



Cisco Media Blender Installation Guide for Cisco Unified Contact Center Enterprise and Hosted Editions

Cisco Media Blender, Release 7.1
September 2009

Americas 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: 408 527-0883

Text Part Number:

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.

CCDE, CCENT, CCSI, Cisco Eos, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco Pulse, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco:Financed (Stylized), Cisco Store, and Flip Gift Card are service marks; and Access Registrar, Aironet, AllTouch, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Fast Step, Follow Me Browsing, FormShare, GainMaker, GigaDrive, HomeLink, iLYNX, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo 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. (0908R).

Cisco Media Blender Installation Guide for Cisco Unified Contact Center Enterprise and Hosted Editions
Copyright © 2009-2012 Cisco Systems, Inc. All rights reserved.



CONTENTS

About this Guide i

Overview i

Audience i

Organization i

Related Documentation ii

Obtaining Documentation, Obtaining Support, and Security Guidelines ii

Documentation Feedback ii

CHAPTER 1

Introduction 1-1

Cisco MB with Unified CCE Configuration 1-1

CHAPTER 2

System Requirements 2-1

Requirements for Cisco MB with Unified CCE 2-1

Hardware Requirements 2-2

Software Requirements 2-2

Supported ACDs 2-3

CHAPTER 3

Before You Install Cisco MB 3-1

Verifying IIS is Installed 3-2

Understanding ServletExec™ 3-2

CHAPTER 4

Installing Cisco MB 4-1

Install the Cisco MB Software 4-2

- Handling errors encountered while installing Cisco MB 7.1 4-2
- Configure Cisco MB and Participating Media 4-3
- Configure Communication Through a Firewall 4-3
 - Polling Over Outbound Socket Connection Mode 4-3
 - Classic HTTP Proxy Mode 4-4
 - Networking Considerations 4-4
- Restart IIS 4-5
- Start Cisco MB 4-5
- Uninstalling Cisco MB 4-6
- Configuring Cisco MB 7.1 to Run in IIS 6.0 Worker Process Isolation Mode 4-7

CHAPTER 5

Post Installation Tasks 5-1

- Grant Administrative Access to Cisco MB 5-1
- Configure Cisco MB for AutoStart 5-2
- Activate Windows Messaging 5-3

CHAPTER 6

Troubleshooting Tips 6-1

- Troubleshooting Tips 6-2
 - Cannot login to the Cisco MB administration desktop after installation 6-2
 - Blank page is displayed when trying to access the Cisco MB Administration page 6-3

GLOSSARY

INDEX



About this Guide

Overview

The *Cisco Media Blender Installation Guide* provides information to help you install the Cisco Media Blender (Cisco MB) Version 7.1 software.

Audience

This guide is written for anyone responsible for installing the Cisco MB, Version 7.1, software.

Organization

This guide is organized as follows:

Chapter 1, “Introduction”	Provides a brief overview of the Unified CCE-integrated Cisco MB configuration that is supported in Version 7.1.
Chapter 2, “System Requirements”	Describes the hardware and software required for installing Cisco MB on a Windows 2003 system running the Internet Information Server (IIS).

Chapter 3, “Before You Install Cisco MB”	Describes tasks to complete before installing the Cisco MB software.
Chapter 4, “Installing Cisco MB”	Describes the tasks to complete to install the Cisco MB software.
Chapter 5, “Post Installation Tasks”	Describes optional tasks to complete after installing the Cisco MB software.
Chapter 6, “Troubleshooting Tips”	Describes the troubleshooting tips after installing the Cisco MB software.

Related Documentation

You need the following documentation:

- *Cisco Media Blender Administration Guide*
- Cisco Media Blender Administration Online Help
- *Cisco Media Blender Switch Administration Guide*
- *Cisco Unified Web and Email Interaction Manager System Administration Guide* and Online Help

Obtaining Documentation, Obtaining Support, and Security Guidelines

For information on obtaining documentation, obtaining support, security guidelines, and also recommended aliases and general Cisco documents, see the monthly What's New in Cisco Product Documentation, which also lists all new and revised Cisco technical documentation, at:

<http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html>

Documentation Feedback

You can provide comments about this document by sending email to the following address:

ccbu_docfeedback@cisco.com



CHAPTER 1

Introduction

Cisco MB Version 7.1 works with Cisco Unified Web Interaction Manager (Unified WIM) to provide Web callback and blended collaboration. You can integrate Cisco MB with an ACD(Avaya) or with Cisco Unified Call Manager/SoftACD, depending upon the driver used and the configuration.

