Avaya Interaction Center

Release 7.1

Installation and Configuration

07-300569
Release 7.1
May 2006

© 2000 to 2006 Avaya Inc. All Rights Reserved.

Notice

While reasonable efforts were made to ensure that the information in this document was complete and accurate at the time of printing, Avaya Inc. can assume no liability for any errors. Changes and corrections to the information in this document might be incorporated in future releases.

Documentation disclaimer

Avaya Inc. is not responsible for any modifications, additions, or deletions to the original published version of this documentation unless such modifications, additions, or deletions were performed by Avaya. Customer and/or End User agree to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation to the extent made by the Customer or End User.

Link disclaimer

Avaya Inc. is not responsible for the contents or reliability of any linked Web sites referenced elsewhere within this documentation, and Avaya does not necessarily endorse the products, services, or information described or offered within them. We cannot guarantee that these links will work all the time and we have no control over the availability of the linked pages.

Warranty

Avaya Inc. provides a limited warranty on this product. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya's standard warranty language, as well as information regarding support for this product, while under warranty, is available through the Avaya Support Web site:

http://www.avaya.com/support

License

USE OR INSTALLATION OF THE PRODUCT INDICATES THE END USER'S ACCEPTANCE OF THE TERMS SET FORTH HEREIN AND THE GENERAL LICENSE TERMS AVAILABLE ON THE AVAYA WEB SITE http://support.avaya.com/LicenseInfo/ ("GENERAL LICENSE TERMS"). IF YOU DO NOT WISH TO BE BOUND BY THESE TERMS, YOU MUST RETURN THE PRODUCT(S) TO THE POINT OF PURCHASE WITHIN TEN (10) DAYS OF DELIVERY FOR A REFUND OR CREDIT.

Avaya grants End User a license within the scope of the license types described below. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the Documentation or other materials available to End User. "Designated Processor" means a single stand-alone computing device. "Server" means a Designated Processor that hosts a software application to be accessed by multiple users. "Software" means the computer programs in object code, originally licensed by Avaya and ultimately utilized by End User, whether as stand-alone Products or pre-installed on Hardware. "Hardware" means the standard hardware Products, originally sold by Avaya and ultimately utilized by End User.

License type(s)

Concurrent User License (CU). End User may install and use the Software on multiple Designated Processors or one or more Servers, so long as only the licensed number of Units are accessing and using the Software at any given time. A "Unit" means the unit on which Avaya, at its sole discretion, bases the pricing of its licenses and can be, without limitation, an agent, port or user, an e-mail or voice mail account in the name of a person or corporate function (e.g., webmaster or helpdesk), or a directory entry in the administrative database utilized by the Product that permits one user to interface with the Software. Units may be linked to a specific, identified Server.

Database License (DL). Customer may install and use each copy of the Software on one Server or on multiple Servers provided that each of the Servers on which the Software is installed communicate with no more than a single instance of the same database.

Shrinkwrap License (SR). With respect to Software that contains elements provided by third party suppliers, End User may install and use the Software in accordance with the terms and conditions of the applicable license agreements, such as "shrinkwrap" or "clickwrap" license accompanying or applicable to the Software ("Shrinkwrap License"). The text of the Shrinkwrap License will be available from Avaya upon End User's request (see "Third-party Components" for more information).

Copyright

Except where expressly stated otherwise, the Product is protected by copyright and other laws respecting proprietary rights. Unauthorized reproduction, transfer, and or use can be a criminal, as well as a civil, offense under the applicable law.

Third-party components

Certain software programs or portions thereof included in the Product may contain software distributed under third party agreements ("Third Party Components"), which may contain terms that expand or limit rights to use certain portions of the Product ("Third Party Terms"). Information identifying Third Party Components and the Third Party Terms that apply to them is available on the Avaya Support Web site:

http://support.avaya.com/ThirdPartyLicense/

Preventing toll fraud

"Toll fraud" is the unauthorized use of your telecommunications system by an unauthorized party (for example, a person who is not a corporate employee, agent, subcontractor, or is not working on your company's behalf). Be aware that there can be a risk of toll fraud associated with your system and that, if toll fraud occurs, it can result in substantial additional charges for your telecommunications services.

Avaya fraud intervention

If you suspect that you are being victimized by toll fraud and you need technical assistance or support, call Technical Service Center Toll Fraud Intervention Hotline at +1-800-643-2353 for the United States and Canada. For additional support telephone numbers, see the Avaya Support Web site:

http://www.avaya.com/support

Trademarks

Avaya, the Avaya logo, DEFINITY, MultiVantage, and COMPAS are either registered trademarks or trademarks of Avaya Inc. in the United States of America and/or other jurisdictions.

All other trademarks are the property of their respective owners.

Downloading documents

For the most current versions of documentation, see the Avaya Support Web site:

http://www.avaya.com/support

COMPAS

This document is also available from the COMPAS database. The COMPAS ID for this document is 113231.

Avaya support

Avaya provides a telephone number for you to use to report problems or to ask questions about your product. The support telephone number is 1-800-242-2121 in the United States. For additional support telephone numbers, see the Avaya Support Web site:

http://www.avaya.com/support

Contents

Preface

This section contains the following topics:

Purpose

The purpose of this guide is to provide detailed information about how to install and configure an out-of-the-box Avaya Interaction Center Release 7.1 system.

Audience

This guide is intended primarily for those who use Avaya Interaction Center (Avaya IC). You should use this guide as an information source for:

- Installing all Avaya IC components.
- Configuring an out-of-the-box Avaya IC system for a development environment, without customizations.

Related documents

The following documents in the Avaya IC Release 7.1 documentation set are related to the installation and configuration of an Avaya IC system:

IC Installation Planning and Prerequisites**:** This document provides information about the supported third-party platforms and other prerequisites required for Avaya Interaction Center, including installation information for those platforms. *IC Installation Planning and Prerequisites* also includes planning and deployment information for Avaya Interaction Center.

OA Installation Planning and Prerequisites**:** This document provides information about the supported third-party platforms and other prerequisites required for Avaya Operational Analyst, including installation information for those platforms. *OA Installation Planning and Prerequisites* also includes planning and deployment information for Avaya Operational Analyst.

OA Installation and Configuration**:** This document provides installation information for all Avaya Operational Analyst components.

Chapter 1: Introduction

Use the following information and procedures to install and configure an out-of-the-box Avaya IC system. If your Avaya IC system includes some customizations, install a development system first. You must test your customizations on the development system before you deploy your production system.

This section describes useful information that you should know before you install and configure an Avaya IC system. This section includes the following topics:

Avaya IC installation files

Avaya Interaction Center (Avaya IC) provides the installation files on the CD-ROMs described in the following table.

CD-ROM	Contents
Avaya IC CD-ROM 1 Windows Servers, Administration	Contains the following files for installation on Windows: • Installers for: – Core servers, including Avaya Full Text Search Engine, Web Scheduled Callback, Business Advocate, Client SDK components, and Web Services components – Avaya Agent Web Client connector – Design & Administration Tools • Documentation • Connectors for supported IVRs • Server SDK

CD-ROM	Contents
Avaya IC CD-ROM 2 Solaris Servers	Contains the following files for installation on Solaris: ● Installers for: – Core servers, including Avaya Full Text Search Engine, Web Scheduled Callback, Business Advocate, Client SDK components, and Web Services components – Avaya Agent Web Client connector ● Connectors for supported IVRs ● Server SDK
Avaya IC CD-ROM 3 AIX Servers	Contains the following files for installation on AIX: ● Installers for: – Core servers, including Avaya Full Text Search Engine, Web Scheduled Callback, Business Advocate, Client SDK components, and Web Services components – Avaya Agent Web Client connector ● Connectors for supported IVRs ● Server SDK
Avaya IC CD-ROM 4 Avaya Agent	Contains site preparation wizards for: ● Avaya Agent ● Avaya Agent Web Client
Avaya IC CD-ROM 5 Siebel Integration	Contains files and documentation required to integrate Avaya IC with Siebel 7.x.
Avaya IC CD-ROM 6 Documentation	Contains the complete set of documentation for Avaya IC with a search function that lets you search across the entire set.

Installing Avaya IC with Avaya Operational Analyst

Avaya Operational Analyst (Avaya OA) provides reporting functionality for Avaya IC.

This section includes the following topics:

Installation order

You must follow the correct installation order to ensure that IC Repository is correctly configured for both Avaya IC and Avaya OA.

Install and configure the components of Avaya IC and Avaya OA in the following order:

1. Install and configure all prerequisites in the following documentation, including the installation of your database software and the creation of your database instance:
   a. For Avaya IC, see *IC Installation Planning and Prerequisites*.
   b. For Avaya OA, see *Operational Analyst Installation Planning and Prerequisites*.
2. Install the Avaya IC servers and administration components, as described in Installing Avaya IC server and administration components on page 29.
3. Configure the additional Avaya IC components required for the deployment, as described in this manual.
4. Install and configure Avaya OA for Avaya IC, as described in *Operational Analyst Installation and Configuration*.

Database properties

Both Avaya IC and Avaya OA require access to the IC Repository database.

Avaya IC and Avaya OA use the values shown in the following table for their database properties.

Property	DB2	Oracle	SQL Server
Database Administration Login	db2inst1	sys	sa level user name
Database Administration Password	db2inst1 password	sys password	sa level password
IC Repository database name See Configuring the IC Repository database connection on page 67.	Database name that you enter in Database Designer. For example, **repository**.	Database name for the Oracle user that you enter in Database Designer. For example, **repository**.	Database schema name that you enter in Database Designer. For example, **repository**.

Customizing Avaya IC

Use the information and procedures in this guide to install and configure an out-of-the-box Avaya IC system with little or no customization. If your Avaya IC system includes customization requirements, use this guide to install a development system. Use the development system to test and, if desired, customize your Avaya IC system.

For more information on how to customize Avaya IC components, see the other documentation in the Avaya IC documentation set. The introduction provided on the Avaya IC documentation CD-ROM includes a complete description of all documentation in the Avaya IC documentation set.

The following table describes some of the Avaya IC documentation that you can use to customize an Avaya IC system.

Avaya IC Component	Documents
Avaya Agent	• *Avaya Agent Integration* • *IC Administration Volume 2: Agents, Customers, & Queues*
Avaya Agent Web Client	• *Avaya Agent Web Client Customization* • *IC Administration Volume 2: Agents, Customers, & Queues*
Avaya IC databases and data models	• *IC Database Designer Application Reference* • *Data Model files*
Client SDK	• *IC Client SDK Programmer Guide*
Servers	• *IC Administration Volume 1: Servers & Domains* • *Agent Data Unit Server Programmer Guide* • *Electronic Data Unit Server Programmer Guide* • *IC Telephony Connectors Programmer Guide* • *Core Services Programmer Guide* • *IC Client and Server Programmer Design Guide* • *VOX Server Programmer Guide*
Telephony	• *IC Administration Volume 1: Servers & Domains* • *IC Telephony Connectors Programmer Guide* • *VOX Server Programmer Guide* • *External Function Library for Avaya IVR* • *Migration Guide*
Web Services	• Web Services HTML document
Workflows	• *Avaya Workflow Designer User Guide* • *Avaya IC Workflow API Reference* • *Media Workflow Reference* • *Agent Script Workflow Reference* • *IC Scripts Language Reference* • *IC Scripts VBA Scripting Reference*
Avaya Business Advocate	• *IC Business Advocate Configuration and Administration* • *Media Workflow Reference*
Avaya IC for Siebel 7	• *Avaya IC for Siebel 7 Integration*

Chapter 2: Installing Avaya IC components

Install and configure the Avaya IC components in the order that the topics appear in this section. For example, install and configure the primary servers before you install and configure the Design & Administration Tools.

This section includes the following topics:

CAUTION:
Do not install Avaya IC on machines that also host software that filters or controls network access. These types of software can cause Avaya IC to fail or seriously impact performance. For example, pornography filters or software firewalls can affect network access in several ways. They can cause a slowdown in network access, cause applications that open a large number of sockets to fail, or rewrite packets.

For information about deploying Avaya IC agent applications, see:

Before you install Avaya IC

This section describes the steps that you must perform before you install Avaya IC components. This section includes the following topics:

Readme files

Read the following Avaya IC readme files:

- Avaya IC Readme file on the Avaya IC CD-ROM
- Avaya IC Readme Addendum on the CRM Technical Support Website at http://www.avaya.com/support/qq

Avaya IC prerequisites

Read the *IC Installation Planning and Prerequisites* and install all prerequisite components.

License file

Obtain the necessary Avaya IC license file for your Avaya IC system. For more information, see *IC Installation Planning and Prerequisites*.

Required administrator privileges

All Avaya IC users who perform certain tasks require administrator privileges. This section includes the following topics that describe the administrator privileges required for the different operating systems:

- Required administrator privileges for Windows on page 25.
- Required administrator privileges for Solaris and AIX on page 25.

Required administrator privileges for Windows

All Avaya IC users who perform the following tasks must have a Windows Administrator login or a Windows login with administrator privileges.

- Install and configure Avaya IC servers
- Install or use Design & Administration Tools

Required administrator privileges for Solaris and AIX

All Avaya IC users who install and configure Avaya IC servers require one of the following UNIX accounts, depending upon which tasks they need to perform.

Root user: You need this account when you:

- Install Avaya IC on a machine that will host a Telephony server for an Avaya switch with Definity or Communication Manager software.
- Configure the Web applications with the Configuration Tool, including the Website, Email Template Administration, Web License Manager, and Letter Generator.

Installation user: Use this account to perform all tasks to install and configure Avaya IC that do not require the root user. The Avaya IC installation directory must be owned by this account.

For example, you can create an installation user account named **avaya**.

Important:
If you do not use a root account to install Avaya IC servers on a machine, and need to configure that machine with a Telephony server for an Avaya switch with DEFINITY or Communication Manager software, reinstall the Avaya IC servers under the root account.

Solaris machines

If you host your servers on Solaris:

- Install a Windowing environment such as X-Windows.
- Set the `DISPLAY` parameter.
- Make sure that the server machine has sufficient space in the `/var/tmp` directory for the Java Virtual Machine installation. The Avaya IC installer typically requires at least 360MB of extra temp space.
- Install the appropriate locales for languages supported by your system. For more information about the required locales, see *IC Installation Planning and Prerequisites*.

AIX machines

If you host your servers on AIX:

- Install a Windowing environment such as X-Windows.
- Set the `DISPLAY` parameter.
- Make sure that the server machine has sufficient space in the `/tmp` directory for the Java Virtual Machine installation. The Avaya IC installer typically requires at least 360MB of extra temp space.
- Install the appropriate locales for languages supported by your system. For more information about the required locales, see *IC Installation Planning and Prerequisites*.

Cautions and tips for installing Avaya IC components

This section includes some important cautions and tips that you need to consider when you install Avaya IC components.

This section includes the following topics:

Cautions and tips for installing Avaya IC servers

Consider the following important cautions and tips when you install Avaya IC servers:

Required disk space

Make sure that you have sufficient space on the target machine to install the selected files. The Avaya IC installation does not check the amount of free disk space on the machine until after you select the components to install.

HP Openview

If a machine that will host an ORB server also hosts HP Openview, turn off HP Openview before you install the Avaya IC servers. If you leave HP Openview running on the machine, HP Openview may prevent the Avaya IC installer from completely copying all required files to the `IC_INSTALL_DIR\IC71\bin` directory.

In a Windows environment, stop the HP ITO Agent service in the Services control panel to shutdown HP Openview. For more information about HP Openview, or for information on how to shutdown HP Openview on Solaris or AIX, see the documentation provided by HP.

InstallShield mode

Only the Avaya Agent site preparation wizard can run in silent mode. All other Avaya IC installers can only run in console mode.

Backup configuration files

The Avaya IC installer backs up configuration files in the following directory before making any changes to those files: `IC_INSTALL_DIR\IC71\bin\config\backup`.

Cautions and tips for Design and Administration Tools

Consider the following important cautions and tips when you install and use the Avaya IC Design and Administration Tools:

- Components installed with Design and Administration Tools on page 28.
- Design and Administration machines on page 28.
- Supported operating systems on page 28.
- Running multiple instances of IC Manager on page 29.

Components installed with Design and Administration Tools

Avaya IC installs all of the Design and Administration Tools on the target machine. You cannot select which tools to install.

The tools and files that you install with the Design and Administration Tools are:

- IC Manager
- Avaya Workflow Designer, with blocks, sample workflows, and related files
- Avaya Database Designer, with the IC Script Editor, design files, and related files

Design and Administration machines

IC Manager and other administrative applications can potentially consume a significant amount of CPU resources. To ensure that the requirements of IC Manager do not interfere with the performance of your Avaya IC servers, deploy your Design and Administration Tools on a dedicated machine.

Supported operating systems

Design and Administration Tools work only on a supported Windows operating system. For more information, see *IC Installation Planning and Prerequisites*.

Running multiple instances of IC Manager

IC Manager does not support concurrent administration. When an administrator selects and updates a record, such as a server or an agent, IC Manager does not lock that record. Another administrator can open and update the same record.

CAUTION:
Simultaneous administration of servers, domains, and Directory server tables in more than one IC Manager can cause corruption of the configuration files and loss of configuration data.

If you plan to have more than one instance of IC Manager, you must clearly define the administrative policies for Avaya IC. For example:

- Only use one instance of IC Manager at a time to administer servers.
- Determine which Avaya IC elements an administrator can update, and assign the appropriate permissions to the login ID for that administrator.
- Do not allow administrators to log in to more than one instance of IC Manager with the same login ID and password.

For more information about multiple instances of IC Manager, see *IC Administration Volume 1: Servers & Domains*.

Installing Avaya IC server and administration components

Tip:
For information about the components on each Avaya IC CD-ROM, see Avaya IC installation files on page 17.

This section includes the following topics:

Installing Avaya IC server and administration components on Windows

You can only install one component at a time with the Avaya IC Windows Servers, Administration installer. You cannot select multiple components to install simultaneously.

To install Avaya IC server and administration components on Windows:

1. Log in to the machine with an account that has the required Administrator privileges.
2. Insert Avaya IC Release 7.1 CD-ROM 1.

   The Avaya IC installer starts automatically. If you disabled Autorun on the machine, navigate to the Servers directory on the CD-ROM and run `install.bat`.
3. When the Avaya IC installer opens, read the entire Avaya IC license agreement carefully, then accept the terms of the agreement. Select **Next**, then follow the prompts in the installer.

   The Avaya IC installer exits if you do not agree to the terms of the agreement.
4. In the Product Installation screen, select one of the options in the following table to install the required component:

Option	Installation location	Files Installed
Core Servers	Core server machine	• Avaya IC core servers • Avaya Full Text Search Engine • Web Scheduled Callback • Business Advocate servers and administrative client • Client SDK components • Web Services components
IC Design and Administration Tools	Design and administration machine	• IC Manager • Database Designer • Workflow Designer
Avaya Agent Web Client Connector	IBM Websphere machine for Avaya Agent Web Client	• Vesp and DCO bridges • JACL scripts • Configuration Tools

5. Continue to follow the prompts in the Avaya IC Windows installer.

   The Avaya IC installer can take several minutes to copy the requested files to the machine. If the target machine does not have sufficient space to install the components, the Avaya IC installer displays an error message.

6. The next step in the Avaya IC installation depends upon the components you want to host on the target machine. Perform one of the following steps:

Type of servers	Location of steps
Primary ORB server machine	Configuring the primary ORB server environment on page 33
Secondary ORB server machine, including Client SDK server machine	Configuring a secondary ORB server environment on page 35
Avaya Agent Web Client	Deploying Avaya Agent Web Client on page 327

Installing Avaya IC components on Solaris and AIX

CAUTION:
Do not install Avaya IC servers on Solaris if you have not yet installed the appropriate locales for those operating systems. For more information about the required locales, see *IC Installation Planning and Prerequisites*.

You can only install one component at a time with the Avaya IC Solaris Servers installer and Avaya IC AIX Servers installer. You cannot select multiple components to install simultaneously.

To install Avaya IC server components on Solaris or AIX:

1. Log in to the machine with an account with the required Administrator privileges.
2. Insert one of the following Avaya IC Release 7.1 CD-ROMs:
   - Avaya IC Release 7.1 CD-ROM 2 for Solaris servers
   - Avaya IC Release 7.1 CD-ROM 3 for AIX servers

   The Avaya IC CD-ROM mounts automatically.
3. To start the Avaya IC installation:
   a. Change to the following directory on the CD-ROM:

Operating system	Directory
Solaris	`<CD-ROM_drive>/icserverSolaris`
AIX	`<CD-ROM_drive>/icserverAix`

   b. Execute `-install.sh`

   If the default temp directory does not have sufficient space to override the TMPDIR environment variable, run: `./install.sh -is:tempdir <dir_name>`

4. When the Avaya IC installer opens, read the entire Avaya IC license agreement carefully, then accept the terms of the agreement. Select **Next**, then follow the prompts in the installer.

   The Avaya IC installer exits if you do not agree to the terms of the agreement.

5. In the Product Installation screen, select one of the options in the following table to install the required component:

Option	Location	Files Installed
Core Servers	Core server machine	• Avaya IC core servers • Avaya Full Text Search Engine • Web Scheduled Callback • Business Advocate Telephony Services Adaptor and Web Advocate Adaptor servers only • Client SDK components • Web Services components
Avaya Agent Web Client Connector	IBM Websphere machine for Avaya Agent Web Client	• Vesp and DCO bridges • JACL scripts • Configuration Tools

6. Continue to follow the prompts in the Avaya IC Windows installer.

   The Avaya IC installer can take several minutes to copy the requested files to the machine. If the target machine does not have sufficient space to install the components, the Avaya IC installer displays an error message.

7. The next step in the Avaya IC installation depends upon the components you want to host on the target machine. Perform one of the following steps:

Machine	Steps
Primary ORB server machine	Configuring the primary ORB server environment on page 33
Secondary ORB server machine, including Client SDK server machine	Configuring a secondary ORB server environment on page 35
Avaya Agent Web Client	Deploying Avaya Agent Web Client on page 327

Configuring the ORB server environment

Important:
For Solaris and AIX only, the Configuration Tool changes the ownership of the implementation file (vesp.imp) and the interface file (vespidl.pk) to root. If you do not want to run Avaya IC as root, you must change the ownership of these files as described in Changing ownership for Avaya IC - Solaris and AIX only on page 38.

