the name of the current Web site by default.



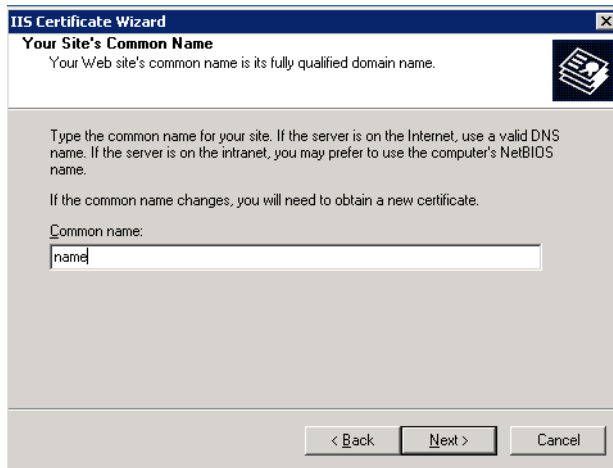
Name and Security Settings window

9. In the Organization Information window, type the organization name (such as Cisco) and unit (such as Service Department). Click **Next**. As this information will be placed in the certificate request, make sure it is accurate.



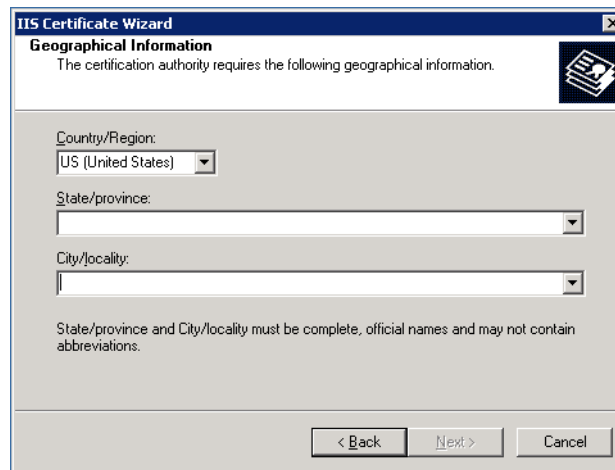
Organization Information window

10. In the Your Site's Common Name window, in the **Common name** field, type the DNS name of the Web Server. Click **Next**.



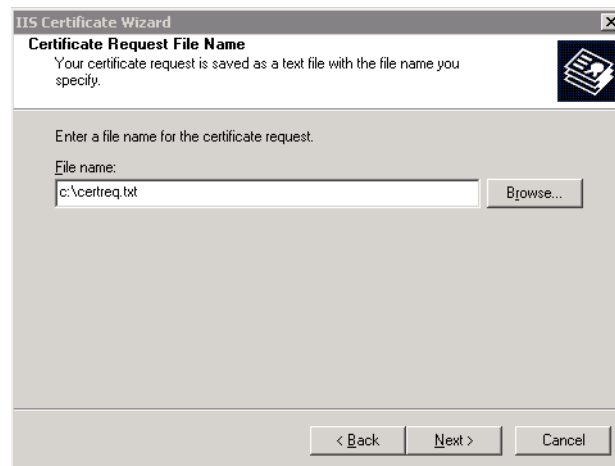
Your Site's Common Name window

11. In the Geographical Information window provide the location information, and click **Next**.



Geographical Information window

12. In the Certificate Request File Name window, type the file name for the certificate request. The default name and location is `c:\certreq.txt`. Click **Next**.



Certificate Request File Name window

13. In the Request File Summary window review the summary and click **Next** to generate the certificate.

Submitting the certificate request

This procedure uses Microsoft Certificate Services to submit the certificate request.

To submit the certificate request

1. Use Notepad to open the certificate file generated in the previous procedure and copy its entire contents to the clipboard. Copy content from
-----BEGIN NEW CERTIFICATE REQUEST-----
to
-----END NEW CERTIFICATE REQUEST-----
2. Open your web browser and type the URL
`http://Certificate_Server/certsrv` where *Certificate_Server* is the name of the computer running Microsoft Certificate Services.
3. Click **Request a Certificate**, and then click **Next**.
4. On the Choose Request Type page, click **Advanced request**, and then click **Next**.
5. On the Advanced Certificate Requests page, select the **Submit a certificate request using a base64 encoded PKCS#10 file or a renewal request using base64 encoded PKCS #7 file** option. Click **Next**.
6. On the Submit a Saved Request page, click in the **Base64 Encoded Certificate Request (PKCS #10 or #7)** text box and paste the certificate request you copied to the clipboard in Step 1. Ensure that you don't leave any blank spaces while pasting the text.
7. In the **Certificate Template** combo box, click **Web Server**.
8. Click **Submit**.
9. Close the web browser.