This chapter includes the following sections:

- [Cisco MB with Unified CCE Configuration, page 1-1](#)

Cisco MB with Unified CCE Configuration

As part of the Cisco Unified CCE multichannel software, Cisco MB works with the Unified WIM to provide Web callback and blended collaboration. Cisco MB supports Cisco Unified Call Manager/SoftACD and Avaya(legacy ACD) using the Cisco CTI driver.



CHAPTER 2

System Requirements

This section describes the hardware and software required for installing Cisco MB on a Windows 2003 system running the Internet Information Services (IIS).

Cisco MB Administration is accomplished through a Web-based user interface. To properly view the Administration UI, your monitor display resolution must be set at a minimum of 1024 x 768 pixels.

System requirements are provided for the following configurations:

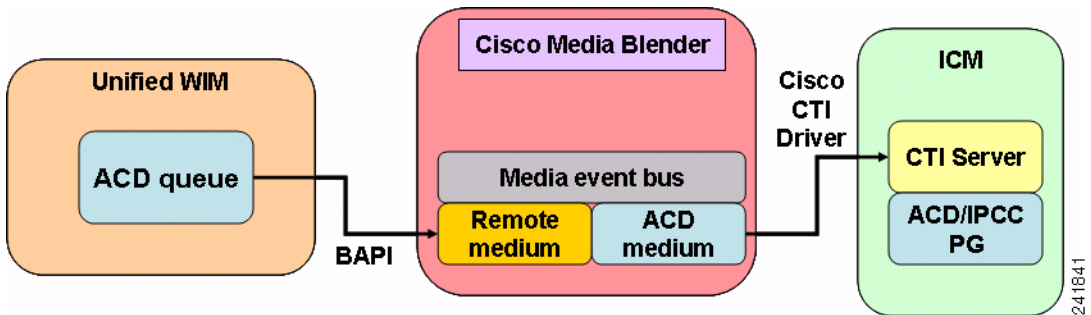
- [Requirements for Cisco MB with Unified CCE, page 2-1](#)

Requirements for Cisco MB with Unified CCE

Cisco MB in the Unified CCE-integrated configuration functions as an event bus. Cisco MB 7.1 can be installed on a standalone server. Cisco MB is not supported when installed on a PG.

[Figure 2-1](#) shows Cisco MB with the Unified CCE integration:

Figure 2-1 Cisco MB with ICM Integration



Hardware Requirements

Following are the hardware requirements for Cisco MB with Unified CCE:

- 2 x 1.4GHz or greater Intel Pentium processors
- 2000+ MB RAM
- 18.2+ GB usable disk space

Software Requirements

Following are the software requirements for Cisco MB with Unified CCE:

- Microsoft Windows 2003 Server (Enterprise Edition)
- Microsoft IIS, Version 6.0
- Java Development Kit (JDK), Version 1.4.2 (provided by Cisco)
- ServletExec, Version 5.0 (provided by Cisco)

Following are the other products with which Cisco MB works. These products are on separate machines, and you will need either Cisco Unified Call Manager/SoftACD or an Automatic Call Distributor(ACD).

- Cisco Unified Web Interaction Manager (Unified WIM)
- Cisco Unified Contact Center Enterprise (Unified CCE) Software, Version 7.0 and higher.

- ACDs using the Cisco CTI driver:
 - Cisco IPCC
 - Avaya Definity ECS G3

**Note**

Check with your Cisco representative for details about the ACD versions.

Supported ACDs

Table 2-1 shows the ACDs that Cisco MB Version 7.1 supports in the Unified CCE-integrated configuration. Also shown are the drivers and CTI strategies for each ACD.

Table 2-1 **Supported ACDs**

ACDs	Cisco MB with Unified CCE/Drivers	CTI Strategies
Cisco IPCC	Cisco CTI driver	AgentReserved
Avaya Definity ECS G3	Cisco CTI driver	Phantom and Predictive

**Note**

See the CTI Strategies for Call Classes section in the *Cisco Media Blender Administration Guide* for additional information about the various types of phantom strategies that are supported for the Avaya Definity ECS G3 ACD.



CHAPTER 3

Before You Install Cisco MB

Before you install Cisco MB, Microsoft Internet Information Services (IIS) must be installed on the Cisco MB machine.