You must run the Configuration Tool on every machine that hosts an ORB server to create a server environment. The configuration mode that you select in the installer depends upon the type of ORB server that you plan to host on the machine.

The machine that hosts the primary ORB server requires a primary server environment. All other machines require a secondary server environment.

This section includes the following topics:

Configuring the primary ORB server environment

This procedure continues from Installing Avaya IC server and administration components on page 29.

To configure the primary server environment:

1. In the **Initial Configuration** tab of the Configuration Tool, confirm that **Primary** is selected in the **Select Mode** drop-down list.
2. Confirm that the IP address in the **IP Address** drop-down list is the correct IP address for the machine that hosts the primary ORB server.

   Important:
   If the primary ORB server runs on a machine with multiple network interface cards, you must select the IP address for the first network interface card on the machine. The primary ORB server cannot run on any other network interface card.
3. Make sure the port assignment in the **Start Port** field is an available port on the target machine. Type a new port assignment if necessary.
4. Select **Start ORB Server**.

5. If the machine will host a Telephony server:
   a. Select and check the **Telephony Switch** box.
   b. From the **Telephony Switch** drop-down list, select the name of the switch with which the Telephony server will communicate.

      The Telephony server must communicate with a switch that is supported for the operating system of the machine. For example, do not select a Nortel switch if you plan to host the Telephony server on an AIX machine. For more information about switch support, see *IC Installation Planning and Prerequisites*.
6. If the Avaya IC system includes an Oracle database:
   a. Select and check the **Oracle Setup** box.
   b. Type the NLS Lang parameter in the **NLS Lang** field to specify the character set of the database.

      The NLS Lang setting must match the value used to create the Oracle database. This value must include UTF8. For example, if your database uses US English language conventions, enter **`AMERICAN_AMERICA.UTF8`**. For more information, see About the NLS Lang setting for Oracle on page 378.
   c. Type the home directory of the Oracle client on the machine that hosts the core servers in the **Oracle Home** field.

      For example, type `/opt/oracle/Ora_ic`
   d. For Oracle databases on Solaris only, type the Oracle SID of the database in the **Oracle SID** field.

      For example, type `icutf8db`. The Oracle SID field is case-sensitive.
   e. For Oracle databases on Solaris only, select the correct version of Oracle from the **Oracle Version** field.
7. If the Avaya IC system includes a DB2 database:
   a. Select and check the **DB2 Setup** box.
   b. Type the home directory of the DB2 client on the machine that hosts the core servers in the **DB2 Home** field.

      For example, type `/usr/lpp/db2_ic`
   c. Type the name of the DB2 instance in the **DB2 Instance** field.

      For example, type `db2inst1`
8. If you host the servers on Solaris or AIX, select the primary locale from the **Locale** drop-down list.

   The drop-down list includes all of the locales supported by the operating system. For example, if your servers use an English locale:

   - For AIX, select EN_US.
   - For Solaris, select en_US.UTF-8.

9. Select **Apply Settings** in the Configuration Tool to configure and start the core servers.
10. Select **OK** in the **Success** dialog box.
11. Select **Exit**.

    The Configuration Tool closes and returns you to the installer.
12. In the Avaya IC installer, follow the prompts.

    For Windows, if you leave the **View Readme** field checked, the Avaya IC Readme opens in Adobe Acrobat. After you have reviewed the Readme, close Acrobat to return to the Avaya IC installer. On Solaris and AIX, the Readme is available on the CD-ROM.
13. The next step in the Avaya IC installation depends upon the components you want to host on the target machine. Perform one of the following steps:

Type of servers	Location of steps
Core servers without Business Advocate	Configuring databases on page 53
Core servers with Business Advocate	Setting up Business Advocate on page 40
Client SDK server components	Deploying Client SDK components on page 365

Configuring a secondary ORB server environment

This procedure continues from Installing Avaya IC server and administration components on page 29.

To configure the secondary server environment:

1. In the **Initial Configuration** tab of the Configuration Tool, confirm that **Secondary** is selected in the **Select Mode** drop-down list.
2. Confirm that the IP address in the **IP Address** drop-down list is the correct IP address for the machine that hosts the secondary ORB server.

   Important:
   If the secondary ORB server runs on a machine with multiple network interface cards, you must select the IP address for the first network interface card on the machine. The ORB server cannot run on any other network interface card.
3. Make sure the port assignment in the **Secondary ORB Port** field is an available port on the target machine. Type a new port assignment if necessary.
4. In the **Primary Host Name** field, type the IP Address or the fully-qualified domain name of the machine that hosts the primary ORB server.

5. In the **Primary ORB Port** field, confirm that the port is the one you configured for the primary ORB server.
6. In the **IC Login** field, type the administrative login ID that will run the Avaya IC servers.

   For more information, see Setting up administrative accounts on page 93.
7. In the **IC Password** field, type the password associated with the IC Login.
8. In the **IC Domain** field, type the name of the Avaya IC domain that includes the primary ORB server. This domain is typically the Default domain.
9. Select **Start ORB Server**.
10. If the machine will host a Telephony server:
    a. Select and check the **Telephony Switch** box.
    b. From the **Telephony Switch** drop-down list, select the name of the switch with which the Telephony server will communicate.

       The Telephony server must communicate with a switch that is supported for the operating system of the machine. For example, do not select a Nortel switch if you plan to host the Telephony server on an AIX machine. For more information about switch support, see *IC Installation Planning and Prerequisites*.
11. If the Avaya IC system includes an Oracle database:
    a. Select and check the **Oracle Setup** box.
    b. Type the NLS Lang parameter in the **NLS Lang** field to specify the character set of the database.

       The NLS Lang setting must match the value used to create the Oracle database. This value must include UTF8. For example, if your database uses US English language conventions, enter **`AMERICAN_AMERICA.UTF8`**. For more information, see About the NLS Lang setting for Oracle on page 378.
    c. Type the home directory of the Oracle client on the machine that hosts the core servers in the **Oracle Home** field.

       For example, type `/opt/oracle/Ora_ic`
    d. For Oracle databases on Solaris only, type the Oracle SID of the database in the **Oracle SID** field.

       For example, type `icutf8db`. The Oracle SID field is case-sensitive.
    e. For Oracle databases on Solaris only, select the correct version of Oracle from the **Oracle Version** field.

12. If the Avaya IC system includes a DB2 database:
    a. Select and check the **DB2 Setup** box.
    b. Type the home directory of the DB2 client on the machine that hosts the core servers in the **DB2 Home** field.

       For example, type `/usr/lpp/db2_ic`
    c. Type the name of the DB2 instance in the **DB2 Instance** field.

       For example, type `db2inst1`
13. If you host the servers on Solaris or AIX, select the primary locale from the **Locale** drop-down list.

    The drop-down list includes all of the locales supported by the operating system. For example, if your servers use an English locale:
    - For AIX, select EN_US.
    - For Solaris, select en_US.UTF-8.
14. Select **Apply Settings** in the Configuration Tool to configure and start the core servers.
15. Select **OK** in the **Success** dialog box.
16. Select **Exit**.

    The Configuration Tool closes and returns you to the installer.
17. In the Avaya IC installer, follow the prompts.

    For Windows, if you leave the **View Readme** field checked, the Avaya IC Readme opens in Adobe Acrobat. After you have reviewed the Readme, close Acrobat to return to the Avaya IC installer. On Solaris and AIX, the Readme is available on the CD-ROM.
18. The next step in the Avaya IC installation depends upon the components you want to host on the target machine. Perform one of the following steps:

Type of servers	Location of steps
Core servers without Business Advocate	Configuring databases on page 53
Core servers with Business Advocate	Setting up Business Advocate on page 40
Client SDK server components	Deploying Client SDK components on page 365

Changing ownership for Avaya IC - Solaris and AIX only

If you installed Avaya IC as the root user and do not want to run Avaya IC servers and services as root in your Solaris or AIX system, you need to change the ownership of the Avaya IC directories and files.

Important:
Avaya recommends that users avoid running Avaya IC software as the root user wherever possible for security reasons. Create a user for the Avaya IC system before you perform these steps. For more information, see *IC Installation Planning and Prerequisites*.

This section includes the following steps that you must perform if you do not want to run Avaya IC as root:

1. Changing ownership of the Avaya IC directories and files on page 38.
2. Changing ownership for Telephony server - Solaris with Avaya switch only on page 39.
3. Changing ownership for Telephony server - AIX with Avaya switch only on page 39.

Changing ownership of the Avaya IC directories and files

To change ownership of the Avaya IC directories and files:

1. Log in as root user.
2. Navigate to `IC_INSTALL_DIR/IC71/bin`.
3. Shutdown all Avaya IC servers, as described in Stopping all servers on page 125.
4. Navigate to the parent directory of `IC_INSTALL_DIR/IC71/`.
5. Execute the following command:

   ```
   chown -R <avayauser>:<avayagroup> IC71
   ```

   where <*avayauser*> represents the non-root user that you use to run the Avaya IC components and <*avayagroup*> is the primary group for <*avayauser*>.
6. Switch to <*avayauser*> and restart the Avaya IC servers, as described in Starting and stopping servers in IC Manager on page 125.

Changing ownership for Telephony server - Solaris with Avaya switch only

For a Solaris system that includes an Avaya switch with Definity or Communication Manager software, change the ownership of every Telephony server.

You configure the SUID bit and root ownership to ensure that the Telephony server for the Avaya switch can start up as the root user to enable agent event reporting. The Telephony server resets its process user ID to <*avayauser*> immediately after startup.

To change ownership for the Telephony server on Solaris:

1. Log in as root user.
2. Navigate to `IC_INSTALL_DIR/IC71/bin`.
3. Execute the following command:

   `chown root cvlansrv`
4. Execute the following command to verify that the SUID bit is set on cvlansrv:

   `ls -l cvlansrv`
5. Execute the `crle` command as follows:

   `crle -s AVAYA_IC71_HOME/lib`

Changing ownership for Telephony server - AIX with Avaya switch only

For an AIX system that includes an Avaya switch with Definity or Communication Manager software, change the ownership of every Telephony server.

During the Avaya IC installation, the SUID bit is automatically set to give root ownership to the Telephony server for the Avaya switch. Root ownership is not required on AIX.

To remove the root permissions:

1. Log in as root user.
2. Navigate to `IC_INSTALL_DIR/IC71/bin`.
3. Execute the following command:

   `chmod u-s cvlansrv`
4. Execute the following command to verify that the SUID bit is not set on cvlansrv:

   `ls -l cvlansrv`

Setting up Business Advocate

This section includes the following topics:

For information about Business Advocate components and how to configure Business Advocate, see *IC Business Advocate Configuration and Administration*.

Important:
The Resource Manager server and Resource Manager components support the Windows 2003 server operating system only. For more information, see *IC Installation Planning and Prerequisites*.

Required administrator privileges for Business Advocate

The following table describes the administrator privileges required to install, configure, and run Business Advocate components on server machines

Implementation mode	Required administrator privileges
Workgroup mode	Administrative user with "Logon as Service" privileges
Active Directory mode	Active Directory user with local server administrator rights and "Logon as Service" privileges

Prerequisites for Business Advocate

If you do not perform all of the prerequisites for Business Advocate, including the installation of Avaya IC, you cannot set up Business Advocate.

Before you install Business Advocate components, do the following:

1. Complete all prerequisites for Business Advocate, as described in *IC Installation Planning and Prerequisites*.
2. Install the Avaya IC server and administration components on the target machines, as described in Installing Avaya IC server and administration components on page 29.

Tip:
For Business Advocate systems that include Standby Resource Manager servers or Administration Tools on a remote server from the Resource Manager server, see *IC Installation Planning and Prerequisites* for additional configuration details.

Sharing the Nethome directory

The Avaya IC Windows installer creates the Nethome directory for Business Advocate. On the machine that will host the first Logical Resource Manager, you must share the Nethome directory with the required privileges for Business Advocate to function correctly.

To share the Nethome directory:

1. In Windows Explorer, share the Nethome directory as **Nethome**.
2. Change the permissions on the share to provide Write and Read permissions for the Business Advocate administrative users.

Configuring a Business Advocate environment

You must configure a Business Advocate environment on all machines that host:

- First Logical Resource Manager
- Standby Resource Manager
- Additional Logical Resource Manager
- Business Advocate administration tools

To create the Business Advocate environment:

1. Log in to the machine with an account that has the required administrator privileges, as described in Required administrator privileges for Business Advocate on page 40.
2. Select **Start** > **Programs** > **Avaya Interaction Center 7.1** > **Advocate Configure**.

   If the Configuration Tool displays a message box that alerts you to a missing license, select **OK**. Verify that your Avaya IC license includes Business Advocate.
3. In the **Configuration** dialog box, select one of the following options from the **Configuration Type** group:
   - First Logical Resource Manager
   - Stand-By Resource Manager
   - Additional Logical Resource Manager
   - Administrative Client
4. In the **Nethome Share** field, type the path for the shared nethome directory in UNC format.

   UNC format is `\\<machine_name>\nethome`

   If you do not know the path, select **Browse** and navigate to the directory through Network Neighborhood. If the shared nethome directory is on the same machine, do not select the local machine directly. You must navigate through Network Neighborhood to ensure that the Browse function uses UNC format.
5. In the **Windows User** group, complete the following fields:
   a. In the **Domain\Username** field, type the domain and username of the user account that you created to run Business Advocate services in the following format:

Implementation mode	Domain\Username format
Workgroup mode	*<local_machine_name>*\ *<advocate_administrative_account>*
Active Directory mode	*<Active_Directory_domain>*\ *<advocate_administrative_account>*

b. In the **Password** field, type the password for the Active Directory user account.

c. In the **Confirm password** field, re-type the password.

6. Select **Start**.
7. The next step depends upon the Business Advocate components you want to host on the target machine. Perform one of the following steps:

Business Advocate component	Location of steps
First Logical Resource Manager	Building the database schema for the first Logical Resource Manager on page 43
Additional Logical Resource Manager	Building the database schema for an additional Logical Resource Manager on page 47

Building the database schema for the first Logical Resource Manager

To build the Business Advocate database schema for the first Logical Resource Manager, follow the steps in one of the following topics:

- Building the Business Advocate database schema for SQL Server on page 43.
- Building the Business Advocate database schema for Oracle on page 45.

Note:
Business Advocate databases do not support DB2.

Building the Business Advocate database schema for SQL Server

To build the Business Advocate database schema for SQL Server:

1. In the **Build Database Schema** window, complete the fields in the following table.

Field	Recommended entry	Notes
Select a DBMS	Select SQL Server.	
Username	Type a DBA user name for the Business Advocate databases.	For example, a DBA user name for SQL Server is **sa**.
Password	Type the password for the DBA user name.	Do not leave your DBA password blank.

2. Check the **Build** box next to the **Local System Store** field, and complete the fields in the following table.

Field	Recommended entry	Notes
Schema file	Accept the default.	Business Advocate automatically completes this field with the network home directory that you specified during installation.
Database Server	Type the name of the machine that hosts the database.	The database server is the machine that hosts the Business Advocate database you created when you completed prerequisites.
Database Name	Type advocate.	The database name is the Business Advocate database you created when you completed prerequisites.

3. Check the **Build** box next to the **Shared Resource Store** field, and complete the fields in the following table.

Field	Recommended entry	Notes
Schema file	Accept the default.	Business Advocate automatically completes this field with the network home directory that you specified during installation.
Database Server	Type the name of the machine that hosts the database.	The database server is the machine that hosts the Business Advocate database you created when you completed prerequisites.
Database Name	Type advocate.	The database name is the Business Advocate database you created when you completed prerequisites.

4. Select **Create Schema**.

   This process can take a few minutes to complete the installation and configuration of the database schema. Monitor the messages on the status line at the bottom left of the **Build Database Schema** window. If desired, select **View Log File** to view the log file.

Building the Business Advocate database schema for Oracle

To build the Business Advocate database schema for Oracle:

1. In the **Build Database Schema** window, complete the fields in the following table.

Field	Recommended entry	Notes
Select a DBMS	Select Oracle.	Business Advocate databases do not support DB2.
Username	Type a DBA user name for the Business Advocate databases.	For example, a DBA user name for Oracle is **system**.
Password	Type the password for the DBA user name.	Do not leave your DBA password blank.

2. Check the **Build** box next to the **Local System Store** field, and complete the fields in the following table.

Field	Recommended entry	Notes
Schema file	Accept the default.	Business Advocate automatically completes this field with the network home directory that you specified during installation.
Database Server	Type the name of the machine that hosts the database.	The database server is the machine that hosts the Business Advocate database you created when you completed prerequisites.
Service	Type the Oracle Local Net Service for the machine.	For information on how to identify the Oracle Local Net Service, see the documentation provided by Oracle.

3. Check the **Build** box next to the **Shared Resource Store** field, and complete the fields in the following table.

Field	Recommended entry	Notes
Schema file	Accept the default.	Business Advocate automatically completes this field with the network home directory that you specified during installation.
Database Server	Type the name of the machine that hosts the database.	The database server is the machine that hosts the Business Advocate database you created when you completed prerequisites.
Service	Type the Oracle Local Net Service for the machine.	For information on how to identify the Oracle Local Net Service, see the documentation provided by Oracle.

4. Select **Create Schema**.

   This process can take a few minutes to complete the installation and configuration of the database schema. Monitor the messages on the status line at the bottom left of the **Build Database Schema** window. If desired, select **View Log File** to view the log file.

Building the database schema for an additional Logical Resource Manager

To build the Business Advocate database schema, follow the steps in one of the following topics:

- Building the Business Advocate database schema for SQL Server on page 47.
- Building the Business Advocate database schema for Oracle on page 48.

Building the Business Advocate database schema for SQL Server

To create the Business Advocate database schema:

1. In the **Build Database Schema** window, complete the fields in the following table.

Field	Recommended entry	Notes
Select a DBMS	Select SQL Server.	
Username	Type a DBA user name for the Business Advocate databases.	For example, a DBA user name for SQL Server is **sa**.
Password	Type the password for the DBA user name.	Do not leave your DBA password blank.

2. Type the location of the shared network home directory that you created for the first Logical Resource Manager.

   Use UNC format, for example, `\\<machine_name>\nethome`

   If you do not know the path, select **Browse** and navigate to the directory through Network Neighborhood. If the shared network home directory is on the same machine, do not select the local machine directly. You must navigate through Network Neighborhood to ensure that the Browse function uses UNC format.

3. Check the **Build** box next to System Store, and complete the fields in the following table.

Field	Recommended entry	Notes
Schema file	Accept the default.	Business Advocate automatically completes this field with the network home directory that you specified during installation.
Database Server	Type the name of the machine that hosts the database.	The database server is the machine that hosts the Business Advocate database you created when you completed prerequisites.
Database Name	Type advocate.	The database name is the Business Advocate database you created when you completed prerequisites.

4. Select **Create Schema**.

   Monitor the messages on the status line at the bottom left of the **Build Database Schema** window. If desired, select **View Log File** to view the log file.

5. Select **Close**.
6. Select **OK** for each of the dialog boxes displayed by the Business Advocate installation.

   This process can take a few minutes to complete the installation and configuration of the database schema.

Building the Business Advocate database schema for Oracle

To create the Business Advocate database schema:

1. In the **Build Database Schema** window, complete the fields in the following table.

Field	Recommended entry	Notes
Select a DBMS	Select Oracle.	
Username	Type a DBA user name for the Business Advocate databases.	For example, a DBA user name for Oracle is **system**.
Password	Type the password for the DBA user name.	Do not leave your DBA password blank.

2. Type the location of the shared network home directory that you created for the first Logical Resource Manager.

   Use UNC format, for example, `\\<machine_name>\nethome`

   If you do not know the path, select **Browse** and navigate to the directory through Network Neighborhood. If the shared network home directory is on the same machine, do not select the local machine directly. You must navigate through Network Neighborhood to ensure that the Browse function uses UNC format.

3. Check the **Build** box next to System Store, and complete the fields in the following table.

Field	Recommended entry	Notes
Schema file	Accept the default.	Business Advocate automatically completes this field with the network home directory that you specified during installation.
Database Server	Type the name of the machine that hosts the database.	The database server is the machine that hosts the Business Advocate database you created when you completed prerequisites.
Service	Type the Oracle Local Net Service for the machine.	For information on how to identify the Oracle Local Net Service, see the documentation provided by Oracle.

4. Select **Create Schema**.

   Monitor the messages on the status line at the bottom left of the **Build Database Schema** window. If desired, select **View Log File** to view the log file.

5. Select **Close**.

6. Select **OK** for each of the dialog boxes displayed by the Business Advocate installation.

   This process can take a few minutes to complete the installation and configuration of the database schema.

Verifying permissions for running Avaya OA ECB with Business Advocate

The Event Collector Bridge (ECB) receives information from Business Advocate on a private MSMQ called **pa_admin**. Avaya OA uses this information to report on Business Advocate.

To enable the primary ECB and the standby ECB to use the pa_admin MSMQ, the user ID that runs the Avaya IC ORB Service 7.1 must have the correct permissions.

To enable Avaya OA ECB on Business Advocate, verify that the permissions on the pa_admin MSMQ are set to **Allow** for **Everyone** for the following:

- Receive Message
- Peek Message
- Get Properties
- Get Permissions

Installing the Avaya IC server SDK

Avaya IC provides a Software Development Kit (SDK) for the Avaya IC servers. The SDK includes all of the files that you require to build your own Avaya IC servers, including:

- Header files
- Libraries
- Sample server project files

Tip:
For information about how to install the Client SDK, see Installing Avaya IC server and administration components on page 29.

To install the server SDK:

1. Navigate to the following directory in the Avaya Interaction Center CD-ROM:

Operating system	Directory path
Windows	<*CD-ROM_drive*>`\Utils\TSSdk\sdkwin32.zip`
Solaris	<*CD-ROM_drive*>`/Utils/TSSdk/sparc_tr.Z`
AIX	<*CD-ROM_drive*>`/Utils/TSSdk/rs6k_tr.Z`

2. Copy the compressed SDK file to your Avaya IC directory.
3. Uncompress the file and extract the contents.
4. Verify that the files have been extracted into the folder that you selected. This folder should include C files and a makefile

For more information, see *IC Client and Server Programmer Design Guide*.

Upgrading Avaya IC

For information on how to upgrade your Avaya IC system from an earlier release of Avaya IC, including an Avaya IC 7.x release, see *IC/OA Software Upgrade and Data Migration*.