Getting the certificate issued

To get the certificate issued

1. Go to **Start > Programs > Administrative Tools > Certificate Authority** to open the **Certification Authority** tool.
2. Select the **Pending Requests** folder.
3. Right-click the certificate request that you just submitted.
4. Choose **Actions > All Tasks > Issue**.
5. In the **Issued Certificates** folder, double-click the certificate to view it.
6. On the **Details** tab, click **Copy to File**, and save the certificate as a Base-64 encoded X.509 certificate.
7. Close the Properties window for the certificate.

8. Close the Certificate Authority tool.

Installing the certificate on the Web Server

To install the certificate on the Web Server

1. Start the IIS Microsoft Management Console (MMC) snap-in.
2. Right-click `Default Web Site`, and then click **Properties**.
3. Click the **Directory Security** tab.
4. Under **Secure communications**, click the **Server Certificate** button to launch the Web Server Certificate Wizard.
5. Select the **Process the pending request and install the certificate** option. Click **Next**.
6. Type the path and file name of the local copy of the certificate, and then click **Next**.
7. Review the overview, click **Next**, and then click **Finish**.

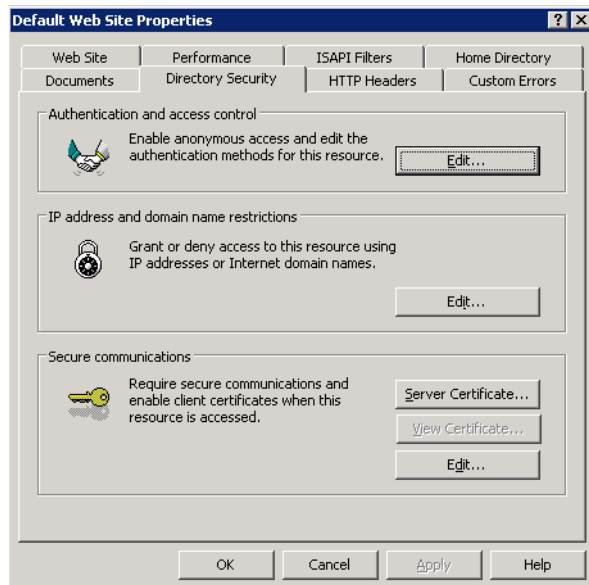
The certificate is now installed on the Web Server.

Configuring SSL access

This procedure uses Internet Services Manager to configure the virtual directory to require SSL for access.

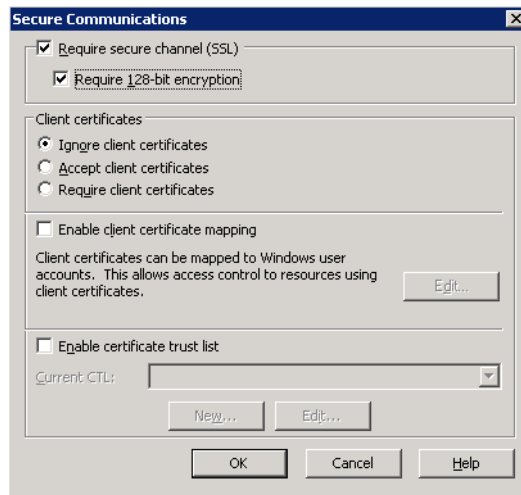
To configure SSL access

1. Go to **Start > Settings > Control Panel > Administrative Tools > Internet Information Services**.
2. Right-click `Default Web Site`, and then click **Properties**.
3. Click the **Directory Security** tab.



Default Web Site Properties window

4. Under **Secure communications**, click **Edit**.
5. In the Secure Communications window, select the **Require secure channel (SSL)** and **Require 128-Bit encryption** options. Click **OK**, and then click **OK** again to close the Properties dialog box.