You should also have some understanding of the ServletExec software, which is on the Cisco MB CD. The ServletExec and Java Development Kit (JDK) software are installed automatically during the Cisco MB installation process.



Note

Be sure you have uninstalled any previous versions of Cisco MB and ServletExec, which must be removed separately. It is not necessary to remove a previous version of the JDK, but you can do so if you want to save space.

This chapter includes the following sections:

- [Verifying IIS is Installed, page 3-2](#)
- [Understanding ServletExec™, page 3-2](#)

Verifying IIS is Installed

Verify that IIS is installed properly and is not running.

-
- Step 1** Go to **Start > Settings > Control Panel > Administrative Tools > Services**.
- Step 2** Select **IIS Admin Service** and check the status.
The status should not be "Started." If it does read "Started," stop the service by completing the following step.
- Step 3** From the Action menu, select Stop.
-

Understanding ServletExec™

When you install Cisco MB, you also install ServletExec Version 5.0, from New Atlanta Communications. ServletExec is a Java-based Web application server that implements the Java Servlet API and JavaServer Pages (JSP) standards defined by Sun Microsystems.

ServletExec will locate the Java Development Kit (JDK) on your machine. The Cisco MB Administrator pages are served through ServletExec, and the pages are set as access-controlled resources (URLs). If you have any questions about ServletExec, see the *ServletExec User Guide* in the `\CiscoMB\servlet_exec\Documentation` directory.

After you have installed Cisco MB, you can configure the ServletExec property file, `resource.properties`, to grant administrative access to specific NT users. See [Grant Administrative Access to Cisco MB, page 5-1](#).

**Note**

If you need to uninstall Cisco MB, be sure to uninstall ServletExec first. If you do not follow this sequence, ServletExec will not uninstall. This happens because uninstalling Cisco MB removes the registry settings for the JDK that are required by ServletExec. If you inadvertently uninstall Cisco MB before ServletExec, there is a workaround. Run the Cisco MB setup.exe again, and click **OK** when asked

"Do you want to uninstall ServletExec?" This will remove ServletExec and exit the setup. You can then run the Cisco MB setup.exe again to install ServletExec and Cisco MB.



CHAPTER 4

Installing Cisco MB

Installing Cisco MB involves the completion of the following tasks:

- Install the Cisco MB software
- Configure Cisco MB and Participating Media
- Configure Communication Through a Firewall
- Restart Internet Information Services (IIS)
- Start Cisco MB

This chapter includes the following sections:

- [Install the Cisco MB Software, page 4-2](#)
- [Configure Cisco MB and Participating Media, page 4-3](#)
- [Configure Communication Through a Firewall, page 4-3](#)
- [Restart IIS, page 4-5](#)
- [Start Cisco MB, page 4-5](#)
- [Uninstalling Cisco MB, page 4-6](#)
- [Configuring Cisco MB 7.1 to Run in IIS 6.0 Worker Process Isolation Mode, page 4-7](#)

Install the Cisco MB Software

Complete the following steps to install the Cisco MB software:

-
- Step 1** Close all application windows except Windows Explorer.
- Step 2** From the Cisco MB CD, double-click **\Media Blender\Setup.exe**.
Select the destination location and install Cisco MB in the directory of your choice. (There should be NO spaces in the path.)
- Step 3** Click **Next**. The ServletExec installation program begins.
- Step 4** Ensure that the Destination Folder for ServletExec correctly points to the folder where you installed IIS.
- Step 5** Click **Next** and follow the prompts to install ServletExec.
- Step 6** Click **Finish**. The setup is complete.
-

Handling errors encountered while installing Cisco MB 7.1

You may encounter the following errors while installing Cisco MB:

- Error while setting IIS 6.0 to run in IIS 5.0 isolation mode. Refer *Cisco MB 7.1 Installation Guide* for more details.
- Could not get IIS root directory. Refer *Cisco MB 7.1 Installation Guide* for more details.

In case you encounter one or both the errors mentioned above during installation, only then follow the below steps:

-
- Step 1** Go to **Start > Programs > Administrative Tools > Internet Information Services (IIS) Manager**.
- Step 2** In IIS Manager, expand the local computer, right-click **Web Sites**, and then click **Properties**.