Reinstalling Avaya IC components

You can reinstall Avaya IC Release 7.1 over an existing Avaya IC Release 7.1 installation. To uninstall Avaya IC files before you reinstall, see Uninstalling Avaya IC on page 440.

To reinstall Avaya IC over an existing Avaya IC installation:

1. Stop all Avaya IC servers and Avaya IC services on the target machine.
2. Follow the instructions in the appropriate section below to reinstall the desired Avaya IC files:
   - Installing Avaya IC server and administration components on page 29.
   - Deploying Avaya Agent on page 307.
   - Deploying Avaya Agent Web Client on page 327.

Chapter 3: Configuring databases

This section describes how to configure the Avaya IC data server, databases, and data sources. All Avaya IC systems require an IC Repository database and a CallCenterQ database.

This section includes the following topics. Perform the steps in these topics in the order set out below.

Before you configure Avaya IC databases

Before you configure the Avaya IC databases, complete the following prerequisites:

Install Avaya IC servers: You must create and configure the primary server environment, then start the primary servers before you can configure the Avaya IC servers and components.

At a minimum, do the following:

- On the machine that hosts the Avaya IC primary ORB server, install the Avaya IC server files and configure the primary server environment.
- On the machine that hosts the Data server, install the Avaya IC server files and configure the server environment. If this machine is different from the one that hosts the primary ORB server, configure a secondary server environment on this machine.

If you have not installed the server files, see Installing Avaya IC server and administration components on page 29.

Install Avaya IC Design & Administration tools: Install these tools on a dedicated machine that has network access to all server machines. For information on how to install these tools, see Installing Avaya IC server and administration components on page 29.

Install database management system: For more information, see *IC Installation Planning and Prerequisites* and the documentation provided with the database management system.

Install and configure the database client software: The database client software also includes the vendor libraries, and support files. Install and configure these files on the machine that hosts the Data server. The Data server requires the database client software to communicate with the database. For example, if your Avaya IC system includes a supported Oracle database, install the Oracle client for that version on the machine that hosts the Data server.

Database connections: Configure and validate the database software connections on the machine where you plan to install the Data server.

Copying the stored procedure library - DB2 only

If you host your Avaya IC databases on DB2, you must copy the qdb2sp stored procedure library from the machine that hosts the primary ORB server to the machine that hosts the Avaya IC database instance.

To copy the qdb2sp stored procedure library to the DB2 server installation hierarchy:

1. On the machine that hosts the DB2 Data server, navigate to the *IC_INSTALL_DIR*/IC71/lib directory where Avaya IC installs the qdb2sp stored procedure library.
2. Use the ftp command or the rcp command to copy the qdb2sp stored procedure library to the following directory on the machine that hosts the DB2 server:

   db2inst1/sqllib/function

   Note:
   Do not copy the stored procedure library to any machine that hosts the DB2 client. The stored procedure library must be copied to the function directory of the DB2 server.

Setting up a Data server

The Data server is specific to the type of database you use in your Avaya IC system. All Avaya IC server and client components use the Data server to communicate with your database. The Data server uses the Avaya IC account for each component or user to link the Avaya IC components and the database server.

All Data servers support connection pooling.

After you configure the Data server, you can configure other Avaya IC applications on the same machine.

This section includes the following topics:

Cautions and tips for configuring a Data server

When you configure the Data server, note the following:

Database machine: Do not install and configure the Data server on the machine that hosts your database.

Host your database server on a dedicated machine, so you can tune your database server to maximize database operations and improve the reliability and performance of the database.

Multiple database types: A Data server can only communicate with one type of database. Install multiple Data servers if your Avaya IC configuration requires more than one type of database. For example, you need a second Data server if you maintain a legacy database in a different type of database.

The CCQ database, IC Repository database, and Avaya OA database must all be the same database type.

DB2 stored procedure library: If you use DB2 for your Avaya IC databases, you must copy the qdb2sp stored procedure library from the machine that hosts the primary ORB server to the DB2 installation hierarchy. If you do not copy the stored procedure library, the Data server will not be able to communicate with the DB2 database server, and Database Designer will not be able to configure the Avaya IC databases. For more information, see Copying the stored procedure library - DB2 only on page 54.

Creating the primary Data server

The primary Data server is typically on the same machine as the primary ORB server.

This section includes the following topics:

- Creating a primary Data server for Microsoft SQL Server on page 56.
- Creating a primary Data server for Oracle on page 58.
- Creating a primary Data server for IBM DB2 on page 61.

Creating a primary Data server for Microsoft SQL Server

To create a primary Data server for Microsoft SQL Server:

1. On the machine where you installed the Design & Administration Tools, select **Start** > **Programs** > **Avaya Interaction Center 7.1** > **IC Manager**.
2. Log in to IC Manager with the pre-assigned login ID and password shown in the following table.

Login	Password
Admin	admin

   The next time you log in, IC Manager will prompt you to change the password.

3. Select the **Server** tab, then:
   a. Select **Server** > **New**.
   b. Select **DataServerMSSQL** from the list of servers.
   c. Select **OK**.
4. In the **General** tab of the Server Editor, complete the fields as shown in the following table.

Field	Recommended entry	Notes
Name	Enter a logical name for the Data server. For example, DataServerMSSQL.	Include the type of database on your Avaya IC system in the name. You need this name to configure IC Repository and the CCQ database.

Field	Recommended entry	Notes
Domain	Select the Avaya IC domain for the server from the drop-down list.	For example, select `Default` from the drop-down list if the server is in the Default domain.
Host	Select the IP address of the machine that hosts the server, or enter the IP address if it is not in the list.	When you select the host, IC Manager fills in the fields for Directory, Port, and Executable.

5. In the **DataServer** tab of the Server Editor, complete the fields as shown in the following table.

Field	Recommended entry	Notes
DB Login	Enter your DBA user name.	The name used by the Data server to access databases.
DB Password	Enter your database password.	The password that corresponds to the database login name used by the Data server to access databases.
Request Handler Thread Pool Size	Enter the number of requests in the thread pool. Default is 30.	Maximum number of threads that handle client requests in the Data server. These threads accept requests from the Data server clients and queues them for execution in the database.
DB Connection Pool Size	Enter the number of connections in the pool. Default is 15. Minimum is 1.	Maximum number of database connections to open in a connection pool.

6. Select the **Debug** tab and perform the following steps:
   a. Select the **Ellipsis** (**…**) button next to **Trace Levels**.

b. In the **Trace Levels** dialog box, check the following boxes.

Field	Recommended entry	Notes
idl	• Check this box for development systems only. • Clear this box for production systems.	idl is a higher level trace that is more readable than msg. idl writes all method invocations to the log file.
flush	• Check this box for development systems only. • Clear this box for production systems.	When the server writes to the log buffer, flush immediately writes the information to the log file. Flush does not wait for the buffer to fill before writing entries to the log file.

c. Select **OK**.

For information about the other options in the **Trace Levels** dialog box, see *IC Administration Volume 1: Servers & Domains*.

7. Select **OK** to save the Data server configuration.
8. Start the Data server:
   a. Select the Data server that you just created.
   b. Right-click on the Data server.
   c. Select **Start** from the drop-down list.

Creating a primary Data server for Oracle

To create a primary Data server for Oracle:

1. On the machine where you installed the Design & Administration Tools, select **Start** > **Programs** > **Avaya Interaction Center 7.1** > **IC Manager**.
2. Log in to IC Manager with the pre-assigned login ID and password shown in the following table.

Login	Password
Admin	admin

The next time you log in, IC Manager will prompt you to change the password.

3. Select the **Server** tab, then:
   a. Select **Server** > **New**.
   b. Select **DataServerOracle** from the list of servers.
   c. Select **OK**.
4. In the **General** tab of the Server Editor, complete the fields as shown in the following table.

Field	Recommended entry	Notes
Name	Type DataServerOracle or another logical name for the Data server.	Include the type of database on your Avaya IC system in the name. You need this name to configure IC Repository and the CCQ database.
Domain	Select the Avaya IC domain for the server from the drop-down list.	For example, select `Default` from the drop-down list if the server is in the Default domain.
Host	Select the IP address of the machine that hosts the server, or enter the IP address if it is not in the list.	When you select the host, IC Manager fills in the fields for Directory, Port, and Executable.

5. In the **DataServer** tab of the Server Editor, complete the fields as shown in the following table.

Field	Recommended entry	Notes
DB Login	Enter the database account name.	The database login name used by the Data server to access databases.
DB Password	Enter the password for the database account.	The password as configured in the Oracle database.
Oracle Home Directory	Enter the pathname of the home directory of the Oracle database.	Oracle Data server only. This home directory overrides the home directory specified in the IC Data Source parameter.

Field	Recommended entry	Notes
Request Handler Thread Pool Size	Enter the number of requests in the thread pool. Default is 30.	Maximum number of threads that handle client requests in the Data server. These threads accept requests from the Data server clients and queues them for execution in the database.
DB Connection Pool Size	Enter the number of connections in the pool. Default is 15. Minimum is 1.	Maximum number of database connections to open in a connection pool.

6. Select the **Debug** tab and perform the following steps:
   a. Select the **Ellipsis** (**…**) button next to **Trace Levels**.
   b. In the **Trace Levels** dialog box, check the following boxes.

Field	Recommended entry	Notes
idl	• Check this box for development systems only. • Clear this box for production systems.	idl is a higher level trace that is more readable than msg. idl writes all method invocations to the log file.
flush	• Check this box for development systems only. • Clear this box for production systems.	When the server writes to the log buffer, flush immediately writes the information to the log file. Flush does not wait for the buffer to fill before writing entries to the log file.

   c. Select **OK**.

   For information about the other options in the **Trace Levels** dialog box, see *IC Administration Volume 1: Servers & Domains*.

7. Select **OK** to save the Data server configuration.
8. Start the Data server.
   a. Select the Data server that you just created.
   b. Right-click on the Data server.
   c. Select **Start** from the drop-down list.

Creating a primary Data server for IBM DB2

To create a primary Data server for IBM DB2:

1. On the machine where you installed the Design & Administration Tools, select **Start** > **Programs** > **Avaya Interaction Center 7.1** > **IC Manager**.
2. Log in to IC Manager with the pre-assigned login ID and password shown in the following table.

Login	Password
Admin	admin

   The next time you log in, IC Manager will prompt you to change the password.

3. Select the **Server** tab, then:
   a. Select **Server** > **New**.
   b. Select **DataServerDB2** from the list of servers.
   c. Select **OK**.
4. In the **General** tab of the Server Editor, complete the fields as shown in the following table.

Field	Recommended entry	Notes
Name	Type DataServerDB2 or another logical name for the Data server.	Include the type of database on your Avaya IC system in the name. You need this name to configure IC Repository and the CCQ database.
Domain	Select the Avaya IC domain for the server from the drop-down list.	For example, select `Default` from the drop-down list if the server is in the Default domain.
Host	Select the IP address of the machine that hosts the server, or type in the IP address if it is not in the list.	When you select the host, IC Manager fills in the fields for Directory, Port, and Executable.

5. In the **DataServer** tab of the Server Editor, complete the fields as shown in the following table.

Field	Recommended entry	Notes
DB Login	Enter your database login name.	The name used by the Data server to access databases.
DB Password	Enter your database password.	The password that corresponds to the database login name used by the Data server to access databases.
Request Handler Thread Pool Size	Enter the number of requests in the thread pool. Default is 30.	Maximum number of threads that handle client requests in the Data server. These threads accept requests from the Data server clients and queues them for execution in the database.
DB Connection Pool Size	Enter the number of connections in the pool. Default is 15. Minimum is 1.	Maximum number of database connections to open in a connection pool.

6. Select the **Debug** tab and perform the following steps:
   a. Select the **Ellipsis** (**…**) button next to **Trace Levels**.
   b. In the **Trace Levels** dialog box, check the following boxes.

Field	Recommended entry	Notes
idl	• Check this box for development systems only. • Clear this box for production systems.	idl is a higher level trace that is more readable than msg. idl writes all method invocations to the log file.
flush	• Check this box for development systems only. • Clear this box for production systems.	When the server writes to the log buffer, flush immediately writes the information to the log file. Flush does not wait for the buffer to fill before writing entries to the log file.

   c. Select **OK**.

   For more information about trace levels, see *IC Administration Volume 1: Servers & Domains*.

7. Select **OK** to save the Data server configuration.
8. Start the Data server:
   a. Select the Data server that you just created.
   b. Right-click on the Data server.
   c. Select **Start** from the drop-down list.

Creating a secondary Data server

An Avaya IC system usually requires more than one Data server. For information about recommended deployments for a secondary Data server, see *IC Installation Planning and Prerequisites*.

To create a secondary Data server, follow the instructions in Creating the primary Data server on page 56.

Avaya IC data sources

Application Design Language (ADL) files contain the data models for Avaya IC databases, including tables, table sets, browsers, and modules. These files also contain the interface for applications such as the Report Wizard and ListQ.

For an out-of-the-box, non-customized Avaya IC installation, use ADL files to perform the following tasks:

- Configure Avaya IC databases
- Create Avaya IC data sources
- Generate applications such as Report Wizard and ListQ

About data sources

All Avaya IC components that must access a database use Avaya IC data sources. These components include servers, workflows, and agent applications. You create an Avaya IC data source when you generate an application from the application ADL file.

All Avaya IC systems require the following data sources:

- Repository data source
- Interaction Center data source

Repository and Interaction Center are only data sources. They do not have a user interface. Although you generate a Windows application to create the data sources, you cannot use repository or interaction_center as an application.

The following table describes the typical data sources in an out-of-the-box Avaya IC installation.

Data Source	ADL File	Description
repository	repository.adl	**Required for all Avaya IC systems.** Used by the Directory server, Report server, and DUStore server for access to the IC Repository.
interaction_center	ccq.adl	**Required for all Avaya IC systems.** Used by most Avaya IC servers to access the database. This data source also handles most server-related transactions, such as workflows. **Note:** Use this data source for all Avaya IC systems that integrate with third party applications.
report_wizard	repository.adl	Optional. Used by Avaya IC systems that include Report Wizard for mappings to retire EDUs to the IC Repository database.
listq	ccq.adl	Optional. Used only by Avaya IC systems that include ListQ.

About Avaya IC applications

Applications, such as Report Wizard and ListQ are optional components of Avaya IC. You can use these components to add a list management feature or reporting functionality.

The following table describes the applications available with Avaya IC.

Application	ADL File	Description
Report Wizard	repository.adl	Sets mappings to retire EDUs to the IC Repository database. You must build the Report Wizard application to use or view data from EDUs. To generate Report Wizard, select **reportwizard** when you generate your Windows application.
ListQ	ccq.adl	ListQ is sometimes known as List Management. This application provides an Outbound List Processing application for Avaya Agent. ListQ handles customer lists for outbound campaigns that you dial manually. To generate ListQ, select **listq** when you generate your Windows application.

Setting the display time for Avaya IC databases

When you create an Avaya IC database, you must set the display time for that database. The display time option determines how Avaya IC handles the difference in time between the agent desktop machine and the time as reported by the database for all database activities, such as Select, Insert, and Update.

The following table describes the display time options for Avaya IC databases.

Display time option	Description
DBMSTIME	Select this option if you want the DateTime data to display as database time, and not adjusted to local time. With DBMSTIME, Avaya IC ignores the difference in time and does not apply the difference to any database activity.
LOCALTIME	Select this option if you want the DateTime data to display as adjusted to local time on the client. With LOCALTIME, Avaya IC uses the difference in time, rounds it to the nearest half hour, and applies this difference to all database activity that involves date and time information.
HOSTTIME	Select this option if you want the DateTime data to display as adjusted to the local host time, including small differences between system clocks. With HOSTTIME, Avaya IC uses the difference in time and applies this difference to all database activity that involves date and time information.

Creating IC Repository

IC Repository manages current and historical data in the form of Electronic Data Units (EDUs), Agent Data Units (ADUs), system configuration, and resource utilization statistics. This data includes agents, workgroups, queues, and tenants. IC Repository forms the structure that your database server needs to accept contact data from the Avaya IC EDU server and ADU server.

Avaya OA queries the data that these Avaya IC components write in the IC Repository database and other Avaya IC databases. Avaya OA then reports on the results of the queries.

To create IC Repository, complete the steps in the following topics:

1. Before you create IC Repository on page 66.
2. Building the IC Repository database on page 66.
3. Generating the IC Repository application on page 73.
4. Generating the Report Wizard application on page 74.
5. Updating the Directory server with IC Repository on page 75.

Before you create IC Repository

Before you build the IC Repository database:

- You must know the names that you will give to your IC Repository and CCQ databases.
- For a localized version of Avaya IC, enable Localization in Database Designer, as described in Enabling Database Designer for localization on page 388.

Building the IC Repository database

The following instructions assume that you have reviewed and modified all components of the IC Repository ADL file in Database Designer. For information about the ADL file, see *IC Database Designer Application Reference*.

Important:
If you use DB2 for your Avaya IC databases, you must copy the qdb2sp stored procedure library from the machine that hosts the primary ORB server to the DB2 installation hierarchy.For more information, see Copying the stored procedure library - DB2 only on page 54.

To build the IC Repository database, perform the steps in the following topics:

1. Configuring the IC Repository database connection on page 67.
2. Configuring the IC Repository connection set on page 71.
3. Creating the IC Repository database on page 72.

Configuring the IC Repository database connection

To configure the IC Repository database connection:

1. In Database Designer, select **File** > **Open**.
2. Open the IC Repository ADL file.

   The ADL file is in `IC_INSTALL_DIR\IC71\design\repository\repository.adl`

   If you enabled Database Designer for localization, select **OK** and ignore the warning. Database Designer automatically generates the ALF file when you save the ADL file. For more information, see Enabling Database Designer for localization on page 388.
3. Expand **Components** > **Physical DB Connections** and select **repositoryDBConnection** in the tree pane.
4. In the DB Connection **Properties** tab, complete the fields in the General group as shown in the following table:

Property	Recommended entry	Notes
Timeout (sec)	Type the maximum number of seconds that the client application waits for a response to a database request before the application assumes the connection to the Data server is lost.	Default value is 60 seconds. If no response is returned within the specified time, the client application closes the connection to the Data server and returns an error. The client application attempts to create a new connection to the database on the next database request.
Description	Type a description of the database connection, if desired.	You can leave this field empty.
Display Time	Select a display time option.	The display time option determines how Avaya IC handles the difference in time between the agent desktop machine and the time as reported by the Database for all database activities, such as select, insert, and update. For more information about the display time options, see Setting the display time for Avaya IC databases on page 65.

5. From the Database Type drop-down menu, select the type of database to which you want to connect.

   Database Designer uses the selected database type to generate a SQL statement which can be applied to the database.

6. Complete the Mandatory fields for your database, as shown in the following table.

Database type	Property	Recommended entry	Notes
All database types	Data Server Type/ Alias	Type the name of the primary Data server.	This server is the one that you created in Setting up a Data server on page 55. For example, defaults are: • **DataServerMSSQL** • **DataServerOracle** • **DataServerDB2**
SQL Server	Database server	Type the host name of the machine that hosts your database server.	For the default database instance, type the host name. For another database instance, type <*machine*>\<*db_name*>
	Database Name	Type the name of the IC Repository database. For example, **`repository`**.	Avaya recommends that you use **`repository`** to reduce the possibility of a migration impact.
Oracle	TNS Name	Type the server alias from the tnsnames.ora file	For example, type support.xyzcorp.com.
	Database Name	Type the name of the Oracle user for the IC Repository database. For example, **`repository`**.	Avaya recommends that you use **`repository`** to reduce the possibility of a migration impact.
	Client Library Home Directory	Type the full directory path for the Oracle client on the machine that hosts the Data server.	For example, type `.../opt/oracle/Ora9`
DB2	DB2 Database Name	Type the name of the DB2 database that includes the Avaya IC schema.	DB2 allows a maximum of eight characters for database names. For example, type `db2IC`.
	IC Schema Name	Type the schema name of the IC Repository database. For example, **`repository`**.	Avaya recommends that you use **`repository`** to reduce the possibility of a migration impact.
	Database Territory	Type the territory that represents the locale of the database that includes the IC Repository schema.	The territory defines the language and locale of the database. For more information, see the DB2 documentation.

7. If necessary, complete the Optional fields for your database, as shown in the following table.

Database type	Property	Recommended entry	Notes
SQL Server	Database Location	Leave this field blank.	Identifies the logical space where the named database is stored. The SQL Server DBMS specifies the database location.
	Database Size	Leave this field blank.	The size of the database location specifies the amount of space that the configured application database occupies. The SQL Server RDBMS specifies the database size.
	Log Location	Leave this field blank.	Database-generated log files store cumulative transaction information. The SQL Server RDBMS specifies a default location for the database log.
	Log Size	Leave this field blank.	The size of the location for database log files specifies the amount of space that the database-generated log files can occupy. The SQL Server RDBMS specifies a default size for the database log.

Database type	Property	Recommended entry	Notes
Oracle	Default tablespace name	Type the name of the default tablespace where objects are created for the Avaya IC databases. For example, type **T_CI**.	The database location identifies the logical space where the named database is stored. If you leave this field blank, and the Oracle RDBMS does not specify a database location, Oracle uses the “system” space to define the database. **Caution:** Configuring a database in the system space can crash your database.
	Default tablespace size	Type the number of bytes for the size of the default tablespace.	**Caution:** If you do not specify a default tablespace size here, and your RDBMS does not define the default tablespace size, the default tablespace can expand to use all available space.
	Temp tablespace name	Type the name of the tablespace that stores temporary files. For example, type **T_CI_TEMP**.	Temporary tables store database-generated intermediate sorting files and client session information for Oracle databases. If you do not specify a location for temporary tables, the location is specified by the Oracle RDBMS.
	Temp tablespace size	Type the number of bytes for the size of the tablespace that includes temporary tables.	The size of the location for temporary tables in Oracle databases specifies the amount of space that the temporary tables can occupy. If you do not specify the amount of space to be allocated for temporary tables, the size is specified by the Oracle RDBMS.

Database type	Property	Recommended entry	Notes
DB2	Catalogued Node	Type the remote node on the machine that hosts the Data server.	Complete this field if you host your Data server on a different machine from the Avaya IC databases.
	Tablespace Name	Type the name of the tablespace used by the IC Repository database.	Complete this field if you created a dedicated tablespace that the IC Repository database uses. **Note:** Avaya OA requires dedicated tablespaces. For more information, see *Avaya OA Installation Planning and Prerequisites*.