Secure Communications window

6. Restart the IIS Service.
Clients browsing to this virtual directory must now use HTTPS.

Configuring the viewing of attachments

To make it easy to view attachments

1. In *CIM_Home\config\egpl_master.properties*:
 - a. Change the value of `webtemp.webdir` from `http://Web_Server/temp` to `https://Web_Server/temp`
 - b. Change the value of `Task.Attachment.WebTemp` from `http://Web_Server/temp` to `https://Web_Server/temp`
2. In *CIM_Home\config\egml_mailconfig.properties* change the value of `Attachment.WebTemp` from `http://Web_Server/temp` to `https://Web_Server/temp`

Testing SSL access

To test SSL access to Cisco Interaction Manager

1. Open your web browser.
2. Use HTTP in the URL for Cisco Interaction Manager:
`http://Web_Server/Partition`

You should see a message such as:

The page must be viewed over a secure channel

Please try the following:

Try again by typing protocol as `https://` at the beginning of the address you are attempting to reach. HTTP 403.4 - Forbidden: SSL required Internet Information Services

3. Now use HTTPS in the URL for Cisco Interaction Manager:
`https://Web_Server/Partition`
4. In the security message that appears, click the **View certificate** button.
5. After verifying certificate information, click **OK**. And then click **Yes** to proceed to the URL.

The Cisco Interaction Manager login window appears.

Appendix A: Additional information

- ▶ [Best practices for distributed installations](#)
- ▶ [Frequently asked questions](#)
- ▶ [Starting and stopping components](#)

This chapter provides the startup and shutdown procedures for all components of Cisco Interaction Manager in a distributed installation. It also outlines the best practices for setting up distributed installations and a set of frequently asked questions.

Best practices for distributed installations

The following best practices are strongly recommended when setting up Cisco Interaction Manager in a distributed environment with multiple web/applications servers configured through a load balancer for user access:

- ▶ The startup type for all the Windows services involved with the functioning of Cisco Interaction Manager must be set to manual. This includes IIS Admin service and the World Wide Web Publishing service on all Web Servers and the Cisco Interaction Manager on all Application Servers and the Services Server. This configuration will ensure that all the components in the setup can be stopped and started in a controlled manner in the recommended starting sequence, even when the servers are rebooted.
- ▶ If there is a need to restart any of the individual components (i.e., Web Server, Application Servers, Services Server, or the Database) of the distributed setup, it is recommended that the shutdown and startup procedures be followed as indicated in this document to restart all the components in the distributed setup. It is not advisable to restart individual components only.
- ▶ All Web Servers must be removed from the load balancer when starting the system. When this is not possible, it is important to ensure that IIS is started on all the Web Servers in quick succession. This will ensure that users accessing the load balancer URL are spread across all the Web/Application Servers uniformly without loading excessively the Web/Application Servers that come up first.
- ▶ When there are four or more secondary Web/Application Servers configured in the deployment, it is recommended to add only the secondary Web Servers to the load balancer and not the primary Web Server.
- ▶ The load balancer must be configured to support sticky sessions (i.e. Session Affinity). Typical ways of achieving this are via cookies or source IPs.
- ▶ Round robin is the preferred algorithm to use for the load balancer.
- ▶ A health check URL is provided by Cisco to validate successful access to the system UI. This URL can be used by the load balancer to confirm if the Web Server and the corresponding Application Server are ready to start taking agent login requests. This URL is
`http://Web_Server_Name/system/web/view/platform/common/checkWebAppHealth.jsp.`

If Web and Application Servers have been started properly, the response received to this URL request will be the string named Service.

Frequently asked questions

Q: Why does the Services Server wait for the primary WebLogic server to complete startup?

A: When the Services Server starts, some of the automatic processes (like Workflow, Retriever, and Scheduler) try to register as JMS listeners. This registration would fail if the primary Application Server were not up, since the WebLogic instance running on the primary Application Server also serves as the JMS server for the setup.

Q: Why can't I start the primary Application Server first?

A: One of the startup classes in the primary WebLogic Application Server generates the license.js file by extracting information from the License Manager service. Since the License Manager service is running on the Services Server, it is important for the Services Server to have started the License Manager first.

Q: What is the role of the primary Application Server?