- Step 3** Click the **Service** tab, select the **Run WWW service in IIS 5.0 isolation mode** check box, and then click **OK**.
- Step 4** To start the World Wide Web services (WWW) service, click **Yes**.
-

Configure Cisco MB and Participating Media

You configure Cisco MB and the ACD medium using plain text property files. These files contain simple name value pairs (properties) that define the behavior of Cisco MB or the appropriate ACD medium. You can modify property files with any text editor. The files typically reside in the `\CiscoMB\servlet\Properties\Blender` directory.

You configure the Application medium and the two-way connection between Cisco MB and Cisco Unified Web Interaction Manager (Unified WIM) using the WIM Administration desktop. See the *Cisco Unified Web and Email Interaction Manager System Administration Guide* and Online Help for details.

Configure Communication Through a Firewall

Cisco MB communicates with Unified WIM using the Sun Microsystems Remote Method Invocation (RMI). The firewall can be set up in either of the following modes:

- Polling over outbound socket connection mode
- Classic HTTP proxy mode

Polling Over Outbound Socket Connection Mode

The recommended mode to use is the polling mode, which provides high throughput and allows outbound socket connections from Cisco MB to Unified WIM. Cisco MB connects to Unified WIM using TCP/IP socket connections. If you use this mode, ensure that your firewall permits outbound socket connections

from Cisco MB to Unified WIM on specified ports. Ports can be chosen when you set up the Unified WIM connection to Cisco MB using the Unified WIM Administration user interface.

Classic HTTP Proxy Mode

In the Classic HTTP proxy mode, the firewall permits only outbound HTTP communication to all ports. Cisco MB connects to Unified WIM using HTTP to the RMI registry port (1099 default). This mode provides the lowest throughput of the two modes and may cause problems if you have a high call volume. To setup the HTTP proxy, complete the following steps:

Step 1 Locate and edit the following file:

```
C:\Program Files\New Atlanta\ServletExec ISAPI\ServletExec
Data\ vmoptions.properties
```

Step 2 Add the following properties and values, separated by spaces:

```
-Dhttp.proxySet=true -Dhttp.proxyHost=<HOSTNAME-OF-PROXY>
-Dhttp.proxyPort=<PORT-OF-PROXY>
```

Step 3 Restart the Web server so the settings will take effect.

Networking Considerations

The following are some networking considerations:

- Both the Unified WIM and the Cisco MB server require static IP addresses.
- Regardless of your firewall setup, you must maintain a hosts file rather than use Domain Name Service (DNS) to identify the IP address of your machines. Using DNS may result in RMI connectivity problems. The hosts file resides at this location on Windows 2003:

```
WINNT\system32\drivers\etc\hosts
```

The hosts file on the Cisco MB machine must have an entry for Unified WIM, and the hosts file for Unified WIM must have an entry for the Cisco MB machine.

- When you are using Cisco MB with the Unified CCE integration and are setting up your network, please note that the link from Cisco MB to the CTI Server should have a round-trip latency of no more than 1000 milliseconds.

Restart IIS

Restart the IIS by completing the following steps:

Step 1 Select **Start > Settings > Control Panel > Administrative Tools > Services**.

Step 2 In the Services window, select **IIS Admin Service** in the Name column.

Step 3 From the Action menu, select **Start**.

Check that the word "Started" appears in the Status column for IIS Admin Service.

Start Cisco MB

Cisco MB uses NT security, and an NT Administrator account for the server or domain might be required to log in to the Administration control panel. See [Grant Administrative Access to Cisco MB, page 5-1](#) for more information.



Note

Before starting Cisco MB, be sure you have completed the configuration of Cisco MB and any participating media following the steps in the *Cisco Media Blender Administration Guide*.

To start Cisco MB, complete the following steps:

-
- Step 1** Log in to the Cisco MB Administration control panel or open a browser and go to `http://<blender-server-name>/admin`.
The Welcome to Media Blender Administration page appears.
- Step 2** From the Administration menu in the left pane, select **SERVER > Start/Shutdown**.
The **Media Blender : Server : Start/Shutdown** page appears.
- Step 3** Click **Start** on the Control panel. Cisco MB displays a "Startup successful" message.
-

Uninstalling Cisco MB

Perform the following steps to uninstall the Cisco MB software:



Note

ServletExec should be uninstalled before uninstalling the Cisco MB.