8. Select **File** > **Save** to save the ADL file. Do not close the file.

Configuring the IC Repository connection set

To configure the connection set for IC Repository:

1. In Database Designer, expand **DB Connection Sets** and select **DefaultDBConnectionSet** in the tree pane.
2. Select **Application** from the **Logical DB Connections** list in the Connection Set **Properties** tab.
3. Make sure the properties are set as shown in the following table:

Field	Recommended entry
Physical DB Connection	Select **repositoryDBConnection**.
Primary	Do not check this box.
Use External Database	Check this box.
Database Name	Type the name of your application database. This name must be the exact name that you will give your application database when you create it. For example, type `ccq`.

4. Select **Repository** from the **Logical DB Connections** list.

5. Make sure the properties are set as shown in the following table:

Field	Recommended entry
Physical DB Connection	Select **repositoryDBConnection**.
Primary	Check this box.

6. Select **File** > **Save** to save the ADL file. Do not close the file.

Creating the IC Repository database

These steps perform the following:

- Create the schema that Avaya IC requires for IC Repository
- Seed IC Repository with the configuration data in the `seed.cfg` file.

You do not need to modify the IC Repository seed data. The following table describes the contents of the seed data for IC Repository:

Type of data	Description
Property data	System configuration data for IC Manager and Avaya Agent.
Initialization data	Default workgroup, queue, and tenant data for Web Management and Email Management. This data also includes templates you can use to create custom workgroups, queues, and tenants.
Mapping data	Default mapping rules for the Report Server. These rules tell the server how to write data from retired EDUs to IC Repository.

To create the IC Repository database:

1. In Database Designer, select **File** > **Database Administration**.
2. Select **defaultDBConnectionSet** from the **DB Connection Set** list.

3. Set the options as shown in the following table:

Field	Database type	Recommended entry
Configure	SQL Server	Select **Configure**.
	Oracle	Select **Configure**.
	DB2	Select one of the following options: ● If you have run the `db2crdb.sh` script to create the database, *or* if you have already configured an Avaya IC database, select **Schema Only**. ● If you have not run the `db2crdb.sh` script *and* if you have not yet configured an Avaya IC database, keep **Schema Only** unchecked and select **Configure**.
Import Seed Data	All database types	Check this box.
Login Id	All database types	Type your IC Manager login ID. **Note:** Do not use your DBA login ID and password.
Password	All database types	Type your password.

4. Select **Run** to configure the database and import the seed data.

   Database Designer pauses briefly between configuring the database and importing the seed data.

5. Select **Close** to close the Database Administration screen. Do not close the ADL file.

Generating the IC Repository application

You generate the IC Repository application to initialize the database with the ADL and version information, and to create the Repository data source.

To generate the IC Repository application:

1. In Database Designer, select **File** > **Generate Windows Application**.
2. Check the following boxes to load the files to the database:
   - Messages
   - IC Scripts

3. Select **repository** from the **Name** list.
4. Type the path for the directory where you want Database Designer to store the application files.

   For example, type `C:\Program Files\Avaya\IC71\apps`.

   If you do not know the directory path, select the **Ellipsis** (**…**) button and navigate to the directory.
5. From the **DB Connection Set** drop-down list, select **defaultDBConnectionSet**.
6. If the fields in the following table do not have entries, re-type your IC Manager account and password.

Field	Recommended entry
Login Id	Type your IC Manager login ID. **Note:** Do not use your DBA login ID and password.
Password	Type your password.

7. Select **OK**.

   Database Designer creates a new folder with the same name as the application in the target directory.

Generating the Report Wizard application

You use the Report Wizard to set mappings to retire EDUs to the IC Repository database. You must build the Report Wizard application to use or view data from EDUs.

Generate the Report Wizard application from the IC Repository ADL file.

To build the Report Wizard application:

1. In Database Designer, select **File** > **Generate Windows Application**.
2. In the **Generate Windows Application** dialog box, complete the fields as shown in the following table:

Field	Recommended entry
Messages	Check this box.
IC Scripts	Check this box.
Forms	Check this box.

Field	Recommended entry
Help File	• Check this box. • Type the path and file name for the help file, as follows: *IC_INSTALL_DIR*\IC71\help\ReportWizard\Reports.chm
Avaya Agent Layout	• Do *not* select this check box.

3. Select **reportwizard** from the **Name** drop-down list.
4. Type the path for the directory where you want Database Designer to store the application files.

   For example, type `C:\Program Files\Avaya\IC71\apps`.

   If you do not know the directory path, select the **Ellipsis** (**…**) button and navigate to the directory.
5. From the **DB Connection Set** drop-down list, select **defaultDBConnectionSet**.
6. If the fields in the following table do not have entries, re-type your IC Manager account and password.

Field	Recommended entry
Login Id	Type your IC Manager login ID. **Note:** Do not use your DBA login ID and password.
Password	Type your password.

7. Select **OK**.

   Database Designer creates a new folder with the same name as the application in the target directory. This folder contains the Report Wizard ADL file.

Updating the Directory server with IC Repository

You must initialize the connection between the Directory server and IC Repository. Until this point in the configuration, your Avaya IC ORB environment obtained configuration information from the machine's local hard drive. After you update the Directory server, the Avaya IC ORB environment obtains and stores configuration information in IC Repository.

To update the Directory server for IC Repository:

1. On the **Server** tab in IC Manager, double-click the Directory server.
2. Select the **Directory** tab.

3. Verify that the IC Repository data source is selected from the **IC Data Source** drop-down list.
4. Select **OK**.
5. Stop and start the Directory server.

   The Alarm Monitor should display a message such as "Server has started:: DS" followed by the IP address of the machine that hosts the Directory server, the port used to communicate with the server, and an identification string.
6. When the Alarm Monitor indicates that the Directory server started properly, refresh IC Manager:

   a. Select **Manager** > **Refresh**.

   b. In the Success message, select **OK**.

   If you do not receive a Success message, perform the steps in Troubleshooting the refresh in IC Manager on page 406.

Note:
If you prefer to create and configure all databases at the same time, you can also create and configure the other databases used by your Avaya IC system at this time. For the Avaya OA databases, see the *Operational Analyst Installation and Configuration*.

Creating the CCQ database

You must create and seed the CCQ database to run all Avaya IC components and applications.

The CCQ database collects, stores, and manages:

- Customer-specific data, including contact information and customer history information
- Application data, including information about Web Management or Email Management

Note:
If you use DB2 for your Avaya IC databases, you must copy the qdb2sp stored procedure library from the machine that hosts the primary ORB server to the DB2 installation hierarchy. If you do not copy the stored procedure library, Database Designer will not be able to configure the Avaya IC databases. For more information, see Copying the stored procedure library - DB2 only on page 54.

To create the CCQ database, complete the steps in the following topics:

1. Modifying the Avaya Agent layout on page 77.
2. Building the CCQ database on page 77.
3. Generating the Interaction Center application on page 84.

Modifying the Avaya Agent layout

If your system does not include Avaya Agent, do not perform this step. Go to Building the CCQ database on page 77.

Avaya IC installs the default Avaya Agent layout in the following directory:

IC_INSTALL_DIR\IC71\design\QConsole\avaya_agent_<lang>.cdl

where ***<lang>*** represents the language that the agent will use on the desktop. For example, if the agent desktop includes Avaya Agent in English, select `avaya_agent_en.cdl`. For more information about Avaya Agent layouts in non-English languages, see Configuring Avaya Agent for a supported language on page 390.

The default layout includes task lists for all media channels, including Telephony, Web Management, and Email Management. To customize the Avaya Agent layout for your contact center, see *Avaya Agent Integration*.

Building the CCQ database

To build the CCQ database, perform the steps in the following topics:

1. Configuring the CCQ database connection on page 77.
2. Configuring the CCQ connection set on page 82.
3. Creating the CCQ database on page 83.

Configuring the CCQ database connection

To configure the CCQ database connection:

1. If you do not already have the CallCenterQ ADL file open in Database Designer, select **File** > **Open**.

   You can find this ADL file in *IC_INSTALL_DIR*\IC71\design\CallCenterQ\ccq.adl

2. Expand **Components** > **Physical DB Connections** and select **ccqDBConnection** in the tree pane.

3. In the DB Connection **Properties** tab, complete the fields in the General group as shown in the following table:

Property	Recommended entry	Notes
Timeout (sec)	Type the maximum number of seconds that the client application waits for a response to a database request before the application assumes the connection to the Data server is lost.	Default value is 60 seconds. If no response is returned within the specified time, the client application closes the connection to the Data server and returns an error. The client application attempts to create a new connection to the database on the next database request.
Description	Type a description of the database connection, if desired.	You can leave this field empty.
Display Time	Select a display time option.	The display time option determines how Avaya IC handles the difference in time between the agent desktop machine and the time as reported by the Database for all database activities, such as select, insert, and update. For more information about the display time options, see Setting the display time for Avaya IC databases on page 65.

4. From the Database Type drop-down menu, select the type of database to which you want to connect.

   Database Designer uses the selected database type to generate a SQL statement which can be applied to the database.

5. Complete the Mandatory fields for your database, as shown in the following table.

Database type	Property	Recommended entry	Notes
All database types	Data Server Type/ Alias	Type the name of the primary Data server.	This server is the one that you created in Setting up a Data server on page 55. For example, defaults are: • DataServerMSSQL • DataServerOracle • DataServerDB2

Database type	Property	Recommended entry	Notes
SQL Server	Database server	Type the host name of the machine that hosts your database server.	For the default database instance, type the host name. For another database instance, type <*machine*>\<*db_name*>.
	Database Name	Type the name of the CallCenterQ database. For example, **`ccq`**.	Avaya recommends that you use **`ccq`** to reduce the possibility of a migration impact.
Oracle	TNS Name	Type the server alias from the tnsnames.ora file	For example, type support.xyzcorp.com.
	Database Name	Type the name of Oracle user for the CallCenterQ database. For example, **`ccq`**.	Avaya recommends that you use **`ccq`** to reduce the possibility of a migration impact.
	Client Library Home Directory	Type the full directory path for the Oracle client on the machine that hosts the Data server.	For example, type `.../opt/oracle/Ora9`
DB2	DB2 Database Name	Type the name of the DB2 database that includes the Avaya IC schema.	DB2 allows a maximum of eight characters for database names. For example, type `db2IC`.
	IC Schema Name	Type the schema name of the CallCenterQ database. For example, **`ccq`**.	Avaya recommends that you use **`ccq`** to reduce the possibility of a migration impact.
	Database Territory	Type the territory that represents the locale of the database that includes the CallCenterQ schema.	The territory defines the language and locale of the database. For more information, see the DB2 documentation.

6. If necessary, complete the Optional fields for your database, as shown in the following table.

Database type	Property	Recommended entry	Notes
SQL Server	Database Location	Leave this field blank.	Identifies the logical space where the named database is stored. The SQL Server DBMS specifies the database location.
	Database Size	Leave this field blank.	The size of the database location specifies the amount of space that the configured application database occupies. The SQL Server RDBMS specifies the database size.
	Log Location	Leave this field blank.	Database-generated log files store cumulative transaction information. The SQL Server RDBMS specifies a default location for the database log.
	Log Size	Leave this field blank.	The size of the location for database log files specifies the amount of space that the database-generated log files can occupy. The SQL Server RDBMS specifies a default size for the database log.

Database type	Property	Recommended entry	Notes
Oracle	Default tablespace name	Type the name of the default tablespace where objects are created for the Avaya IC databases. For example, type **T_CCQ**.	The database location identifies the logical space where the named database is stored. If you leave this field blank, and the Oracle RDBMS does not specify a database location, Oracle uses the “system” space to define the database. **Caution:** Configuring a database in the system space can crash your database.
	Default tablespace size	Type the number of bytes for the size of the default tablespace.	**Caution:** If you do not specify a default tablespace size here, and your RDBMS does not define the default tablespace size, the default tablespace can expand to use all available space.
	Temp tablespace name	Type the name of the tablespace that stores temporary files. For example, type **T_CCQ_TEMP**.	Temporary tables store database-generated intermediate sorting files and client session information for Oracle databases. If you do not specify a location for temporary tables, the location is specified by the Oracle RDBMS.
	Temp tablespace size	Type the number of bytes for the size of the tablespace that includes temporary tables.	The size of the location for temporary tables in Oracle databases specifies the amount of space that the temporary tables can occupy. If you do not specify the amount of space to be allocated for temporary tables, the size is specified by the Oracle RDBMS.

Database type	Property	Recommended entry	Notes
DB2	Catalogued Node	Type the remote node on the machine that hosts the Data server.	Complete this field if you host your Data server on a different machine from the Avaya IC databases.
	Tablespace Name	Type the name of the tablespace used by the CallCenterQ database.	Complete this field if you created a dedicated tablespace that the IC Repository database uses. **Note:** Avaya OA requires dedicated tablespaces. For more information, see *Avaya OA Installation Planning and Prerequisites*.

7. Select **File** > **Save** to save the ADL file. Do not close the file.

Configuring the CCQ connection set

To configure the CCQ connection set:

1. In Database Designer, expand **DB Connection Sets** and select **DefaultDBConnectionSet** in the tree pane.
2. Select **CallCenterQ** from the **Logical DB Connections** list in the Connection Set **Properties** tab and make sure the properties are set as shown in the following table:

Field	Recommended entry
Physical DB Connection	Select **ccqDBConnection**.
Primary	Check this box.

3. Select **Repository** from the **Logical DB Connections** list and make sure the properties are set as shown in the following table:

Field	Recommended entry
Physical DB Connection	Select **ccqDBConnection**.
Primary	Do not check this box.

Field	Recommended entry
Use External Database	Check this box.
Database Name	Type the name of your IC Repository database. This name must be the exact name that you gave your IC Repository database. For example, type **`repository`**.

4. Select **File** > **Save** to save the ADL file. Do not close the file.

Creating the CCQ database

These steps create the schema for the CCQ database and seed the database with the configuration data in the **`seed.cfg`** file. You do not need to modify the seed file.

The seed data contains system data for the Web Management servers and Web Self-Service. You must seed the CCQ database with this data if your system includes Web Management and Email Management.

To create the CCQ database:

1. Select **File** > **Database Administration**.
2. Select **DefaultDBConnectionSet** from the **DB Connection Set** list.
3. Set the options as shown in the following table:

Field	Database type	Recommended entry
Configure	SQL Server	Select **Configure**.
	Oracle	Select **Configure**.
	DB2	Select one of the following options: ● If you have run the `db2crdb.sh` script to create the database, *or* if you have already configured an Avaya IC database, select **Schema Only**. ● If you have not run the `db2crdb.sh` script *and* if you have not yet configured an Avaya IC database, keep **Schema Only** unchecked and select **Configure**.
Import Seed Data	All database types	Check this box.

4. If the fields in the following table do not have entries, re-type your IC Manager account and password.

Field	Recommended entry
Login Id	Type your IC Manager login ID. **Note:** Do not use your DBA login ID and password.
Password	Type your password.

5. Select **Run** to configure the database.

   Database Designer pauses briefly between configuring the database and importing the seed data.

6. Select **Close**. Do not close the ADL file.

Generating the Interaction Center application

You generate the Interaction Center application to initialize the database with the ADL and version information and to create the Interaction Center data source.

Tip:
You also can use these instructions to generate ListQ.

If you are configuring a localized version of Avaya IC, you must import the localized seed data after you perform this step. For more information, see Importing localized seed data on page 392.

To generate the Interaction Center application:

1. In Database Designer, select **File** > **Generate Windows Application** to open the **Generate Windows Application** dialog box.
2. Complete the fields as shown in the following table:

Field	Recommended entry
Messages	Check this box.
IC Scripts	Check this box.
Forms	Check this box.

3. If the Avaya IC system includes Avaya Agent, complete the fields as shown in the following table:

Field	Recommended entry
Avaya Agent Layout	• Check this box. • Type the path and file name for the layout file, as follows: *IC_INSTALL_DIR*\IC71\design\QConsole\avaya_agent_<*lang*>.cdl where <*lang*> is the language of the agent desktop. For example, if Avaya Agent is in English, select avaya_agent_en.cdl
EDU Layout	• Check this box. • Type the path and file name for the layout file, as follows: *IC_INSTALL_DIR*\IC71\design\QConsole\eduviewer_<*lang*>.xsl where <*lang*> is the language on the agent desktop. For example, if Avaya Agent is in English, select eduviewer_en_US.xsl

For more information about Avaya Agent layouts in non-English languages, see Configuring Avaya Agent for a supported language on page 390.

4. Select **interaction_center** from the **Name** list.
5. Type the path for the directory where you want Database Designer to store the application files.

   For example, type C:\Program Files\Avaya\IC71\apps.

   If you do not know the path, select the **Ellipsis** (**...**) button and navigate to the directory.
6. From the **DB Connection Set** drop-down list, select **defaultDBConnectionSet**.
7. If the fields in the following table do not have entries, re-enter your IC Manager account and password.

Field	Recommended entry
Login Id	Type your IC Manager login ID. **Note:** Do not use your DBA login ID and password.
Password	Type your password.

8. Select **OK**.

   Database Designer creates a new folder with the same name as the application in the target directory. This folder contains the Interaction Center ADL files.
9. Select **File** > **Exit** to close Database Designer.

Chapter 4: Configuring core servers

Avaya Interaction Center (Avaya IC) installation copies all Avaya IC server files to the target machines. You cannot copy only the files for selected servers on a machine. If your Avaya IC configuration requires only certain servers on a machine, run the Avaya IC installation on that machine to copy the server files, then configure only those servers that you want to host on the machine.

This section describes how to configure the core servers, including the Avaya IC domains and accounts required for these servers. This section includes the following topics that provide information and the steps that you need to follow to configure the core servers:

Before you configure Avaya IC core servers

Before you configure the Avaya IC core servers, make sure that you:

1. Install and configure all prerequisite software and hardware, as described in *IC Installation Planning and Prerequisites*.
2. Copy the Avaya IC server files to the target machines, as described in Installing Avaya IC server and administration components on page 29.
3. Configure the server environment, as described in Configuring the ORB server environment on page 33.
4. Configure the Avaya IC databases. For more information, see Configuring databases on page 53.

Creating sites

A site is a physical location that agents or servers can occupy in an Avaya IC system. For a single site system, you can use the Default site that is preconfigured.

For an Avaya IC system that includes multiple physical locations, create a site for each physical location. The site name should identify the physical location. Avaya IC uses the site information for routing decisions.

For more information about sites, see *IC Administration Volume 1: Servers & Domains*.

To create a site:

1. In IC Manager, select **Tools** > **Site**.
2. In the **Site Editor** dialog box, select **New**.
3. In the **Create Site** dialog box, complete the following fields:
   a. Type a name for the site that identifies the physical location in the **Name** field.
   b. Type a description of the site in the **Description** field.
   c. Select **OK**.
4. In the **Site Editor** dialog box, select **OK**.

Using Avaya IC domains

At a minimum, an Avaya IC system should include the preconfigured domains installed with Avaya IC. Create multiple Avaya IC domains for your servers and agents to increase performance and allow Avaya IC to handle higher contact rates. For example, use a Voice domain for the servers used for Telephony.

To use domains, review and perform the steps in the following topics:

1. Preconfigured domains on page 89.
2. Guidelines for Avaya IC domains on page 90.
3. Creating domains on page 91.
4. Establishing the failover order for domains on page 91.

Preconfigured domains

Avaya IC includes several domains that are preconfigured with failover paths. The following table describes the preconfigured domains.

Preconfigured domain	Members	Failover path
Default	• Alarm server • Directory server • License server • ORB server	• Default
Email	None	• Email • Email_Helper • Web • Default
Email_Helper	None	• Email_Helper • Email • Default
Prompter1	None	• Prompter1 • Default • Voice1
User1	None	• User1 • Prompter1 • Voice1 • Default • Email • Email_Helper • Web • Web_Helper
Voice1	None	• Voice1 • Default
Web	None	• Web • Web_Helper • Email • Default

Preconfigured domain	Members	Failover path
Web_Helper	None	• Web_Helper • Web • Default
Website	None	• Website • Web • Voice1 • Default

Guidelines for Avaya IC domains

Avaya IC domains can span server machines at different locations and multiple domains can share the same server machine. A failover order is associated with each domain. The failover order defines how the members of a domain will failover to servers in other domains. If a server in one domain becomes unavailable, the requests to that server are routed to a server in the failover domain.

Tip:
Plan your failover policy carefully. If you specify a failover domain at a remote site, you must be sure that you have a high-bandwidth connection between the two sites or system performance will be adversely affected.

While you are deciding on the domains you need in your Avaya IC environment, consider the following guidelines:

- Use logical names that include identifying information, such as the site, the media channel, or the agent workgroup.
- Set up the failover paths for domain that include agents to ensure that the domains failover to one or more domains with an ORB server, Alarm server, and Directory server. If the domains that contain agents do not failover to domains with these servers, then Avaya Agent cannot function correctly.
- Do not assign an agent or a server to more than one domain. If you assign an agent or server to a second domain, IC Manager automatically deletes that agent or server from the first domain.
- Do not associate multiple servers of the same type with the same domain, with the possible exception of the ORB server. You can have multiple ORB servers in the same domain if those servers reside on different machines.

You should also assign agents to User domains. Typically, you should divide your agents between two User domains. If you configure the failover of each User domain to the other domain, then you will have a minimum amount of interruption if a Blender server or agent Workflow server fails.

For examples of how to divide Avaya IC servers between domains, see *IC Installation Planning and Prerequisites*. For more information about domains and failover, see *IC Administration Volume 1: Servers & Domains*.

Creating domains

You can add as many domains as you need to handle the agents and servers in your Avaya IC system. For suggested deployments, see *IC Installation Planning and Prerequisites*.

CAUTION:
Do not delete the Default domain. Avaya IC requires the Default domain to function.

To create a domain:

1. Select **Domain** on the IC Manager toolbar.
2. Select **Servers** in the **Items** box at the top of the Domain Manager.
3. Right-click on **All Domains** and select **New**.
4. Type the name of the new domain.

   The domain name can have a maximum of 32 characters or underscores, starting with an alphabetic character. It cannot have spaces. Use an underscore, if necessary.
5. Select **OK** to create the domain.

   IC Manager displays the new domain name under **All Domains** on the left pane of the Domain Manager.

Establishing the failover order for domains

If a server becomes unavailable, failover redirects all requests from the clients of the unavailable server to an alternative server in a failover domain. A server's client can be an agent desktop application or another server.