A: The primary Application Server serves as a JMS Server (i.e. Messaging Server) for the entire distributed setup. It maintains nailed connections to all agent browsers (and customer browsers in case of Chat) for the purpose of delivering messages to the Cisco Interaction Manager consoles. It is also capable of servicing agent login requests. However, we recommend that it be excluded from this role in order to minimize the load on this server when there are four or more secondary Web/Application Servers.

Q: What is the role of the Web Server?

A: The Web Server is used to serve static content to the web browser and redirect dynamic content requests (i.e. JSP requests) to the Application Server. The primary Web Server also serves attachments to email and knowledge base articles when agents wish to view them from the Cisco Interaction Manager consoles.

Q: How can I verify that the load is equally distributed on all the web/application servers after a system re-start?

A: The URL `http://Web_Server_Name/system/web/view/platform/debug/listsessions.jsp` can be accessed for each primary and secondary Web/Application servers to list down the active/inactive user sessions running on them.

Q: What are the checklist items to verify in case of distributed setups?

A: The following items have been identified as checklist items for distributed setups:

- ▶ The value of the Messaging applet IP address setting (Common.messaging.applethost) in the master and active databases must be set to be that of the Primary Web Server. The network on which the agent browsers reside must be able to resolve the IP address of the primary Web Server. Accordingly, external or internal IP addresses must be used.

This setting value can also contain the Fully Qualified Domain Name of the primary Web Server as long as it maps to its alternate IP address.

You can verify the value of this setting by running the following query on the master and active databases:

```
SELECT SETTING_ACT_VAL FROM EGPL_PREF_GLOBALSETTINGS
WHERE SETTING_NAME = 'Common.messaging.applethost'
```

- ▶ The ThreadCount for eGainPushletQueue configured in the primary Application Server must be equal to the maximum number of users expected to access the UI concurrently through all the web/application servers. This information will be in the file:

```
CIM_Home\config\weblogic\config_<server_name>.xml
```

- ▶ The WebLogic server license file (i.e. *BEA_Home\license.bea* file) on all the Application Servers (primary and secondary) must contain ISV specific entries. When the Cisco Interaction Manager installation program runs, the license.bea file is updated with entries of type="ISV" and expiration="never" towards the beginning of the file. The installer internally executes the command utility *BEA_Home\UpdateLicense.cmd license_isv.bea*
- ▶ The WebLogic server jar file (i.e. weblogic.jar) on all the Application Servers (primary and secondary) must correspond to the ISV version. When the Cisco Interaction Manager installation program runs, an ISV version of the weblogic.jar file is copied to the folder *BEA_Home\weblogic81\server\lib* from the folder *CIM_Home\lib\ext\platform*. The original weblogic.jar file under the folder *BEA_Home\weblogic81\server\lib* is renamed as weblogic.jar_orig.

Starting and stopping components

This procedure assumes that Cisco Interaction Manager is configured to run as a Windows service on the Services Server and the Application Servers (Primary and Secondary). This is the default configuration for running Cisco Interaction Manager.

Starting sequence

To start the Cisco Interaction Manager application, Windows services on the different machines must be started in the following order:

1. **Services Server:** Start Cisco Interaction Manager.
2. **Primary Application Server:** Start Cisco Interaction Manager.
3. **Secondary Application Servers:** Start Cisco Interaction Manager.
4. **Web Servers:** Start IIS Admin service, World Wide Web Publishing service, and the Default Web Site on all servers.
5. **Load balancer:** Enable the routing logic to allow web requests to come into Cisco Interaction Manager.

Stopping sequence

To shut down the Cisco Interaction Manager application, Windows services on the different machines should be stopped in the following order.

1. **Load balancer:** Disable the routing logic to ensure that no web requests are allowed to come into Cisco Interaction Manager.
2. **Web Servers:** Stop IIS Admin service and World Wide Web Publishing service on all servers.
3. **Secondary Application Servers:** Stop Cisco Interaction Manager on all servers and ensure that the java process corresponding to the WebLogic server is terminated.
4. **Primary Application Server:** Stop Cisco Interaction Manager and ensure that the java process corresponding to the WebLogic server is terminated.
5. **Services Server:** Stop Cisco Interaction Manager and ensure that all the java, javaw, cmd, and rmid processes corresponding to Cisco services are terminated.

Starting Services Server and primary Application Server

The Services Server and the primary Application Server must be started in a well-coordinated manner as they have certain dependencies on each other.