-
- Step 1** Stop the IIS and WWW services.
- Step 2** Click **Start > Settings > Control Panel > Add/Remove Programs**.
- Step 3** Select **ServletExec 5.0 ISAPI**.
- Step 4** Click **Change/Remove** and click **OK** when asked "Do you want to uninstall ServletExec?"
- Step 5** Select **Cisco Media Blender 7.1**.
- Step 6** Click **Change/Remove** and follow the uninstaller instructions.
- Step 7** Click **OK** when un-installation completes.
- Step 8** Start the IIS and WWW services.
-

Configuring Cisco MB 7.1 to Run in IIS 6.0 Worker Process Isolation Mode

You can run IIS 6.0 in one of two modes:

- Worker process isolation mode
- IIS 5.0 isolation mode

During installation of Cisco MB 7.1, IIS is set to run in IIS 5.0 isolation mode.



Note

The impact of making IIS to run in worker process isolation mode is - Cisco MB application will not be initialized on starting IIS until a client has specifically requested service. Hence, each time on restarting IIS, you will have to access Cisco MB admin page (<http://<Cisco MBHostName>/admin>) to start Cisco MB application.

Perform the following steps to configuring Cisco MB 7.1 to run in IIS 6.0 worker process isolation mode:

-
- Step 1** Go to **Start > Programs > Administrative Tools > Internet Information Services (IIS) Manager**.
 - Step 2** In IIS Manager, expand the local computer, right-click **Web Sites**, and then click **Properties**.
 - Step 3** Click the **Service** tab, clear the **Run WWW service in IIS 5.0 isolation mode** check box, and then click **OK**.
 - Step 4** To start the WWW service, click **Yes**.
If the switch to worker process isolation mode is successful, a folder named Application Pools appears in the IIS Manager listing for your local computer.
 - Step 5** Go to **Application Pools > DefaultAppTool**. Right click, go to **Properties > Recycling** tab, uncheck “Recycle worker process (in minutes)”.
 - Step 6** Go to **Application Pools > DefaultAppTool**. Right click, go to **Properties > Performance** tab, uncheck “Shutdown worker process after being idle for (time in minutes)”



CHAPTER 5

Post Installation Tasks

After you have installed and configured Cisco MB, there are some optional tasks you can choose to perform. You can do any of the following:

- [Grant Administrative Access to Cisco MB, page 5-1](#)
- [Configure Cisco MB for AutoStart, page 5-2](#)
- [Activate Windows Messaging, page 5-3](#)

Grant Administrative Access to Cisco MB

You have the option of configuring the ServletExec property file, `resource.properties`, located in the `<drive>:\Program Files\New Atlanta\ServletExec ISAPI\ServletExec Data\default\` directory, to grant administrative access to specific NT users. Here are the contents of that file:

```
Blender.groups=  
Blender.users=Administrator  
BlenderNew.groups=  
BlenderNew.users=Administrator  
wlPageCompile.groups=  
wlPageCompile.users=Administrator
```

Note that "Administrator" is the default. The spelling of this default varies when using the Spanish locale (use "Administrador") or the French locale (use "Administrateur"). You can also add NT user names separated by commas. A valid user name would be that of any NT user on the machine on which Cisco MB is installed. Here is an example:

```
Blender.users=Administrator, jsmith, bjones  
BlenderNew.users=Administrator, jsmith, bjones  
wlPageCompile.users=Administrator, jsmith, bjones
```

After adding new user names, restart IIS.

**Note**

NT users (jsmith and bjones in the above example) should have local log on rights on the machine running IIS. Also, if you configure IIS to use Basic Authentication, the default Windows NT Domain used by IIS for authentication is the domain of the machine on which IIS is running. If the NT users (jsmith, bjones) are on a different domain, you must set this domain name under Basic Authentication using the Internet Service Manager. For more details, see the IIS 5.0(0) documentation. When IIS is installed on your system, you can access the IIS documentation by typing <http://localhost/iishelp/> in your browser location field and pressing Enter.

Configure Cisco MB for AutoStart

Once installation is complete, you can ensure that Cisco MB and all media automatically start when the Web server and the Blender servlet are started.

To ensure automatic start of Cisco MB:

-
- Step 1** Edit the `blender.properties` file, which resides in the `CiscoMB\servlet\properties\blender` directory.
 - Step 2** Set the `autostart` property to `true`.
-

Important: Do not set this property to `true` until you are sure that all of your media are properly configured and Cisco MB starts successfully.