A client or server logs in to the Avaya IC system by invoking a DS.Login request. At the time that this request is invoked, there is no information available to identify the group of the client or domain of the server making the request. Avaya IC components assume that the requester is in the Default domain.

While membership in a domain determines how the domain members communicate to servers, it also defines how failover is performed. We strongly recommend that you take the time to pre-plan your server failover strategy before proceeding.

You must ensure that your failover plan follows the deployment guidelines, including:

User domain failover: If your User domain does not include a secondary ORB server, this domain must failover to a domain that includes an ORB server, such as the Default domain.

Data server failover: When an agent logs in, Avaya IC cannot determine that agent's assigned domain until after the login request succeeds. Therefore, during the login process, Avaya IC components assume that all agents belong to the Default domain. To ensure that the Data servers handling login requests failover correctly, these servers must include the Default domain in their server group.

IC Email server failover: The domain that includes your IC Email server must failover to the domain that includes your WebACD server.

WebACD server failover: The domain that includes your WebACD server must failover to the domain that includes your IC Email server.

For more suggestions on how to plan your failover strategy, see the deployment scenarios in *IC Installation Planning and Prerequisites*. You can also establish failover order on a server-by-server basis. For more information, see *IC Administration Volume 1: Servers & Domains*.

To establish the failover order for a domain:

1. In the Domain Manager, select **Servers** in the **Items** box.
2. Select on the name of the domain for which you want to establish failover.
3. In the right pane, select the **Failover** tab.
4. Select the failover domain from the list in the **Available** pane.
5. Select **Add** to move the backup domain into the **Members** pane.

   You can specify multiple domains to be used for failover. Avaya IC uses these failover domains in the order specified. Use the up-arrow and down-arrow located above the **Members** list to rearrange failover order. Do not move a failover domain above the primary domain.
6. Select **OK** to assign the servers in the domain for failover.

Setting up administrative accounts

Avaya IC requires two types of administrative accounts:

Non-human users: These administrative accounts are reserved for non-human Avaya IC users, such as servers and IVRs. For guidelines, see Using administrative accounts for non-human users on page 94.

Human users: These administrative accounts are reserved for human Avaya IC users, such as supervisors and managers. For guidelines, see Using administrative accounts for human users on page 95.

This section describes the minimum number of administrative accounts required to install and configure Avaya IC, and how to create those accounts. Topics include:

For more information about administrative and agent accounts, see *IC Administration Volume 2: Agents, Customers, & Queues*.

About Avaya IC passwords

All Avaya IC accounts, including administrative accounts and accounts for non-human users, must have passwords that meet the requirements that you specify in the Agent/Security properties for the workgroup or for individual agents. These requirements can include:

- Maximum length
- Minimum length
- Minimum number of alphabetic characters
- Minimum number of numeric characters

For more information, see *IC Administration Volume 2: Agents, Customers, & Queues*.

Using administrative accounts for non-human users

Some Avaya IC components, such as the Configuration Tool and some servers, require administrative accounts. These accounts should not be used by a human Avaya IC user.

Important:
Configure all Avaya IC accounts for non-human users to ensure that the password for these accounts does not expire or change.

These administrative accounts are non-human accounts for Avaya IC components only. You do not need to create these accounts in a User domain. When you create an administrative account for an Avaya IC server or component, such as the ICM server, the account must be in either of the following domains:

- The same domain as the component that uses the account
- A domain in a failover path from the domain of the component

The following table describes the minimum number of administrative accounts your Avaya IC system requires for non-human Avaya IC users.

Important:
If you plan to use an account created by the seed data, Avaya recommends that you change the password on the account.

Account	Component	Description	Login
New account	Avaya IC servers	Create an administrative account in: ● The same domain as the component that uses the account OR ● A domain in a failover path from the domain of the component **Note:** Do not use the Admin account created by the seed data, or an account that you use to log in to IC Manager.	As defined by user. Not available in seed data.
Admin	IC Manager login	Administration account that you use to log in to the Configuration Tool and IC Manager when you configure Avaya IC. Domain: User1 Role: Administrator **Note:** IC Manager forces you to change the password for this account.	Login: Admin Password: admin

Account	Component	Description	Login
website	Configuration Tool and Avaya IC servers	You use this account to configure the Website Web application and Web Management services. The Avaya IC components in the DMZ use this account to access other Avaya IC servers and components. Domain: Website Role: Operator	Login: website Password: website
icmbridge	ICM Bridge	You use this account to configure the Attribute server. For more information, see Creating the Attribute server on page 181. Include a Workflow server in the same domain as the ICM account. Domain: Website Role: Operator	Login: icmbridge Password: icmbridge
dcobridge1	DCO Bridge	The Java Application Bridge uses this account to access Avaya IC servers, such as the Data server. Each Java Application Bridge in an Avaya IC system requires a unique DCO Bridge account. Domain: User1 Role: Agent	Login: dcobridge1 Password: dcobridge1

Using administrative accounts for human users

All human Avaya IC users who require administrative privileges, such as access to IC Manager and other Design & Administration Tools, require administrative accounts. These accounts should not be used by a non-human Avaya IC user. You should require that the Avaya IC user regularly change the password for these accounts.

When you create an administrative account for a human Avaya IC user, the account must be in a User domain. You can create an administration domain that is restricted to administrative accounts for human users.

Creating administrative accounts

You must create the domain for the administrative accounts before you perform these steps.

You may want to create an additional administrative account in the User domain that can communicate with the parent directory server. This account is useful if you have a problem with the configuration of one or more domain. After you configure a temporary account, log in to IC Manager and confirm that you can use this account for administrative access.

To create administrative accounts:

1. In IC Manager, select the **Agent** tab.
2. Select **Administrator** in the left pane.

   If **Administrator** is not visible in the left pane, select **Manager** > **Refresh** to update the information that is available in IC Manager.
3. Select **Agent** > **New**.
4. Select the **General** tab and complete the following fields:

Field	Description
First Name	Required field Type agent's first name.
Last Name	Required field Type agent's last name.
Preferred Name	Required field Type agent's preferred name.
Employee ID	Type the agent's company employee ID (optional).
Login ID	Required field Type a login ID that the agent uses for all Avaya IC applications.
Domain	Required field Select the appropriate domain from the list.
Task Load	Required field Set to 0.

Field	Description
Task Ceiling	Required field. Set to 0.
Site	Select a site from the drop-down list. **Note:** Avaya IC uses the Site to compile statistics for groups or agents or queues.

5. Select the **Security** tab and complete the fields as shown in the following table:

Field	Recommended entry
Password	Type the password for this account.
Confirm	Re-type the password for this account.
Force password change on login	Perform one of the following: ● Check this field for human Avaya IC users ● Do not check this field for non-human Avaya IC users
Disable login	Do not check this field.
Administrator	Check this field. **Note:** Do not check any of the other roles.

6. Select **OK**.

Using system and sample workflows

When you install Workflow Designer, you also install system and sample workflows. Avaya IC installs the project folders for system and sample workflows in subfolders of the following directory:

IC_INSTALL_DIR\IC71\design\IC\Flows\Avaya

CAUTION:
Do not change a system workflow. If you change a system workflow, one or more components of your Avaya IC system will not function.

Sample workflows

The following table describes the sample workflows for Avaya IC.

Workflow project	Description
Blender	Required for all installations.
ICEmail	Required for installations that include Email Management.
Prompter	Required for installations that include Prompter.
TS	Required for all installations that include Telephony.
WACD	Required for all installations that include Web Management or Email Management.

For a complete list of the workflows in these projects, including the directories where Avaya IC installs the workflows, see *Avaya Workflow Designer User Guide*.

Using sample workflows

You can use the sample workflows to set up and test your Avaya IC system. When you test your system, review the settings of the sample workflows for the media channels and components in your Avaya IC system.

You can customize these workflows to meet the business requirements of your contact center. For example, the Email Analysis flows in the ICEmail project contain three sample routing hints for testing purposes. You must review and change these properties to routing hints that meet your contact center's needs.

After you customize the sample workflows, recompile the workflows and load them in the database. For more information, see *Avaya Workflow Designer User Guide*.

Workflows in Avaya IC seed data

The Avaya IC seed data includes compiled system and sample workflows for all projects. When you created the CCQ database, you imported the compiled workflows with the seed data and stored them in the database.

You must update some of these workflows, such as the workflows in the TS project before you can use them in your Avaya IC. Instructions for updating the sample workflows are in the appropriate chapter.

Configuring core servers

The Avaya IC installation program automatically created some of the core servers when you installed the Avaya IC servers and administration components, as described in Installing Avaya IC server and administration components on page 29.

Important:
Use caution if you modify server configuration parameters. Errors can seriously impact the performance of your Avaya IC system.

This section describes the steps you need to perform to configure the remaining core servers. You have already created and configured some core servers. Before you configure media channels and media-specific servers, perform the steps in the following topics to configure the remaining core servers:

Note:
If you reconfigure a running server in IC Manager, stop and restart the server for the settings to take effect. Do not check the Auto start option until you successfully add and configure the servers and start them manually.

These topics only contain information about required server parameters. For more detailed information, see *IC Administration Volume 1: Servers & Domains*.

Server naming guidelines

Under certain circumstances, the Workflow server fails to connect with a server that uses the server type as the name of the server. For example, if an ADU server is named "ADU" or a Web Advocate Adaptor server is named "WAA".

To ensure optimal functioning of your Avaya IC system, Avaya recommends that you use the following naming conventions for your Avaya IC servers:

- Always use a unique server name of up to 32 characters long with no spaces.
- Name your Data servers Data_*<databasetype>*_*<domain>*. For example, **Data_Oracle_Default**.
- In a single site environment, name all other servers *<servername>*_*<domainname>*. For example: **ADU_User1**.
- In a multi-site environment, name all other servers *<servername>*_*<sitename>*_*<domainname>*. For example: **ADU_London_User1**.
- Do *not* set the server name to be the same as the server type, or Avaya IC may encounter errors during operation. For example, use **TS_Voice1** as the name of your Telephony server, not just **TS**.

Important:
Do not use the name **localVDU** or **localADU** for EDU or ADU servers. These are used when the servers are taken off-line to prevent communication with other EDU and ADU servers.

Recommended tuning parameters for Avaya IC servers

A set of recommended tuning parameters to enhance the performance of an Avaya IC system is available in *IC Administration Volume 1: Servers & Domains*.

Creating an ADU server

Typically, an Avaya IC deployment includes more than one ADU server.

If the Avaya IC system includes an ADU server that handles queue ADU entries for a WebACD server, that ADU server must not accept failover requests from an ADU server that handles agent accounts. For more information, see *IC Administration Volume 1: Servers & Domains*.

For Business Advocate the ADU server contains statistics for service classes.

An ADU server must be able to communicate directly with the parent Directory server. For more information about the parent Directory server, see Creating a Directory server on page 103.

To create an ADU server:

1. In IC Manager, select **Server** > **New**.
2. Select **ADU** from the list of servers and select **OK**.
3. Select the **General** tab, and complete the fields shown in the following table.

Field	Recommended entry	Notes
Name	ADU_<*domain*>	Include the domain in the server name to identify the server.
Domain	Select the Avaya IC domain for the server from the drop-down list.	For example, select `Voice` from the drop-down list if the server is in the Voice domain.
Host	Select the machine's IP address from the drop-down list, or enter the IP address if it is not in the list.	When you select the host, IC Manager fills in the fields for Directory, Port, and Executable.

4. Select the **ADU** tab.
5. In the **Idle Time (min)** field, ensure that the number of minutes entered in this field is greater than the length of a typical agent shift.

   Important:
   If an agent is logged into an Avaya IC agent desktop application for longer than the idle time set in the ADU server, the ADU for the agent will time-out. An ADU time-out can cause problems such as inconsistent data in Avaya OA reports and the inability to defer email contacts. Therefore, the idle time should be longer than a typical agent shift and all agents should log out of Avaya IC at the end of a shift.

   You can use the default settings for the ADU server. For more information about the parameters, see *IC Administration Volume 1: Servers & Domains*.
6. Select **OK** to save your configuration settings.

Note:
Do not start this server before you configure all core servers. To ensure that the servers start correctly, see Starting and stopping Avaya IC servers on page 120.

Creating a DUStore server

All Avaya IC systems that include Email Management require a DUStore server. You can also add a DUStore server for Telephony or Web Management. For more information about deployment scenarios for Avaya IC servers, see *IC Installation Planning and Prerequisites*.

The Avaya IC installation program does not automatically add this server.

To create a DUStore server:

1. In IC Manager, select **Server** > **New**.
2. Select **DUStore** from the list of servers and select **OK**.
3. Select the **General** tab, and complete the fields shown in the following table.

Field	Recommended entry	Notes
Name	DUStore_<*domain*>	Include the domain in the server name to identify the server.
Domain	Select the Avaya IC domain for the server from the drop-down list.	Include the DUStore server in the same domain as the EDU server for the channel. For example, select `Email_Helper` from the drop down list if this server handles email contacts. For more information about recommended domains, see *IC Installation Planning and Prerequisites*.
Host	Select the machine's IP address from the drop-down list, or enter the IP address if it is not in the list.	When you select the host, IC Manager fills in the fields for Directory, Port, and Executable.

4. Select the **DUStore** tab and complete the fields shown in the following table.

Field	Recommended entry	Notes
IC Data Source	Select the IC Data Source, which is the ADL file, for the IC Repository database.	If you used the default name, select `repository`.
Default deletion age (Days)	Enter the number of days that Avaya IC holds an EDU in absence of other information.	Default is 60 days. After this period, the DUStore deletes the EDU from the DUStore table and retires the EDU to the database.

Field	Recommended entry	Notes
Deleted per scan	Enter the number of EDUs the DUStore retires to the database when it scans the system for expired EDUs.	Default is 1000.
Scan Interval (min)	Enter the period of time, in minutes, the server scans for expired EDUs.	Default is 15. Higher values may save some CPU time; lower values make for more predictable behavior during prototyping and testing. Assume that other timers in the EDU could be off by as much as (this interval + 1) to start.
Purge Alarm	Check to raises an alarm if a delete scan finds any EDUs that meet the criteria for deletion and retirement to the database.	Default is checked.

5. Select **OK** to save your configuration settings.

Note:
Do not start this server before you configure all core servers. To ensure that the servers start correctly, see Starting and stopping Avaya IC servers on page 120.

Creating a Directory server

The Directory server maintains a list of all the servers in Avaya IC. When you create multiple Directory servers, they share one common directory.

This section includes the following topics:

Configuring the primary Directory server

You must designate one Directory server to synchronize the directories and ensure that changes made by one Directory server are reflected throughout the network. This designated Directory server is called the parent. If there is only one Directory server in Avaya IC, IC Manager automatically assigns parent status to that server. For more information, see *IC Administration Volume 1: Servers & Domains*.

Usually, the primary Directory server is on the same machine as the primary ORB server.

To configure the primary Directory server:

1. In IC Manager, select the **Server** tab.
2. Double-click the Directory server to open the Server Editor.
3. Select the **Directory** tab and complete the fields as shown in the following table.

Field	Recommended entry	Notes
IC Data Source	Select the IC Repository data source from the IC Data Source drop-down list.	If you used the default name, select `repository`.
Is Parent	Check this box as this Directory server will be the parent directory server.	The parent Directory server synchronizes the directories for all Directory servers.
Backup	Enter the name of a backup file to be created. This file used a backup copy of the directory. Click the Start button to create the file in the server's home directory.	Avaya IC appends an .ffd extension to the file name.
Restore	Enter file name of the backup file used as the name of the directory you want to restore. Click the Start button to restore the directory.	The file name you enter must be a previously created backup directory file.
First update lag (sec)	Enter the number of seconds that the Directory server waits before sending updates to the first of its children.	During normal operation, set this value to 0. (A small delay occurs automatically.) There is no maximum value. If this value is greater than 0, the Advanced tab contains a couple with the name "PropagationDelay" and a value equal to the current buffer updates setting.
Succeeding update lag (sec)	Enter the number of seconds that the Directory server pauses before sending an update to the next child.	During normal operation, set this value to 0 or 1. There is no maximum value. If this value is greater than 0, the Advanced tab contains a couple with the name "LagBetweenChildren" and a value equal to the current childlag setting.

4. Select **OK** to save the Directory server configuration.
5. Stop and restart the Directory server.

Creating a secondary Directory server

To create a secondary Directory server:

1. In IC Manager, select the **Server** tab, then:
   a. Select **Server** > **New**.
   b. Select **Directory** from the list of servers.
   c. Select **OK**.
2. Select the **General** tab and complete the fields as shown in the following table.

Field	Recommended entry	Notes
Name	Directory_<*domain*>	Include the domain in the server name to identify the server.
Domain	Select the domain from the drop-down list.	For example, select `Default` from the drop-down list if the server is in the Default domain.
Host	Select the machine's IP address from the drop-down list, or type in a new IP address.	When you select the host, IC Manager fills in the fields for Directory, Port, and Executable.

3. Select the **Directory** tab and complete the fields as shown in the following table.

Field	Recommended entry	Notes
IC Data Source	Select the IC Repository data source from the IC Data Source drop-down list.	If you used the default name, select `repository`.
Is Parent	Do not check this box, as this Directory server is a secondary, or child, Directory server.	The parent Directory server synchronizes the directories for all Directory servers.
Backup	Enter the name of a backup file to be created. This file used a backup copy of the directory. Click the Start button to create the file in the server's home directory.	Avaya IC appends an .ffd extension to the file name.
Restore	Enter file name of the backup file used as the name of the directory you want to restore. Click the Start button to restore the directory.	The file name you enter must be a previously created backup directory file.

Field	Recommended entry	Notes
First update lag (sec)	Enter the number of seconds that the Directory server waits before sending updates to the first of its children.	During normal operation, set this value to 0. (A small delay occurs automatically.) There is no maximum value. If this value is greater than 0, the Advanced tab contains a couple with the name "PropagationDelay" and a value equal to the current buffer updates setting.
Succeeding update lag (sec)	Enter the number of seconds that the Directory server pauses before sending an update to the next child.	During normal operation, set this value to 0 or 1. There is no maximum value. If this value is greater than 0, the Advanced tab contains a couple with the name "LagBetweenChildren" and a value equal to the current childlag setting.

4. Select **OK** to save the Directory server configuration.
5. Copy the `ds.ffd` file from the machine that hosts your primary Directory server to the machine that hosts your secondary Directory server.
6. In IC Manager, start the secondary Directory server.

Creating an EDU server

Create at least one EDU server for each media type in your Avaya IC system. For example, using the preconfigured domains, if your Avaya IC system includes all three channels, create the following EDU servers:

- VoiceEDUServer in the Voice1 domain
- WebEDUServer in the Web_Helper domain
- EmailEDUServer in an Email_Helper domain

The Avaya IC installation program does not automatically add these servers.

Important:
Avaya IC requires that you place each EDU server in a separate Avaya IC domain. An Avaya IC domain cannot include more than one EDU server. For more information about recommended deployment scenarios and guidelines for the EDU server, see *IC Installation Planning and Prerequisites*.

To create an EDU server:

1. Select **Server** > **New** in IC Manager.
2. Select **EDU** from the list of servers. Select **OK**.
3. In the **Initialize EDU** dialog box, select the media type from the drop-down list. Select **OK**.
4. Select the **General** tab, and complete the fields shown in the following table.

Field	Recommended entry	Notes
Name	EDU_<*domain*>_<*media*>	Include the domain in the server name to identify the server. For example, if you must create an EDU server for voice media, type EDU_Voice1_Voice.
Domain	Select the Avaya IC domain for the server from the drop-down list.	For voice contacts, add the EDU server to the same domain as the associated Telephony server. For chat contacts and email contacts, add the EDU server to a "Helper" domain. For example, select `Email_Helper` from the drop-down list if this server handles email contacts. For more information about recommended domains, see *IC Installation Planning and Prerequisites*.
Host	Select the machine's IP address from the drop-down list, or type in the IP address if it is not in the list.	When you select the host, IC Manager fills in the fields for Directory, Port, and Executable.

5. Select the **EDU** tab and review the default settings.

   You can use the default settings for the EDU server to get your system up and running. For more detailed information about these parameters and how to customize them for your system, see *IC Administration Volume 1: Servers & Domains*.

6. Select **OK** to save your configuration settings.

Note:
Do not start this server before you configure all core servers. To ensure that the servers start correctly, see Starting and stopping Avaya IC servers on page 120.

Creating a Report server

The Report server writes values from EDUs to the IC Repository database. Avaya OA uses these values to generate historical reports.

The Avaya IC installation program does not automatically add this server.

If you set the Server Trace Level field on the Debug tab to 10, the Report server saves text files with information about each EDU in the *IC_INSTALL_DIR*\IC71\temp directory. The Report server names these text files <*eduid*>.txt. Avaya IC does not automatically delete these files. You must manually delete them when they are no longer needed for debugging. If you do not reset the Server Trace Level, the files will continue to accumulate in the *IC_INSTALL_DIR*\IC71\temp directory.

To create a Report server:

1. Select **Server** > **New** in IC Manager.
2. Select **Report** from the list of servers. Select **OK**.
3. Select the **General** tab and complete the fields shown in the following table.

Field	Recommended entry	Notes
Name	Enter a name for the Report server. For example, Report_<*domain*>	Include the domain in the server name to identify the server.
Domain	Select the Avaya IC domain for the server from the drop-down list.	For example, select Voice1 from the drop-down list if the server is in the Voice domain.
Host	Select the machine's IP address from the drop-down list, or enter the IP address if it is not in the list.	When you select the host, IC Manager fills in the fields for Directory, Port, and Executable.

4. Select the **Report** tab, and complete the fields shown in the following table.

Field	Recommended entry	Notes
IC Data Source	Select the IC Data Source for the IC Repository database.	For example, if you used the default name to create the IC Repository application, the data source name is repository.

5. Select **OK** to save your configuration settings.

Note:
Do not start this server before you configure all core servers. To ensure that the servers start correctly, see Starting and stopping Avaya IC servers on page 120.

Creating a Workflow server

The Avaya IC installation program does not automatically add a system Workflow server. Typically, an Avaya IC system includes more than one Workflow server.

To create the Workflow server, perform the steps in the following topics:

1. Configuring multiple Workflow servers on page 109.
2. Creating a Workflow server on page 110.
3. Completing the Workflow server configuration on page 113.

Configuring multiple Workflow servers

For a large Avaya IC system that has a high contact delivery rate and that hosts servers across multiple machines, you can distribute the workflow responsibilities across multiple Workflow servers to maximize performance and response.