1. Start Cisco Interaction Manager on the Services Server through the Windows Services control panel.
2. Look for the message Waiting for Application Server to start t3, associated with a timestamp close to the current time, in the file
`CIM_Home\logs\0_pid_dsm_log.txt`
3. Start Cisco Interaction Manager on the primary Application Server.

4. Look for the message Application Server started t3, associated with a timestamp close to the current time, in the file
CIM_Home\logs\0_pid_dsm_log.txt
5. Look for the message Server started in RUNNING mode, associated with a timestamp close to the current time, in the file
CIM_Home\logs\egain_weblogic_server.log

Starting secondary Application Servers

The secondary Application Servers must be started one after another using the following steps:

1. Start the service named Cisco Interaction Manager on the Secondary Application Server through the Windows Services control panel.
2. Look for the message Application Server started t3, associated with a timestamp close to the current time, in the file
CIM_Home\logs\0_pid_dsm_log.txt
3. Look for the message Server started in RUNNING mode, associated with a timestamp close to the current time, in the file
CIM_Home\logs\egain_weblogic_server.log

Appendix B: Reference sheet

- ▶ [Configuration details](#)
- ▶ [File Server details](#)
- ▶ [Database details](#)
- ▶ [Application Server details](#)
- ▶ [Web Server details](#)
- ▶ [Services Server details](#)
- ▶ [Archive details](#)

Configuration details

Additional partition

- Yes: 1 2 3 Other
 No

Configuration type and option

- Single server
 Split server
 Distributed server
 Option: 1 2 3 Other

File Server details

#	Item	Value
1.	Location of CIM home directory	

Database details

#	Item	Value
1.	System Administrator user name	
2.	System Administrator password	
3.	Partition Administrator user name	
4.	Partition Administrator password	
5.	Partition name	
6.	Partition description	
Master database parameters		

#	Item	Value
7.	Server name	
8.	Database name	
9.	Database listener port	
10.	Datafile path	
11.	Datafile initial size	
12.	Datafile maximum size	
13.	Datafile increment size	
14.	Logfile initial size	
15.	Logfile maximum size	
16.	Database administrator user name	
17.	Database administrator password	
18.	CIM Database user name	
19.	CIM Database password	
Partition Database parameters		
20.	Server name	
21.	Database name	
22.	Database listener port	
23.	Datafile path	
24.	Datafile initial size	
25.	Datafile maximum size	
26.	Datafile increment size	
27.	Logfile initial size	
28.	Logfile maximum size	
29.	Database administrator user name	
30.	Database administrator password	

#	Item	Value
31.	CIM Database user name	
32.	CIM Database password	

Application Server details

#	Item	Value
1.	Location of BEA home directory	
2.	Location of WebLogic home directory	
3.	Location of JDK home directory	
4.	Location of file server	
5.	Location of CIM home directory	
6.	Web server name	
7.	Services server name	
WebLogic server parameters		
8.	Domain location	
9.	Server name	
10.	User name	
11.	Password	
12.	Listen port	
13.	SSL listen port	
RMI parameters		
14.	RMI registry port	
15.	RMI activation port	
Master database parameters		

#	Item	Value
16.	Server name	
17.	Database name	
18.	Database listen port	
19.	CIM Database user name	
20.	CIM Database password	
Partition database parameters		
21.	Server name	
22.	Database name	
23.	Database listen port	
24.	CIM Database user name	
25.	CIM Database password	

Web Server details

#	Item	Value
1.	File server name	
2.	User name to connect to file server share	
3.	Password to connect to file server share	
4.	Application server name	

Services Server details

#	Item	Value
1.	Location of JDK home directory	
2.	Location of CIM home directory	
3.	File server name	

Archive details

#	Item	Value
Partition parameters		
1.	Partition name	
2.	Database administrator user name	
3.	Database administrator password	
Archive database parameters		
4.	Server name	
5.	Database name	
6.	Database listener port	
7.	Datafile path	
8.	Datafile initial size	
9.	Datafile maximum size	
10.	Datafile increment size	
11.	Logfile initial size	
12.	Logfile maximum size	
13.	Administrator user name	

#	Item	Value
14.	Administrator password	
15.	CIM Database user name	
16.	CIM Database password	