Activate Windows Messaging

Cisco MB logs messages into a log file. You can view these messages on the Cisco MB Administration user interface on the Latest Log page. You can also choose to configure Cisco MB to log alert and error messages (but not trace messages) to the Windows application event log. By using the Windows log, you can view errors for all applications on your system at the same time.

To set up Windows messaging, complete the following steps:

-
- Step 1** Manually copy the following DLLs from `<drive>:\CiscoMB\bin` to `C:\WINNT\system32`:
- ```
WindowsEventMessages.dll
WindowsEventWrapper.dll
```
- Step 2** Edit the `<drive>:\CiscoMB\servlet\properties\logManager.properties` file. Uncomment (remove the "#") from the following line:
- ```
#logManager.LogStream.Error.LogOutputAdapter_3=cmbWindowsEventAdapter
```
- Step 3** Edit the `<drive>:\CiscoMB\servlet\properties\logOutputAdapters.properties` file. Uncomment all the lines beginning with "logOutputAdapter.cmbWindowsEventAdapter." These lines are grouped together under the comment "properties for cmbWindowsEventAdapter."
- Step 4** To view the events, start the Windows Event Viewer utility. Go to **Start > Programs > Administrative Tools > Event Viewer > Application Log**. Events generated by Cisco MB will have either "cmb" or "AlertCMBCommon" displayed in the Source column.
-

■ **Activate Windows Messaging**



CHAPTER 6

Troubleshooting Tips

This chapter describes the troubleshooting tips you may need to refer after installing the Cisco MB software.

This chapter includes the following sections:

- [Troubleshooting Tips, page 6-2](#)

Troubleshooting Tips

Cannot login to the Cisco MB administration desktop after installation

Symptom Cisco MB administration desktop is not accessible after installation.

Error Message HTTP Error 401.1 - Unauthorized: Access is denied due to invalid credentials. Internet Information Services (IIS)

Recommended Action If the host where Cisco MB 7.1 is installed is not part of a domain, then the anonymous username should be of the format *<hostname/username>*. To do this, perform the following steps:

-
- Step 1** Click **Start > Control Panel > Administrative Tools -> Internet Information Services**.
 - Step 2** In IIS Manager, expand the local computer, right-click **Default Website** and select **Properties**.
 - Step 3** In the **Directory Security** tab, under anonymous access and authentication control, click **Edit**.
 - Step 4** Prefix the username with the hostname.
 - Step 5** Click **OK**.
 - Step 6** Restart IIS and WWW services.
-

Blank page is displayed when trying to access the Cisco MB Administration page

Symptom A blank page is displayed when you try to access the Cisco MB Administration page.

Error Message None.

Recommended Action Ensure that the URL of the Cisco MB Administration page is added to the list of trusted sites if **internet** is selected as the **web content zone** under **Tools > Internet Options > Security** in the Web Browser.



GLOSSARY

A

ACD

Automatic Call Distribution. A feature that automatically routes incoming calls to the next available or longest idle agent or attendant in a line hunt group.

ACD Medium

The ACD medium on the Cisco Media Blender (Cisco MB) handles CTI messages coming from an ACD.

Agent

An individual who receives and handles customer calls and web-based requests within a contact center.

Application Medium

The Application medium communicates with Cisco Unified Web Interaction Manager (Unified WIM) and accepts and shares session and agent-related events with the other Cisco MB media.

B

Blended Collaboration

Blended Collaboration sessions typically begin when a caller submits a Web-based request by clicking a callback button on a web page. The caller completes a callback form and Unified WIM retrieves caller information (name, phone number, skill group). Blended collaboration in the Unified CCE integration is provided when the agent is assigned by Unified CCE (when using IPCC) or by the ACD (when using a legacy ACD). When Unified CCE software selects an agent for the task, the Web collaboration interface appears on the agent desktop. At the same time, the agent's telephone places an outbound call to the customer.

C

Caller

An individual submitting a phone call or Web-based request to a contact center.

CTI

Computer Telephony Integration. A term for connecting a computer to a telephone switch. The computer issues telephone switch commands to move the calls around.CDP

CTI Driver

Software designed to accommodate the CTI package and middleware used in a Cisco MB configuration. The CTI driver supports the legacy ACDs when Cisco MB is part of the Unified CCE integration.

CTI strategy

Software that determines the call flow of the outbound call to the caller.

D

Driver

A module that controls data transferred to and received from peripheral devices.