For example, you can set up the following workflow servers to process contacts in the different media channels and to handle the different agent-related tasks:

Workflow server for the voice channel: Runs voice contact routing workflows to process voice contacts. These Workflow servers are in a voice domain. For more information, see Configuring a Workflow server for Telephony on page 168.

Workflow server for the chat channel: Runs web contact routing workflows to process incoming chat contacts. These Workflow servers are in a Web domain. For more information, see Configuring a Workflow server for Web Management on page 203.

Workflow server for the email channel: Runs email contact routing workflows and email analysis workflows to process incoming and outbound email contacts. These Workflow servers are in an email domain. For more information, see Configuring a Workflow server for Email Management on page 261.

Workflow server for agent prompting: Runs Prompter workflows and agent script workflows. For information on how to configure a Workflow server to run Prompter flows, see Creating a Workflow server on page 110.

Workflow server for agent searches and transfers: Runs agent search and transfer workflows for the Unified Agent Directory. These Workflow servers are in a User domain. For more information about configuration for these servers, see Configuring a Workflow server for transfers and conferences on page 303.

Creating a Workflow server

These instructions create a basic Workflow server. You must configure this Workflow server to handle the appropriate tasks. For more information, see Configuring multiple Workflow servers on page 109. For more detailed information about parameters in the Workflow server, see *IC Administration Volume 1: Servers & Domains*.

To create a Workflow server:

1. In IC Manager, select **Server** > **New**.
2. Select **Workflow** from the list of servers.
3. Select **OK**.
4. Select the **General** tab, and complete the fields shown in the following table.

Field	Recommended entry	Notes
Name	Workflow_<*domain*>	Include the domain in the server name to identify the server.
Domain	Select the Avaya IC domain for the server from the drop-down list.	For example, select `Users1` from the drop-down list if the server is in the Users1 domain.
Host	Select the machine's IP address from the drop-down list, or enter the IP address if it is not in the list.	When you select the host, IC Manager fills in the fields for Directory, Port, and Executable.

5. Select the **Workflow** tab and perform the following steps:
   a. From the **IC Data Source** drop-down list, select the data source that this Workflow server uses.

      Most Workflow servers use the Interaction Center data source. The default name for this data source is interaction_center.

Note:
For a Workflow server that runs Prompter flows and agent script workflows, the IC Data Source must match the database that was used to build and store the workflows.

b. Review the remaining fields on the tab, as shown in the following table. You will need to complete some of these fields, such as the **Synchronous Startup Flows**, when you create Workflow servers for specific tasks.

Field	Recommended entry	Notes
Reload Flows	Select this button to reload workflows in the Workflow server.	You can choose to update file-based workflows and workflows stored in the database, and whether to force an immediate reload rather than wait for running workflows to complete execution. Select Force immediate reload to reload all currently loaded flows even if the version numbers are the same.
Unload Flow	Select this button to unload a workflow from the server. You will be prompted to enter the workflow name.	When the workflow is next requested, the latest version of the workflow will be loaded from the Database or File System. If the workflow is currently running, it will complete before being unloaded. You must manually increment the workflow version number. If the version has not been incremented, the workflow is not reloaded.
Run Flow	Select this button to run a workflow that updates the variable that contains queue-workflow information.	Enter the workflow name. The queue-workflow information is required by contact routing flows in a Blender environment. Update the variable whenever any change is made to the queue.
IC Data Source	Select a data source from the drop-down list.	For most Workflow servers, select the Interaction Center data source. If you used the default name, select `interaction_center`.
Preload Flows	Select the Ellipsis (…) and specify the workflow to be loaded when the server is first started.	If you have a workflow that must react very quickly when the event triggering it is received by Avaya IC, use the Preload Flows option to have that flow ready and waiting in memory. When the event actually occurs, Avaya IC can run the flow without having to load it first. Syntax: *`projectname.flowname`* **Note:** Preloading a large flow can slow down server startup.

Field	Recommended entry	Notes
Synchronous Startup Flows	Select the Ellipsis (…) and specify the workflow to be loaded before the startup workflows and before the server accepts requests.	For example, Workflow servers that run contact routing workflows need to run web_routing.update_qw_cache as a synchronous startup workflow.
Startup Flows	Select the Ellipsis (…) and specify the workflow to be run when the Workflow server starts.	These workflows are run in addition to Initial Startup Script. Workflows in this list are not guaranteed to execute in any particular order in relation to themselves, Initial Script, or arriving requests. Note that the Initial Script field also specifies a flow to be started, but that parameter can set only one flow. You can specify multiple Startup Scripts.
Semaphores	Select the Ellipsis (…) and specify the list of semaphores used by the workflows.	For more information about semaphores, see the *Avaya IC Media Workflow Reference*.
Directory tables	Select the Ellipsis (…) and specify the Directory server tables to be preloaded in memory at startup.	
Event Threads	Accept the default or enter a number of threads.	The default entry is 10. The number of threads that are listening and available to process events sent to the server.
Enable Heap Validate	Do not check this field unless: ● Instructed by Avaya Technical Support ● Debugging a workflow	This field is for debugging workflows only. Impacts performance of the Workflow server if checked. If the Workflow server fails when it runs a workflow, use this field to check each block as the workflow runs to ensure that the block does not corrupt the Heap.

6. Select **OK**.

Note:
Do not start this server before you configure all core servers. To ensure that the servers start correctly, see Starting and stopping Avaya IC servers on page 120.

Completing the Workflow server configuration

For the Agent Prompting Workflow server, configure your agent desktop and your agents for Prompter and wrapup functionality. A sample Prompter workflow is included in the seed data.

This sample workflow is only intended to help you test Prompter and agent wrapup. For information about how to create and modify Prompter workflows, see *Agent Script Workflow Reference*.

You complete the configuration of other Workflow servers when you configure the media channels and other components, such as the Unified Agent Directory, in your Avaya IC system. You do not need to perform these steps at this point in your installation and configuration.

Creating a Blender server

The Blender server controls agent availability across the different channel types and monitors ADU change events.

The Blender server depends on the Workflow server. Therefore, you cannot configure the Blender server if you have not already performed the steps in Creating a Workflow server on page 109. If the Blender server connects to a Workflow server for a media channel, create the Blender server after you configure the Workflow server.

Do not assign a Blender server to a domain that cannot be reached by agents. If agents cannot reach the Blender server, the Avaya IC system will operate incorrectly.The domain for a Blender server must meet **one** of the following guidelines:

- The Blender server must be in the same domain as a Workflow server and an ADU server.

  OR

- The failover path for the domain of the Blender server must include a Workflow server and an ADU server.

> **Important:**
> If the Blender server domain does not include a Workflow server and an ADU server, or those servers are not in the failover path for the Blender server, you will not be able to start the Blender server. For more information, see *IC Installation Planning and Prerequisites*.

The Avaya IC installation program automatically adds this server.

To create a Blender Server:

1. In IC Manager, select **Server** > **New**.
2. Select **Blender** from the list of servers.
3. Select **OK**.

4. Select the **General** tab, and complete the fields shown in the following table.

Field	Recommended entry	Notes
Name	Blender_<*domain*>	Include the domain in the server name to identify the server.
Domain	Select the Avaya IC domain for the server from the drop-down list.	For example, select `Default` from the drop-down list if the server is in the Default domain.
Host	Select the machine's IP address from the drop-down list, or enter the IP address if it is not in the list.	When you select the host, IC Manager fills in the fields for Directory, Port, and Executable.

5. Select the **Blender** tab, and complete the fields shown in the following table.

Field	Recommended entry	Notes
WorkFlow Server	Select the Workflow server used by this Blender server from the drop-down list.	If you only have one Workflow server and one Blender server, select Workflow_system. If your configuration includes multiple Workflow and Blender servers, select the Workflow server that you created to work with this Blender server.
Flow Set	Enter the name of the workflow project that contains the Blender flows.	The default name is blender.
Initialization Flow	Enter the name of the workflow that initializes the Blender server.	Default name is initialization.
Initialization Data Name	You can leave this field blank.	Optional field. The initialization data name contains values to be added to indata when InitRule is run. InitRule has an indata Event and outdata Event that fill in indata with a string (InitName) and seqcouple (InitData).
Initialization Data	You can leave this field blank.	Optional field. The name to add to indata when InitRule is run.

Field	Recommended entry	Notes
Client Login Flow	Enter the name of the Client Login workflow.	Default name is clientlogin.
Client Logout Flow	Enter the name of the Client Logout workflow.	Default name is clientlogout.

6. Select **OK** to save your configuration settings.

Note:
Do not start this server before you configure all core servers. To ensure that the servers start correctly, see Starting and stopping Avaya IC servers on page 120.

Creating an HTTP Connector server

The Avaya IC installation program does not automatically add this server.

Prompters use the HTTP Connector server. You can create separate HTTP Connector servers for each of these features. You can host more than one HTTP Connector server on the same machine, if the HTTP Connector servers use different HTTP ports.

To create an HTTP Connector server:

1. Select **Server** > **New** in IC Manager.
2. Select **HTTP Connector** from the list of servers. Select **OK**.
3. Select the **General** tab, and complete the fields shown in the following table.

Field	Recommended entry	Notes
Name	HTTPConnector_<*domain*>	Include the domain in the server name to identify the server.
Domain	Select the Avaya IC domain for the server from the drop-down list.	For example, select `Default` from the drop-down list if the server is in the Default domain.
Host	Select the machine's IP address from the drop-down list, or enter the IP address if it is not in the list.	When you select the host, IC Manager fills in the fields for Directory, Port, and Executable.

4. Select the **HTTP Connector** tab and complete the fields shown in the following table.

Field	Recommended entry	Notes
IC Data Source	Select the application name associated with the server. This name should match the IC Data Source setting for the corresponding Workflow server.	If you used the default name, select `interaction_center`. You created this data source in Generating the Interaction Center application on page 84.
Workflow Server	Select the name or type of the Workflow server that this connector should use to execute Workflows and Prompter flows.	
Doc Directory	Accept the default or enter a new directory path.	The directory where the server looks for java script and error pages to serve to prompter and agent applications. Always consider as the relative path from the *AVAYA_IC71_HOME*.
Start Page	Accept the default or enter a new file name.	The name of the file that the Prompter serves when a client asks for a director.
HTTP Port	Enter 9170 for default port.	The server uses this port for HTTP requests. If you must change this port, see *IC Installation Planning and Prerequisites* for a list of the default port numbers used by the other Avaya IC servers. Port conflicts can cause serious problems within the Avaya IC system. **Note:** If you run multiple HTTP Connector servers on the same machine, ensure that they use different ports.

Field	Recommended entry	Notes
Request Timeout (sec)	Enter the number of seconds that the HTTP Connector should wait for a response from one of its clients.	The upper limit of the response time (in seconds) of the Workflow server. The HTTP Connector assumes the current HTTP request from the client has timed out if it did not receive a response from the Workflow server within this time interval. The default is 60 seconds.
Session Timeout (sec)	Enter the time in seconds that the agent has to complete a page and submit the information back to the server.	The maximum idle time for a session. Agent needs to complete and submit the information of the current page within the specified interval value. The HTTP Connector assumes the session as timed out if it did not receive any response from the agent within this time interval. The default is 600 seconds.

5. Select **OK** to save your configuration settings.
6. If the Avaya IC system includes support for:
   - Traditional Chinese, configure the language support as described in Configuring an HTTP Connector server for Traditional Chinese on page 397.
   - Russian, configure the language support as described in Configuring an HTTP Connector server for Russian on page 397.

Note:
Do not start this server before you configure all core servers. To ensure that the servers start correctly, see Starting and stopping Avaya IC servers on page 120.

Creating a Notification server

The Avaya IC installation program does not automatically add this server.

Before you create the Notification server, configure the SMTP and POP3 email servers and verify the configuration, as described in *IC Installation Planning and Prerequisites*.

To create a Notification server:

1. Select **Server** > **New** in IC Manager.
2. Select **Notification** from the list of servers. Select **OK**.

3. Select the **General** tab and complete the fields in the following table.

Field	Recommended entry	Notes
Name	Notification_<*domain*>	Include the domain in the server name to identify the server.
Domain	Select the Avaya IC domain for the server from the drop-down list.	For example, select `Default` from the drop-down list to add the server to that domain.
Host	Select the machine's IP address from the drop-down list, or enter the IP address if it is not in the list.	When you select the host, IC Manager fills in the fields for Directory, Port, and Executable.

4. Select the **Notification** tab and complete the fields in the following table.

Field	Recommended entry	Notes
IC Data Source	Select the Interaction Center data source.	If you used the default name, select `interaction_center`. You created this data source in Generating the Interaction Center application on page 84.
SMTP Server Name	Enter the name of your Email server.	This is the server that Avaya IC uses for outbound email. For example, enter MailSrvExchange.
SMTP Domain	Enter the domain where your IC Email server is located	For example, enter xyzcorp.com
Default Sender Email Address	Enter a valid email address that acts as the sender of the notification emails.	For example, enter notify@xyzcorp.com. **Note:** Do not use an agent address as the Default Sender Email Address.
Poll Interval (sec)	60	Number of seconds between polls.
Poll Future (sec)	86,400	Number of seconds for a long poll. The default equals 24 hours.
Search Limit	250	Number of database records for Notification Server to process at the same time.
Work Schedule Name	Enter the name of the work schedule, if desired.	The name of the work schedule the server should use to determine business time.

Field	Recommended entry	Notes
Notification Agent	Accept the default, or enter another agent number, if desired.	The number representing the agent for which this service instance responds. Agent #0 is the default, and catches all messages. You can also configure multiple Notification server agents, where Agent #1 is for all escalations and Agent #2 is for email and printer. **Note:** If you configure multiple Notification server agents, you cannot specify an Agent #0, because Agent #0 responds to all messages.
Fire Direct Notification	Check this field, if desired.	Select this option if the server should fire notifications.
Fire Escalations	Check this field, if desired.	Select this option if the server should send scheduled escalations.
Fire Scheduled Reports	Check this field, if desired.	Select this option if the server should run scheduled reports.
Language	Select the language in which data for this server will be written.	The allowable codes are: • en (English) • fr (French) • de (German) • es (Spanish) • it (Italian) • pt (Portuguese) • zh (Chinese, Simplified) • ko (Korean) • ja (Japanese) • th (Thai) • zt (Traditional Chinese) • ru (Russian)

5. Select **OK** to save your configuration settings.
6. To configure an alternate email encoding for a language such as Japanese, see Configuring a Notification server for alternate email encodings on page 396.

Note:
Do not start this server before you configure all core servers. To ensure that the servers start correctly, see Starting and stopping Avaya IC servers on page 120.

Starting and stopping Avaya IC servers

After you add and configure the servers, you can modify the server configuration in IC Manager. However, if you modify multiple servers, you must start and stop the servers in a specific order. Dependencies between the servers determine the order. If you start and stop the servers in the wrong order, your Avaya IC system may lose data or encounter other problems. For more specific details, see *IC Administration Volume 1: Servers & Domains*.

CAUTION:
Never stop the DUStore server before you stop the EDU server. If you stop the DUStore server first, you may lose EDU data. Always stop these servers in the following order:

1. EDU server
2. ADU server
3. DUStore server
4. Report server

This section covers startup and shutdown for all Avaya IC servers, including some that you do not install and configure until later in the installation process.

This section includes the following topics:

Determining server dependencies

Starting and stopping servers in Avaya IC is a simple process. However, you should exercise caution because starting or stopping Avaya IC processes in the wrong order can lead to data loss or system errors. In addition, if your Avaya IC installation spans multiple machines, you need to pay attention to the order in which the machines are shut down because of the impact on other Avaya IC services.

This section includes the following topics:

Server startup dependencies

Servers can be started:

- Explicitly by an administrator
- Automatically when the machine on which they reside is started
- As a result of a request from a client

Tip:
The start up time for each server depends on such factors as user population, number of queued emails, and database size. If your servers take a long time to start, you can reduce the server load by adjusting some of these dependencies.

To view the state of each server, use the Alarm Monitor in IC Manager. As servers are started, that server's state will change to "Up," and ORB server sends informational messages to the Alarm Monitor. If IC Manager is running and the Alarm server should fail, Avaya IC will prompt the administrator to re-monitor alarms immediately.

The ICM, IC Website (Tomcat), CIRS, and ICM Bridge (Attribute server) are dependent on several Avaya IC servers. These components perform a client login that, at minimum, requires the Directory, Alarm, ORB, and Data servers to be running.

To work with a Web Server such as IIS, IBM HTTP server, and Sun ONE server, Avaya IC uses ISAPI and NSAPI filters respectively. These interfaces are used to enable Web Management, DataWake, and Tomcat support via plugins that can recover if a dependent component is not available.

The VOX server interfaces with an IVR (Interactive Voice Response) Unit. If the VOX server connects to an external IVR, you should start the IVR first. The VOX server will attempt to connect to the configured IP address and port, for the length of time specified in the VOX server's Maximum Wait Time and Disable Wait parameters. If the IVR connects to the VOX server, the VOX server must be started first.

Tip:
For an Avaya IC deployment that includes Avaya IC and Avaya OA components on the same machine, to avoid potential port conflicts, always start the Avaya IC components first, then start the Avaya OA components.

Server shutdown dependencies

Important:
Shutting down any Avaya IC server process or machine may have an impact on agent clients and dependent processes. Therefore, you should only do so during non-business hours unless you are dealing with an emergency situation.

If failover is configured, the clients should revert from their primary to their backup servers. The connections to the backup server will remain active until the client logs out, is restarted, or another disruption in service occurs.

If failover is not configured and you stop an Avaya IC server, active clients may either raise alarms or show error dialogs and potentially fail if the server is down long enough.

If you need to shutdown an Avaya IC server, you should:

- Do so during a scheduled maintenance period where clients are shutdown and incoming activity can be curtailed.
- Use the IC Manager Shutdown option to ensure the correct communication flow between Avaya IC components, Avaya IC clients, and the other services that should be stopped. The Shutdown option ensures that all Avaya IC server processes on that machine are shutdown in the correct order. It does not shut down dependent Avaya IC processes located on other machines. To use this option, see Stopping all servers on page 125.

Before stopping the services on a machine, you need to consider the impact it will have. Other dependent clients (both agent clients and Avaya IC processes) may need to be shutdown first.

To confirm that an Avaya IC process was shutdown properly, use the System Administration tools provided with your operating system make sure that the process is no longer active. IC Manager may report some servers as being stopped while they are actually finishing important clean up tasks such as committing data to the database.

Avaya IC processes should be restarted as soon as practical in order to minimize the impact on clients. In many cases, the processes will restart automatically when the machine comes back up, or when client requests trigger the server to restart.

Dependent clients will attempt to reconnect if they lose communication with an Avaya IC process. If the stopped process does not recover in time, requests will failover based on the server configuration and the failover strategy implemented at your site.

If you need to shutdown individual Avaya IC servers, follow the correct shutdown order to prevent data loss. Stopping a server obviously results in a disruption of the services provided by that server. The following table shows the impact of shutting down certain servers.

Server	Impact
Alarm server	This server is typically the last to be shutdown so that other servers can still submit alarms.
Data server	Without a Data server, other servers will be unable to commit, read, or write from the database.
DUStore server	If you have configured the ADU and EDU servers to persist data units, these servers become dependent on the DUStore server. Shutting down the DUStore server before the EDU or ADU servers will result in data units not being saved.
Event Collector server	Without the Event Collector, real time statistics will not be collected for the associated domain.
ORB server	This server is responsible for process management. If the ORB server is not running, no other Avaya IC server can start.

Starting and stopping the ORB server

The ORB server controls other Avaya IC servers. You must start the ORB server to open IC Manager. When you start the ORB server, the Alarm, Directory, EDU, and ADU servers start up in sequence.

CAUTION:
Do not use **Stop Server** in IC Manager, the Windows Task Manager, or the Windows Services control panel to start or stop the ORB server.

The Avaya IC Configuration Tool starts the ORB server the first time. If you must stop and start the ORB server again, use the Avaya IC Admin utility or the IC Manager **Shutdown** option.

This section includes the following topics:

ORB server components

The following table describes the components of the ORB server.

Component	Description
orbsrv.exe	Executable for the ORB server
qntorbsrv.exe	Windows service executable that starts the **`orbsrv`** executable.
Avaya IC ORB Service 7.1	Windows only. Helper service that represents the **`qntorbsrv.exe`** executable in the Windows Services control panel

Configuring the ORB server to start automatically on Windows

The ORB server is set to automatically start when you install the server. However, if you reboot a machine and the ORB server does not start, you can follow these steps to manually configure the ORB server.

To configure the ORB server to start automatically on a Windows machine:

1. Select **Start** > **Control Panel** > **Services** to open the Windows Services control panel.
2. Double-click **Avaya IC ORB Service 7.1** in the list of services.
3. In the **General** tab, select **Automatic** from the **Startup Type** drop-down list.
4. Select **OK**.

Configuring the ORB server to start automatically on Solaris and AIX

To configure the ORB server to start automatically on a Solaris or AIX machine:

1. Log in as root.
2. Navigate to the *`IC_INSTALL_DIR`*`/IC71/bin` directory
3. Execute **`setup_orb`**.

Starting and stopping servers in IC Manager

IC Manager allows you to start multiple servers at the same time. The Status column displays the server's new status. If the system cannot start a server, IC Manager displays an error message.

CAUTION:
Never stop the DUStore server before you stop the EDU server. If you stop the DUStore server first, you may lose EDU data.

After you add and configure a server, stop and restart that server.

To start or stop a server:

1. Select the **Server** tab in IC Manager.
2. Select the server from the list on the right side of the window.
3. Select the **Start** or **Stop** traffic light.

Stopping all servers

You can simultaneously shut down all servers that reside on a machine. The server shutdown feature in IC Manager shuts down the servers in the correct order. This process can take several minutes to complete as all servers must complete their current tasks before shutting down. For example, if there are a lot of persistent EDUs for email contacts, the DUStore server can take several minutes to write the EDUs to the database.

To shut down all servers:

1. Select **Server** > **Shutdown** in IC Manager.
2. Select the IP address or the name of the machine where you want to shut down the servers.
3. Select **OK**.

Starting and stopping servers with the Avaya IC Admin utility

You can use the Avaya IC Admin utility to:

- Start the ORB server and all Avaya IC servers that have Autostart enabled, as described in Starting servers with the Avaya IC Admin utility on page 126.
- Stop the ORB server and all associated Avaya IC servers, as described in Stopping all servers with the Avaya IC Admin utility on page 126.