I

Intelligent Contact Management (ICM) software

The Cisco system that implements enterprise-wide call distribution across contact centers. ICM software provides Pre-Routing®, Post-Routing®, and performance monitoring capabilities.

IPCC

Internet Protocol Contact Center. A virtual ACD which provides intelligent call routing, network-to-desktop CTI, IVR integration, call queuing, and consolidated reporting.

L

Legacy ACD

The Avaya Definity ECS G3 ACD supports the Unified CCE integration that use the Cisco CTI driver.

M

Media Blender Administrator

An individual responsible for installing, configuring, and administering Media Blender.

Medium

An electronic form of session-based information. Cisco MB functions as an event bus and shares events between participating media. In a typical installation, Cisco MB shares events between an Application medium and an ACD medium.

P

Peripheral Gateway (PG)

The computer and process within the Unified CCE system that communicates directly with the ACD, PBX, or IVR at the contact center. The Peripheral Gateway reads status information from the peripheral and sends it to the Central Controller. In a private network configuration, the Peripheral Gateway sends routing requests to the Central Controller and receives routing information in return.

Phantom Line

Phone lines set aside for providing callback to customers. Used with Phantom line CTI strategies, phantom lines wait in queue on behalf of the caller, ensuring the caller receives callback only when an agent is available.

Phantom Strategy

A CTI strategy that places a call in the ACD queue and waits for call assignment (agent selection). Once the agent is selected, the outbound call is placed to the customer.

PIM

Peripheral Interface Manager. The Cisco proprietary interface between a peripheral and the Peripheral Gateway (PG).

Predictive Strategy

A CTI strategy that places the call to the customer first and then places the caller in an inbound ACD queue.

R

RMI

Remote Method Invocation. A remote procedure mechanism for communicating between two Java programs within (potentially) separate Java Virtual Machines.

Routing logic

Logic set up on the ACD to ensure calls are routed to agents who possess appropriate skills.

S

Switch

An ACD or PBX.

W

Web Callback

A feature of the Unified WIM that allows a customer to use a "callme" button on a company's Web site. The resulting callback request is handled by the Unified CCE software (for Cisco MB in the Unified CCE integration). Web callback, sometimes referred to as "callback only," is for simple callbacks that do not involved blended Web collaboration or blended text chat.

U

Unified WIM

Cisco Unified Web Interaction Manager (Unified WIM) provides agents with a comprehensive set of tools for serving customers in real-time. It enables call center agents to provide immediate personalized service to customers through text chat messaging and page-push abilities. Agents could also use Unified WIM to assist customers while on the phone, by navigating through web pages that the customer is currently browsing.



INDEX

A

Access to Cisco MB

granting [5-1](#)

ACD Support [2-3](#)

Cisco MB with Unified CCE [2-1](#)

Autostart [5-2](#)

B

Basic Cisco MB Configuration

Hardware Requirements [2-1](#)

Software Requirements [2-1](#)

C

Cisco MB Configurations

With Unified CCE [1-1](#)

Classic HTTP proxy mode [4-4](#)

Configuring Cisco MB [4-3](#)

CTI Strategies [2-3](#)

E

Errors

Logging to Windows Event Log [5-3](#)

F

Firewall Communication

Classic HTTP Proxy Mode [4-4](#)

networking considerations [4-4](#)

Polling Over Outbound Socket Connection
Mode [4-3](#)

H

hardware requirements

Cisco MB with Unified CCE [2-2](#)

I

IIS

restarting [4-5](#)

Installing the Cisco MB software [4-2](#)

J

Java Development Kit version [2-2](#)

L

Logging to Windows Event Log [5-3](#)

N

networking considerations [4-4](#)

P

post-installation tasks

- activate Windows messaging [5-3](#)

- configuring Cisco MB for autostart [5-2](#)

- granting access to Cisco MB [5-1](#)

pre-installation tasks

- Understanding ServletExec [3-2](#)

- Verifying IIS is installed [3-2](#)

R

Requirements

- Cisco MB with Unified CCE [2-1](#)

resource.properties file

- example [5-1](#)

S

ServletExec

- installing [3-2](#)

software requirements

- Cisco MB with Unified CCE [2-2](#)

Starting Cisco MB [4-5](#)

T

Troubleshooting Tips [6-2](#)

- Blank page is displayed when trying to access the Cisco MB Administration page [6-3](#)

- Cannot login to the Cisco MB administration desktop after installation [6-2](#)

W

Windows Messaging [5-3](#)