For information about how to start and stop Web services, such as the ICM server, see Starting and stopping Avaya IC services on page 127,

Starting servers with the Avaya IC Admin utility

To start servers with the Avaya IC Admin utility:

1. In a command window, navigate to the directory shown in the following table.

Operating system	Directory
Windows	*IC_INSTALL_DIR*\IC71\bin
Solaris and AIX	*IC_INSTALL_DIR*/IC71/bin

2. Execute the following command:

   icadmin so

Stopping all servers with the Avaya IC Admin utility

To stop all servers on a machine with the Avaya IC Admin utility:

1. Navigate to the directory shown in the following table.

Operating system	Directory
Windows	*IC_INSTALL_DIR*\IC71\bin
Solaris and AIX	*IC_INSTALL_DIR*/IC71/bin

2. Execute the following command:

   icadmin tv <*IC_administrative_user*> <*password*>

Accessing the help for the Avaya IC Admin utility

The Avaya IC Admin utility includes additional commands that are not listed in this section. The help for the Avaya IC Admin utility includes Information about those additional commands.

To access the help for the Avaya IC Admin utility:

1. Navigate to the directory shown in the following table.

Operating system	Directory
Windows	*IC_INSTALL_DIR*\IC71\bin
Solaris and AIX	*IC_INSTALL_DIR*/IC71/bin

2. Execute the following command:

   icadmin help

Starting and stopping Avaya IC services

When you use the **Web** tab of the Configuration Tool to configure Web applications, the Configuration Tool creates services for Avaya IC.

Tip:
Avaya recommends that you configure all Avaya IC services to autostart.

This section describes how to stop, start, and configure startup options for the Avaya IC services, and how to set startup options for the services. This section includes the following topics:

Starting and stopping services on Windows

Use the Windows Service Panel to start, stop, and configure startup options for Avaya IC services.

Note:
Depending upon the components installed on the machine, not all of the following Windows services will display in the Windows Service Panel.

To start, stop and configure Avaya IC services on Windows:

1. In the Services control panel, right-click on one or more of the following services:
   - Avaya IC 7.1 ICM Service
   - Avaya IC 7.1 CIRS Service
   - Avaya IC 7.1 SDK Service
   - Avaya IC 7.1 Web Services Service
   - World Wide Web Publishing Service (for IIS)
   - Avaya IC Jakarta Service 7.1
   - Avaya IC WebLM Service 7.1
   - Avaya IC Web Management Service 7.1
   - Avaya IC Email Template Management Service 7.1
   - Avaya IC Test Service 7.1
2. From the right-click menu, select one of the options in the following table:

Task	Options
Start Avaya IC services	Select **Start**.
Stop Avaya IC services	Select **Stop**.
Set startup options	1. Select **Properties**. 2. Select **Automatic** from the **Startup Type** drop-down list. 3. Select **OK**.

Starting and stopping services on Sun Solaris and IBM AIX

This section includes the following topics:

Starting and stopping the ICM server

Execute all ICM server commands from the *IC_INSTALL_DIR*/IC71/bin directory. For the ICM server to be able to log in, the Avaya IC servers must start before the ICM server.

Starting the ICM server: To start the ICM server, execute the following command:

```
nohup ./icm.sh start
```

Stopping the ICM server: To stop the ICM server, execute the following command where -force is an optional parameter that terminates the server processes:

```
nohup ./icm.sh stop -force
```

Setting the ICM server to autostart: To set the ICM server to autostart, add the following command to the UNIX startup facility:

```
nohup bin/icm.sh start
```

Starting and stopping the CIRS server

Execute all CIRS server commands from the *IC_INSTALL_DIR*/IC71/bin directory. For the CIRS server to be able to log in, the Avaya IC servers must start before the CIRS server.

Starting the CIRS server: To start the CIRS server, execute the following command:

```
nohup ./cirs.sh start
```

Stopping the CIRS server: To stop the CIRS server, execute the following command where -force is an optional parameter that terminates the server processes:

```
nohup ./cirs.sh stop -force
```

Setting the CIRS server to autostart: To set the CIRS server to autostart, add the following command to the UNIX startup facility:

```
nohup IC_INSTALL_DIR/IC71/bin/cirs.sh start
```

Starting and stopping Sun ONE Server Web server

Starting Sun ONE Server: To start Sun ONE Server, execute the following command:

```
<SunONE_install_dir>/servers/<my_ONE_server>/start
```

Stopping Sun ONE Server: To stop Sun ONE Server, execute the stop script packaged with the Web server:

```
<SunONE_install_dir>/servers/<my_ONE_server>/stop
```

Setting Sun ONE Server to autostart: To set Sun ONE server to autostart, add the following command to the UNIX startup script:

```
<SunONE_install_dir>/https-<my_ONE_server>/start
```

Starting and stopping IBM http Web server

Execute the IBM http Web server commands from the *IC_INSTALL_DIR*/IC71/bin directory.

Starting IBM http Web Server: To start IBM http Web Server, execute the following command:

```
./httpserver.sh start
```

Stopping IBM http Web Server: To stop IBM http Web Server, execute the following command:

```
./httpserver.sh stop
```

Setting IBM http Web Server to autostart: To set IBM http Web server to autostart, add the appropriate command to the UNIX startup script. For example, add:

```
nohup IC_INSTALL_DIR/IC71/bin/httpserver.sh start
```

Starting and stopping Tomcat Web applications

Execute all Tomcat commands for the Web Applications from the *IC_INSTALL_DIR*/IC71/bin directory.

Starting all services on a machine: To start services for all Web applications, execute the following command:

```
nohup ./ictomcat.sh start all
```

Stopping all services on a machine: To stop all services for Web applications, execute the following command where `-force` is an optional parameter that terminates the server processes:

```
nohup ./ictomcat.sh stop all -force
```

Starting an individual Web application: To start an individual Web application, execute the appropriate command from the following table:

Web application	Start command
Website	`nohup ./ictomcat.sh start website`
Web License Manager	`nohup ./ictomcat.sh start weblm`
Email Template Administration	`nohup ./ictomcat.sh start rlmanager`
Client SDK server	`nohup ./ictomcat.sh start SDK`
Web Services server	`nohup ./ictomcat.sh start webservices`

Stopping an individual Web application: To stop an individual Web application, execute the appropriate command from the following table. `-force` is an optional parameter that terminates the server processes.

Web application	Stop command
Website	`nohup ictomcat.sh stop website -force`
Web License Manager	`nohup ictomcat.sh stop weblm -force`
Email Template Administration	`nohup ictomcat.sh stop rlmanager -force`
Client SDK server	`nohup ./ictomcat.sh stop SDK -force`
Web Services server	`nohup ./ictomcat.sh start webservices -force`

Setting Tomcat Web applications to autostart

To set them to autostart, add the following command to the UNIX startup facility:

nohup *IC_INSTALL_DIR*/IC71/**bin/ictomcat.sh start all**

For the Tomcat Web applications to be able to log in, the Avaya IC servers must start first.

Chapter 5: Installing Avaya IC licenses

Avaya Interaction Center (Avaya IC) components will not run if you do not install the license server, and obtain the appropriate license file. For information on how to obtain a license, see *IC Installation Planning and Prerequisites*.

If Avaya IC components cannot access the License server and WebLM, agents may not be able to log in, and servers may not be able to start. To provide redundant operation in the event of a failure, install at least one Web License Manager (WebLM) and License server per site, with a minimum of two WebLMs and License servers per Avaya IC system.

To configure Avaya IC licensing, perform the steps in the following topics:

Before you configure Avaya IC licenses

Before you install and configure WebLM:

1. Obtain a license file for your Avaya IC components from Avaya, as described in *IC Installation Planning and Prerequisites*.
2. Install and configure all prerequisite software and hardware, including a Web server and a JDK, as described in *IC Installation Planning and Prerequisites*.
3. On Solaris and AIX machines, install a Windowing environment such as X-Windows on the machine that hosts the WebLM.
4. Install and configure an Avaya IC server environment on the machine that hosts the WebLM,

Configuring the Web License Manager

The Web License Manager (WebLM) is a Web application that hosts your Avaya IC licence. You must configure the Web LM on each machine that hosts an Avaya IC or Avaya OA license. You use the **Web** tab of the Configuration Tool to configure the WebLM.

This section describes how to install and configure the Web License Manager for each operating system that Avaya IC supports. This section includes the following topics:

Hosting multiple Web applications on one machine

If the Avaya IC system includes more than one Web application on the same machine as the WebLM, Avaya recommends that you configure all of the Web applications on the target machine at the same time.

Important:
If you do not configure all of the Web applications simultaneously, leave the options for all Web applications on the target machine checked when you re-run the Configuration Tool to create the new Web applications. If you do not leave the options for the previously created Web applications checked, the Configuration Tool may delete those Web applications.

Advanced properties for the Web LM

The Web tab also includes advanced properties for the Java Virtual Machine.

Only configure the advanced properties if you expect a high volume of traffic for the Web License Manager. For more information, see Configuration Tool advanced properties on page 447.

Configuring the WebLM on Windows

Use these instructions if you plan to host the WebLM on a Windows machine.

You do not need to stop the IIS Web server on Windows machines.

To configure the Web License Manager to run on a Windows machine:

1. To start the Configuration Tool, select **Start** > **Programs** > **Avaya Interaction Center 7.1** > **Configuration Tool**.
2. Log in with your IC Manager login ID and password.
3. Select the **Web** tab.
4. Complete the general fields in the following table.

Field	Description	Sample entry
JDK Home	The path to the directory where the Java SDK is installed. For more information about the Java SDK, see *IC Installation Planning and Prerequisites*.	`C:\j2sdk1.4.2_08`
Tomcat Base Port	The port used to configure the following ports: ● Tomcat HTTP ports for Web applications ● Tomcat AJP (Web server connector) ports	Default: 9600
IIS Website	The name of the IIS Web server that the Web application will use. **Tip:** For a localized version of IIS, type the localized name for the IIS Web server.	Default Web Site
Web Server Host	The name of the machine that hosts the Web server. Do not include the DNS domain.	testbox
DNS Domain	The network (DNS) domain of the machine that hosts your Web server. Do not enter an Avaya IC domain. **Note:** Verify the default DNS domain carefully to ensure that it is correct.	xyzcorp.com

Field	Description	Sample entry
Web Server Port	The port that your Web server uses for communication. Make sure that the port matches the protocol used by your Web server for communication. The default ports are: ● HTTP port is 80. ● HTTPS port is 443. Do not change the default port unless you assign a different port to the Web server.	Default: 80
IC Test	Optional. IC Test is a Web application that you can use to test your Tomcat configuration. If you install multiple versions of Tomcat, the Configuration Tool creates an IC Test application on each version of Tomcat. The Configuration Tool also creates a separate Tomcat server to host IC Test. To access IC Test, use the Tomcat HTTP port in the URL. For example, type: http://<*server*>.<*domain*>.com:9606/ictest **Note:** The port number is not required if you install a single version of Tomcat, or access IC Test from the separate Tomcat server for IC Test.	Checkmark in box

5. Check the **Configure Web License Manager** box.
6. Select **Apply Settings**.
7. Select **OK** in the **Success** dialog box.
8. Select **Exit**.
9. To complete the configuration:
   a. Open the Windows Services control panel.
   b. Start Avaya IC WebLM Service 7.1.

   For more information about how to start and stop Web application services, see Starting and stopping Avaya IC services on page 127.

Configuring the WebLM on Solaris

Use these instructions if you plan to host the WebLM on a Solaris machine.

Important:
To configure the Web License Manager on Solaris, you must log in as a user with write permissions on the Web server directories and the Avaya IC installation directories. The root user usually has these write permissions.

To configure the Web License Manager to run on a Solaris machine:

1. Stop the Sun ONE server that hosts the Web site application with the stop script packaged with the Web server: **`<SunONE_install_dir>/servers/<my_ONE_server>/stop`**
2. Start the Configuration Tool:
   a. Navigate to `IC_INSTALL_DIR/IC71/bin`
   b. Run **`./configure`**
3. Log in with your IC Manager login ID and password.
4. Select the **Web** tab.
5. Complete the general fields in the following table that apply to the operating system on the target machine.

Field	Description	Sample entry
JDK Home	The path to the directory where the Java SDK is installed. For more information about the Java SDK, see *IC Installation Planning and Prerequisites*.	`/opt/j2sdk1_4_2_08`
Tomcat Base Port	The port used to configure the following ports: ● Tomcat HTTP ports for Web applications ● Tomcat AJP (Web server connector) ports	Default: 9600
Web Server Home	The installation path for the Sun ONE Server instance that hosts the Web application.	`/opt/SUNWwbsvr`
Web Server Name	The root name of the server as found in the Sun ONE™ Server home directory. **Note:** Do not include **`https-`** in the Web server name.	testbox.xyzcorp.com
Web Server Host	The name of the machine that hosts the Web server. Do not include the DNS domain.	testbox

Field	Description	Sample entry
DNS Domain	The network (DNS) domain of the machine that hosts your Web server. Do not enter an Avaya IC domain. **Note:** Verify the default DNS domain carefully to ensure that it is correct.	xyzcorp.com
Web Server Port	The port that your Web server uses for communication. Make sure that the port matches the protocol used by your Web server for communication. The default ports are: ● HTTP port is 80. ● HTTPS port is 443. Do not change the default port unless you assign a different port to the Web server.	Default: 80
IC Test	Optional. IC Test is a Web application that you can use to test your Tomcat configuration. If you install multiple versions of Tomcat, the Configuration Tool creates an IC Test application on each version of Tomcat. The Configuration Tool also creates a separate Tomcat server to host IC Test. To access IC Test, use the Tomcat HTTP port in the URL. For example, type: http://<*server*>.<*domain*>.com:9606/ictest **Note:** The port number is not required if you install a single version of Tomcat, or access IC Test from the separate Tomcat server for IC Test.	Checkmark in box

6. Check the **Configure Web License Manager** box.
7. Select **Apply Settings**.
8. Select **OK** in the **Success** dialog box.
9. Select **Exit**.
10. To complete the configuration, perform the following steps to ensure that all WebLM services start properly:
    a. In the Sun ONE Server installation directory:
    - Open the https-admserv directory.
    - If the directory includes a file called start-ICEnv.backup, execute the following command to rename the file:

```
mv start-ICEnv.backup oldstart-ICEnv
```

b. Start the Sun ONE server that hosts the Web License Manager application with the following start script:

```
<SunONE_install_dir>/servers/<my_ONE_server>/start
```

c. Navigate to the *IC_INSTALL_DIR*/IC71/bin directory.

d. Use the following script to start Tomcat:

```
nohup ./ictomcat.sh start weblm
```

Important:
For Solaris and AIX only, the Configuration Tool changes the ownership of the implementation file (vesp.imp) and the interface file (vespidl.pk) to root. If you do not want to run Avaya IC as root, you must change the ownership of these files as described in Changing ownership for Avaya IC - Solaris and AIX only on page 38.

Configuring the WebLM on AIX

Use these instructions if you plan to host the WebLM on an AIX machine.

Important:
To configure the Web License Manager on AIX, you must log in as a user with write permissions on the Web server directories and the Avaya IC installation directories. The root user usually has these write permissions.

To configure the Web License Manager to run on an AIX machine:

1. Stop the IBM HTTP Server that hosts the Website application with the stop script packaged with the Web server: **./httpserver.sh stop**
2. Start the Configuration Tool:
   a. Navigate to *IC_INSTALL_DIR*/IC71/bin
   b. Run **./configure**
3. Log in with your IC Manager login ID and password.
4. Select the **Web** tab.
5. Complete the general fields in the following table that apply to the operating system on the target machine.

Field	Description	Sample entry
JDK Home	The path to the directory where the Java SDK is installed. For more information about the Java SDK, see *IC Installation Planning and Prerequisites*.	/usr/java142

Field	Description	Sample entry
Tomcat Base Port	The port used to configure the following ports: ● Tomcat HTTP ports for Web applications ● Tomcat AJP (Web server connector) ports	Default: 9600
Web Server Home	The installation path for the IBM HTTP server instance that hosts the Web application.	`/usr/HTTPServer`
Web Server Name	A Solaris-only field. You do not need to complete this field for AIX.	Leave this field blank.
Web Server Host	The name of the machine that hosts the Web server. Do not include the DNS domain.	testbox
DNS Domain	The network (DNS) domain of the machine that hosts your Web server. Do not enter an Avaya IC domain. **Note:** Verify the default DNS domain carefully to ensure that it is correct.	xyzcorp.com
Web Server Port	The port that your Web server uses for communication. Make sure that the port matches the protocol used by your Web server for communication. The default ports are: ● HTTP port is 80. ● HTTPS port is 443. Do not change the default port unless you assign a different port to the Web server.	Default: 80
IC Test	Optional. IC Test is a Web application that you can use to test your Tomcat configuration. If you install multiple versions of Tomcat, the Configuration Tool creates an IC Test application on each version of Tomcat. The Configuration Tool also creates a separate Tomcat server to host IC Test. To access IC Test, use the Tomcat HTTP port in the URL. For example, type: http://<*server*>.<*domain*>.com:9606/ictest **Note:** The port number is not required if you install a single version of Tomcat, or access IC Test from the separate Tomcat server for IC Test.	Checkmark in box

6. Check the **Configure Web License Manager** box.
7. Select **Apply Settings**.

8. Select **OK** in the **Success** dialog box.
9. Select **Exit**.
10. To complete the configuration, perform the following steps to ensure that all WebLM services start properly:
    a. Start the IBM HTTP Server that hosts the Web License Manager application with the following start script:

    ```
    ./httpserver.sh start
    ```

    b. Navigate to the *IC_INSTALL_DIR*/IC71/bin directory.
    c. Use the following script to start Tomcat:

    ```
    nohup ./ictomcat.sh start weblm
    ```

Important:
For Solaris and AIX only, the Configuration Tool changes the ownership of the implementation file (vesp.imp) and the interface file (vespidl.pk) to root. If you do not want to run Avaya IC as root, you must change the ownership of these files as described in Changing ownership for Avaya IC - Solaris and AIX only on page 38.

Installing the license file

After you obtain the license file, install the file in the WebLM. For more information on how to obtain a license file, see *IC Installation Planning and Prerequisites*.

CAUTION:
Do not change your license file after you receive it from Avaya. WebLM will not accept a modified license.

To install the license file:

1. In your Web browser, navigate to the following URL for the WebLM:
   http://<*machine_name*>.<*domain*>:<*webLM_port*>/WebLM/LicenseServer

   For example, **http://testbox.xyzcorp.com:9601/WebLM/LicenseServer**

   Note:
   The URL for the WebLM is case-sensitive.

   If your contact center uses a proxy server or enhanced security for Internet Explorer, include this address in the browser exception list and the trusted sites list.
2. Select **License Administration**.

3. Type **admin** in the **Password** field and select **Continue**.

   WebLM forces you to change this password immediately to help prevent unauthorized access to your license file. For more information, see Changing the administrative password on page 145.

4. In the **License File Name** field, type the directory path to your license file.

   If you do not know the directory path, select **Browse** and navigate to the license file.

5. Select **Install**.

   If the installation is successful, WebLM displays a confirmation page. If you installed an incorrect license file, or WebLM could not access the location of the license file on your network, WebLM displays an error page.

6. Select the Avaya Interaction Center hyperlink under **Licensed Products**, and confirm that the number of agents and servers matches your expectations.

7. Restart the License Manager:

   a. Select the **Back** button in your Web browser to return to the WebLM main page.

   b. Select **License Administration**.

   c. Type the password for your administrative account in the **Password** field and select **Continue**.

   d. Under **Restart License Manager**, select **Restart**.

Configuring multi-site licenses

If your Avaya IC system includes multiple sites, or a redundant multi-server solution, Avaya provides you with a series of segmented licenses for Avaya IC. One license file is created with a segment for each WebLM server. Each segment contains the software and agent licenses for a specific WebLM server. This license file can be used by all the WebLM servers because the license information for a specific server is distinguished by the MAC address of the first physical network interface card. A WebLM server can obtain its licensing information from another WebLM server if its license file became corrupt.

These segmented licenses are also known as peer-to-peer licenses or multi-site licenses.

Note:
If network latency is an issue, you can create a separate license file for each WebLM server. The license file will only contain the license information for a specific server. This configuration will reduce network traffic, but the license information will be lost if the license file becomes corrupt.

To configure multi-site licenses:

1. Install the appropriate segmented license in all WebLMs in your Avaya IC system, by following the instructions in Installing the license file on page 141.
2. After you install the licenses, return to the **License Administration** page.
3. Configure the peer servers for the segmented license, by following the instructions below.
4. Repeat the configuration process on every machine in your Avaya IC system that hosts a WebLM.

Configuring peer servers for multi-site licenses

To configure peer servers for multi-site licenses:

1. In the **License Administration** page, scroll down to the Peer Server Administration section at the bottom of the page.
2. Select **View/Edit Host List**.
3. In the **Peer Host Administration** page, enter the URL for the WebLM on each machine, including the fully-qualified domain name and port.

   Avaya recommends that you do not use the IP address of the machine in the URL. A sample URL is:

   `<machine_name>.<domain>:<webLM_port>/WebLM/LicenseServer/`

   For example, **`testbox.xyzcorp.com:9601/WebLM/LicenseServer/`**

   Note:
   The URL for the WebLM is case-sensitive.

4. Select **Submit Changes**.

   Repeat steps 3 and 4 for every machine in your system that hosts a WebLM except the machine that you are configuring.

   If you are unable to add a peer host machine to the Peer Host Administration page, make sure that the other machine is up and running, and that the appropriate segmented license is installed.

Configuring the License server

This section includes information about how to configure the License server that is automatically installed with the primary ORB server. Use the same configuration parameters in all other License servers in the Avaya IC system.

Do not host more than one License server on a machine. If your Avaya IC system requires multiple License servers, you must host them on different machines.

To configure the License server:

1. In IC Manager, double-click the License server in the list of servers.
2. Select the **General** tab and complete the fields in the following table.

Field	Recommended entry	Notes
Name	License_<*domain*>	Include the domain in the server name to identify the server.
Domain	Select the Avaya IC domain for the server from the drop-down list.	For example, select **Default** from the drop-down list if the server is in the Default domain.
Host	Select the machine's IP address from the drop-down list, or type the IP address if it is not in the list.	When you select the host, IC Manager fills in the fields for Directory, Port, and Executable.

3. Select the **License Server** tab and complete the fields in the following table.

Field	Recommended entry	Notes
Warn about upcoming license expiry	Check this field.	
Time in advance of expiry (hours)	If you selected Warn about Upcoming License Expiry, enter the amount of time before the license expires that you want to be warned.	Default is 96 hours. You can

Field	Recommended entry	Notes
Alarm on no licenses	Check this field.	
WebLM Server URLs	1. Select the Ellipsis (…) button. 2. Add the URL of the server page for each WebLM License Manager. 3. Select the OK button. **Note:** The URL for the WebLM is case-sensitive.	Repeat this step for each WebLM in your Avaya IC system. For example, the default URL is `http://<machine_name>.<domain>:<port>/WebLM/LicenseServer` **Important:** Avaya recommends that you do not use the IP address of the machine in the URL.

4. Select **OK**.
5. Start the License Server.
6. Confirm that the Alarm Manager at the bottom of the IC Manager window displays a confirmation message, such as "At least one WebLM server configuration is working". If you do not see this alarm message, your license is not working correctly.

Changing the administrative password

The Web License Manager does not impose constraints on the administrative password. However, Avaya recommends that you use a combination of alphabetic and numerical characters.

To change the administrative password for Web License Manager:

1. In your internet browser, navigate to the URL of the server page for the WebLM.

   A sample URL is **`http://<machine_name>.<domain>.<webLM_port>/WebLM/LicenseServer`**

   The URL for the WebLM is case-sensitive.
2. Select **License Administration**.
3. Type your current password in the **Old Password** field.
4. Complete the following fields under **Change Administrator Password**:
   - Old password
   - New password
   - Re-type new password
5. Select **Change password**.

Chapter 6: Configuring Telephony

The Avaya Computer Telephony for IC (Telephony) is part of the voice channel of Avaya Interaction Center (Avaya IC).

You can use the information in this chapter to set up a simple Telephony environment with one Telephony server and one PBX or ACD. Avaya IC also supports more complex Telephony environments, including multiple Telephony servers with multiple PBXs or ACDs that work independently or together as an integrated environment. You can also configure an IVR.

To configure Telephony, perform the steps in the following topics:

Your Avaya IC system can also include the following optional configurations:

- Multi-site heterogeneous switches, as described in *IC Telephony Connectors Programmer Guide*.
- Return on No Answer (RONA), as described in *IC Telephony Connectors Programmer Guide*.
- Connections to an IVR, as described in *VOX Server Programmer Guide*.

Before you configure Telephony

Before you configure Telephony and related components, make sure that you:

1. Install and configure all prerequisite software and hardware. The prerequisites can include one or more of the following:
   - Database
   - Telephony switch, equipment, and software
   - IVR (optional)

   For more information about the prerequisites and supported platforms for Telephony, see *IC Installation Planning and Prerequisites*.
2. Copy the Avaya IC server files to the target machines, as described in Installing Avaya IC server and administration components on page 29.
3. Configure a secondary server environment, as described in Configuring the ORB server environment on page 33.
4. Perform all the steps to configure the Avaya IC core servers, databases, and related components, as described in Configuring core servers on page 99.

Configuring the ACD name parameter

You must configure an ACD name parameter for each ACD in your Avaya IC system. You can include identifying information, such as department or site in the ACD name.

To configure the ACD name parameter:

1. In IC Manager, select the **Configuration** tab.
2. From the **Tables** list in left pane, select **Telephony** > **ACD Name**.
3. Select **New**.
4. Type an alphanumeric name for the ACD in the **ACD Name** field.

   Do not use spaces or special characters in the name.
5. Select **OK**.
6. Refresh the Directory server:
   a. Select **Manager** > **Refresh**.
   b. In the Success message, select **OK**.

   If you do not receive a Success message, perform the steps in Troubleshooting the refresh in IC Manager on page 406.

Creating the Telephony server

The Telephony server (TS) is the connector server for the voice channel. This server interfaces with a switch (PBX), monitors phone calls, and controls telephony routing. This server uses the EDU server to record information on telephone calls. The Telephony server is specific to the switch you are using.

This section describes how to set up a Telephony server for a single site that does not receive more than 10,000 voice contacts per hour. To configure a Telephony server for a more complex system or a higher volume site, or for more information about the Telephony server, see *IC Telephony Connectors Programmer Guide*.

For information about how to configure the VDN, CDN, or CCT on each link of the switch to communicate with the Telephony server, see *IC Installation Planning and Prerequisites*.

To create a Telephony server:

1. Select **Server** > **New** in IC Manager.
2. Select **TS** from the list of servers. Select **OK**.
3. Select the **General** tab and complete the fields as shown in the following table.

Field	Recommended entry	Notes
Name	TS_<*domain*>_<*switch*>	Include the name of the domain and the name of the switch in the server name to identify the server.
Domain	Select the Avaya IC domain for the server from the drop-down list.	For example, select `Voice1` from the drop-down list if the server is in the Voice domain.
Host	Select the machine's IP address from the drop-down list, or enter the IP address if it is not in the list.	When you select the host, IC Manager fills in the fields for Directory, Port, and Executable.

4. Perform the steps in the following table to complete the Telephony server configuration.

Telephony switch	Location of step
Avaya DEFINITY or Avaya Communication Manager (Avaya DEFINITY/Communication Manager)	Configuring the Telephony server for Avaya DEFINITY/Communication Manager on page 150
Aspect	Configuring the Telephony server for Aspect on page 151

Telephony switch	Location of step
Nortel Meridian	Configuring the Telephony server for Nortel Meridian Link on page 154
Nortel Symposium	Configuring the Telephony server for Nortel Symposium on page 155
Ericsson MD110	Configuring the Telephony server for Ericsson MD110 on page 156

Configuring the Telephony server for Avaya DEFINITY/ Communication Manager

For information about the interface between Avaya products and the Avaya IC Telephony server, see *IC Telephony Connectors Programmer Guide*.

Tip:
This section includes only the basic required properties. You can also configure advanced properties or properties on the **Configuration** tab. For example, you can add a parameter to handle blocked ANIs. For more information, see *IC Administration Volume 1: Servers & Domains* and *IC Telephony Connectors Programmer Guide*.

To configure the Telephony Server for Avaya DEFINITY/Communication Manager:

1. If you have not already done so, double-click the Telephony server in the list of servers.
2. Select the **TS** tab and complete the fields as shown in the following table:

Field	Recommended entry	Notes
ACD Name	Select the name of the ACD assigned to the Avaya switch.	The name of the ACD that this TS is serving from a pick list of names assigned to the ACD during system configuration.
ACD Type	Select Avaya	The type of ACD with which the TS will communicate.
ACD Model	Select Definity	The model of the ACD that corresponds to the selected ACD Type.

Field	Recommended entry	Notes
ACD Protocol	Select asai	The protocol to be used between the TS and the ACD. If your system includes a Legacy TS with switch with Avaya DEFINITY software, see *IC/OA Software Upgrade and Data Migration*.
Site	Select the site of your TS.	Select the site that this server is associated with. The TS uses this information to retrieve the queues for internal monitoring.
ACD Link	Enter the IP address (or a name if it can be resolved into an IP) of the MAPD card set.	The device through which the TS communicates with the ACD. Maximum length is 32.
Signal Number	Specify a signal number when configuring multiple Avaya users on a single machine. There is no default value in the TS, but IC Manager sets this value to 1. Maximum length is 8.	The signal extension number of the ASAI line associated with each TS. The signal number is mandatory, if it is not specified, the TS will not be able to establish the link between users.
Call Control	Check to enable call control on every call.	If checked, enables the TS to monitor calls, not stations, on the system.

3. Select **OK**.

Configuring the Telephony server for Aspect

For information about the interface between the Aspect CallCenter switch and the Avaya IC TS, see *IC Telephony Connectors Programmer Guide*.

Tip:
This section includes only the basic required properties. You can also configure advanced properties or properties on the **Configuration** tab. For example, you can add a parameter to handle Aspect data variables. For more information, see *IC Administration Volume 1: Servers & Domains* and *IC Telephony Connectors Programmer Guide*.

To configure the Telephony Server for Aspect:

1. If you have not already done so, double-click the Telephony server in the list of servers.
2. Select the **TS** tab and complete the fields as shown in the following table.

Field	Recommended entry	Notes
ACD Name	Select the name of the ACD assigned to the Aspect switch.	The name of the ACD that this TS is serving from a pick list of names assigned to the ACD during system configuration.
ACD Type	Select Aspect	The type of ACD with which the TS will communicate.
ACD Model	Select Aspect9	Aspect9 applies to all the supported versions of the Aspect ACD.
ACD Protocol	Select AspectCMI	The protocol to be used between the TS and the ACD. Avaya IC automatically selects AspectCMI when ACD Type of Aspect is selected.
Site	Select the site of your TS.	Select the site that this server is associated with. The TS uses this information to retrieve the queues for internal monitoring.
Aspect Contact Server Host	Enter the IP address of the machine that hosts the Aspect Contact server.	
Data Interlink Number	Enter the Data Interlink number.	The Data Interlink number from the Aspect ACD the TS uses to communicate with the ACD.
Aspect Header	Enter the link definition on the Aspect switch.	If this field is empty, the server uses the machine name of the ACD.
Device	Enter the TCP/IP port where the TS needs to create a connection.	Default is 7,046. For a list of default port numbers for components in the Avaya IC suite, see the *IC Installation Planning and Prerequisites*.
Monitored Agent Group	Enter the number assigned to the agent group to monitor.	Default is 1. Do not complete this field if the TS is monitoring all the agent groups on Avaya IC.

Field	Recommended entry	Notes
Monitored Trunk Group	Enter the number assigned to the trunk group to monitor.	Default is 1. Do not complete this field if the TS is monitoring all the trunk groups on Avaya IC.
Monitor All Agent Groups	Check this box if you want the TS to monitor all agent groups.	Default is unchecked. This overrides the entry in the Monitored Agent Group field.
Monitored Super Agent Group	Enter the number assigned to the super agent group to monitor.	Default is 1. Leave this field blank if you do not want the TS to monitor the super agent group.
Monitor All Trunk Groups	Check this field if you want the TS to monitor all trunk groups.	Default is unchecked. This overrides the entry in the Monitored Trunk Group field.
Blind Transfer CCT	Enter the Call Control Table number used to perform blind transfers.	
Make Call CCT	Enter the Call Control Table number used to make calls within the Aspect switch.	
External Calls CCT	Enter the Call Control Table number used to make calls external to the Aspect switch.	
Route CCT	Enter the Call Control Table number used to route calls external to the Aspect switch.	
Transfer CCT	Enter the Call Control Table number used during call transfers.	
Transfer Init CCT	Enter the Call Control Table number used during transfer init operations.	
Predictive CCT	Enter the Call Control Table number used during predictive operations.	

3. Select **OK**.

Configuring the Telephony server for Nortel Meridian Link

For information about the interface between Nortel Meridian switches and the Avaya IC TS, see *IC Telephony Connectors Programmer Guide*.

Tip:
This section includes only the basic required properties. You can also configure advanced properties or properties on the **Configuration** tab. For example, you can add a parameter to handle queues with mixed case names. For more information, see *IC Administration Volume 1: Servers & Domains* and *IC Telephony Connectors Programmer Guide*.

To configure the Telephony Server for Meridian Link:

1. If you have not already done so, double-click the Telephony server in the list of servers.
2. Select the **TS** tab and complete the fields as shown in the following table.

Field	Recommended entry	Notes
ACD Name	Select the name of the ACD assigned to the switch.	The name of the ACD that this TS is serving from a pick list of names assigned to the ACD during system configuration.
ACD Type	Select Nortel	The type of ACD with which the TS will communicate.
ACD Model	Select Meridian	The model of the ACD that matches the selected ACD Type.
ACD Protocol	Select MLP.	The protocol used by Meridian Link Module.
Site	Select the site of your TS.	Select the site that this server is associated with. The TS uses this information to retrieve the queues for internal monitoring.
Link	The logical identifier for the MLP link, which is defined in CT Connect.	The Link establishes a path between a CT Connect client and a given PBX interface. The logical identifier is established in the CT Connect server configuration program.
Node	Enter the hostname or IP address of the server where CT Connect is running.	The Node needs to translate to an IP address via DNS or host table.

3. Select **OK**.

Configuring the Telephony server for Nortel Symposium

For information about the interface between Nortel Meridian switches and the Avaya IC TS, see *IC Telephony Connectors Programmer Guide*.

Tip:
This section includes only the basic required properties. You can also configure advanced properties or properties on the **Configuration** tab. For example, you can add a parameter to handle queues with mixed case names. For more information, see *IC Administration Volume 1: Servers & Domains* and *IC Telephony Connectors Programmer Guide*.

To configure the Telephony Server for Symposium:

1. If you have not already done so, double-click the Telephony server in the list of servers.
2. Select the **TS** tab and complete the fields as shown in the following table.

Field	Recommended entry	Notes
ACD Name	Select the name of the ACD assigned to the switch.	The name of the ACD that this TS is serving from a pick list of names assigned to the ACD during system configuration.
ACD Type	Select Nortel	The type of ACD with which the TS will communicate.
ACD Model	Select Symposium	The model of the ACD that matches the selected ACD Type.
ACD Protocol	Select MLS	The protocol used by Symposium Call Center Server.
Site	Select the site of your TS.	Select the site that this server is associated with. The TS uses this information to retrieve the queues for internal monitoring.
Link	The logical identifier for the MLS link, which is defined in CT Connect.	The Link establishes a path between a CT Connect client and a given PBX interface. The logical identifier is established in the CT Connect server configuration program.
Node	Enter the hostname or IP address of the server where CT Connect is running.	The Node needs to translate to an IP address via DNS or host table.

3. Select **OK**.

Configuring the Telephony server for Ericsson MD110

For information about the interface between Ericsson switches and the Avaya IC TS, see *IC Telephony Connectors Programmer Guide*.

Tip:
This section includes only the basic required properties. You can also configure advanced properties or properties on the **Configuration** tab. For more information, see *IC Administration Volume 1: Servers & Domains* and *IC Telephony Connectors Programmer Guide*.

To configure the Telephony server for Ericsson MD110:

1. If you have not already done so, double-click the Telephony server in the list of servers.
2. Select the **TS** tab and complete the fields as shown in the following table.

Field	Recommended entry	Notes
ACD Name	Select the name of the ACD assigned to the switch.	The name of the ACD (switch) that this TS is serving from a pick list of names assigned to the ACD during system configuration.
ACD Type	Select Ericsson	The type of ACD with which the TS will communicate.
ACD Model	Select MD110	The model of the ACD that matches the selected ACD Type.
ACD Protocol	Select CSTA1	The protocol used by the Application Link Server to communicate with the TS and the switch.
Site	Select the site of your TS.	The site that this TS is associated with. The TS uses this information to retrieve the queues for internal monitoring.
Link	Enter the CT Connect link name that was defined on the CTCServer in the CT Connect configuration.	This name identifies the switch's connection, protocols, and settings. It establishes a path between the CT Connect client and the switch.
Node	Enter the name of the server where CT Connect is running.	This parameter needs to translate to an IP address via DNS or host table.

3. Select the **Configuration** tab

4. For each of the configuration parameters in the following table:
   a. Select **New**.
   b. In the **CTI Type Editor** dialog box:
      1. From the **CTI Type** drop-down list, select **Couple**.
      2. In the **Name** field, enter the name of the parameter from the Name column.
      3. In the **Value** field, enter the value of the property from the Value column.
      4. Select **OK**.

Name	Value	Notes
ericsson_request_interval	Enter 320.	Value must be greater than 320 Sets the period of time in milliseconds between the requests sent by the switch.
allow_names_mixed_case	Enter true.	Values: true or false. Set to true to enable the processing of queue names in the same case used in the switch. Set to false to force all queue names to lower case.
rona_on_divert	Enter false.	Values: true or false. Tells the Telephony server not to wait for a divert event from the switch as an indication of RONA. This setting is needed because the Ericsson MD110 switch does not provide a divert event to redirects calls when RONA is enabled.
device_lock_period	Enter value greater than 5	Value must be greater than 5 By default, this parameter is set to 5 seconds. Set it to a higher value than 5. Set this parameter if an agent cannot hang up a conference that the agent initiated to an external party. This behavior can result from some call progress events being hard to reach due to network congestion or if the Ericsson MD110 is configured to accept a variable number of digits with optional digit suppression.

5. Select **OK**.

Creating the Telephony Queue Statistics server

The Telephony Queue Statistics server (TSQS) monitors the voice channel and maintains queue statistics in the ADU Server. These statistics include contact count and age of oldest contact.

Note:
If Business Advocate handles all routing for voice contacts, you do not need a TSQS server.

The Avaya IC installation program does not automatically add this server.

To create the TSQS:

1. In IC Manager, select **Server** > **New**.
2. Select **TsQueueStatistics** from the list of servers. Select **OK**.
3. Select the **General** tab and complete the fields as shown in the following table.

Field	Recommended entry	Notes
Name	TsQueueStatistics_<*domain*>	Include the domain in the server name to identify the server.
Domain	Select the Avaya IC domain for the server from the drop-down list.	For example, select `Voice1` from the drop-down list if the server is in the Voice domain.
Host	Select the machine's IP address from the drop-down list, or enter the IP address if it is not in the list.	When you select the host, IC Manager fills in the fields for Directory, Port, and Executable.

4. Perform the steps in the following table to complete the TSQS server configuration.

Telephony switch	Location of step
Avaya DEFINITY or Avaya Communication Manager	Configuring the TSQS server for Avaya DEFINITY/Communication Manager on page 159
Aspect	Configuring the TSQS server for Aspect on page 160
Nortel Meridian	Configuring the TSQS server for Nortel Meridian Link on page 161

Telephony switch	Location of step
Nortel Symposium	Configuring the TSQS server for Nortel Symposium Call Center on page 162
Ericsson MD110	Configuring the TSQS server for Ericsson MD110 on page 163

Configuring the TSQS server for Avaya DEFINITY/Communication Manager

Tip:
This section includes only the basic required properties. For information about the advanced properties, see *IC Administration Volume 1: Servers & Domains*.

To configure the TSQS for Avaya DEFINITY or Avaya Communication Manager:

1. If you have not already done so, double-click the TSQS server in the list of servers.
2. Select the **TSQS** tab and complete the fields as shown in the following table.

Field	Recommended entry	Notes
ACD Name	Select an ACD Name.	The name of the ACD (switch) that this TSQS is serving. Provides a pick list of name(s) assigned to the switch during system configuration. Each TSQS on the system must have a unique ACD Name.
Site	Select the site where the TSQS is located.	The site used by your TS configured for the Avaya switch.
ACD Type	Select Avaya.	The ACD Type option used by your TS configured for the Avaya switch.
ACD Model	Displays Definity after you select Avaya as ACD Type.	The ACD Model option used by your TS configured for the Avaya switch.
ACD Protocol	Select asai.	The ACD Protocol option used by your TS configured for Avaya switch.

3. Select **OK**.

Configuring the TSQS server for Aspect

Tip:
This section includes only the basic required properties. For information about the advanced properties, see *IC Administration Volume 1: Servers & Domains*.

To configure the TSQS for Aspect:

1. If you have not already done so, double-click the TSQS server in the list of servers.
2. Select the **TSQS** tab and complete the fields as shown in the following table.

Field	Recommended entry	Notes
ACD Name	Select an ACD Name	The name of the ACD (switch) that this TSQS is serving. Provides a pick list of name(s) assigned to the switch during system configuration. Each TSQS on the system must have a unique ACD Name.
Site	Select the site where the TSQS is located.	The Site used by your TS configured for the Aspect switch
ACD Type	Select Aspect.	The ACD Type option used by the TS configured for the Aspect switch.
ACD Model	Select Aspect9.	Aspect9 applies to all the supported versions of the Aspect ACD.
ACD Protocol	Displays AspectCMI after you select Aspect8 as the ACD Model.	Select the ACD Protocol option used by your Telephony server configured for the Aspect switch.
Switch Name	Enter the IP address of the link that connects the switch to the TSQS.	This is different from the IP address used by the switch.
Switch Port	Enter the port number used by the switch.	Default is 8000.

3. Select **OK**.

Configuring the TSQS server for Nortel Meridian Link

Tip:
This section includes only the basic required properties. For information about the advanced properties, see *IC Administration Volume 1: Servers & Domains*.

To configure the TSQS for Nortel Meridian Link:

1. If you have not already done so, double-click the TSQS server in the list of servers.
2. Select the **TSQS** tab and complete the fields as shown in the following table.

Field	Recommended entry	Notes
ACD Name	Select an ACD Name.	The name of the ACD (switch) that this TSQS is serving. Provides a pick list of name(s) assigned to the switch during system configuration. Each TSQS on the system must have a unique ACD Name.
Site	Select the site where the TSQS is located.	The site used by your TS configured for the Nortel switch using Meridian Link Module.
ACD Type	Select Nortel.	The ACD Type option used by your TS configured for the Nortel switch using Meridian Link Module.
ACD Model	Select Meridian.	The ACD Model option used by your TS configured for the Nortel switch using Meridian Link Module.
ACD Protocol	Select MLP.	The ACD Protocol option used by your TS configured for the Nortel switch using Meridian Link Module.
Switch Name	Enter the name or IP address of Meridian Max to which the switch connects through MLP.	This setting is defined when the switch administrator configures the Meridian Max.
Switch Port	Enter the port number used by the switch.	Default is 44245.

3. Select **OK**.

Configuring the TSQS server for Nortel Symposium Call Center

Tip:
This section includes only the basic required properties. For information about the advanced properties, see *IC Administration Volume 1: Servers & Domains*.

To configure the TSQS for Nortel Symposium Call Center:

1. If you have not already done so, double-click the TSQS server in the list of servers.
2. Select the **TSQS** tab and complete the fields as shown in the following table.

Field	Recommended entry	Notes
ACD Name	Select an ACD Name.	The name of the ACD that this TSQS is serving. Provides a pick list of names assigned to the switch during system configuration. Each TSQS on the system must have a unique ACD Name.
Site	Select the site where the TSQS is located.	The site used by the TS configured for the Nortel Meridian switch using Symposium Call Center Server.
ACD Type	Select Nortel.	The ACD Type option used by your TS configured for the Nortel Meridian switch using Symposium Call Center Server.
ACD Model	Select Symposium.	The ACD Model option used by your TS configured for the Nortel Meridian switch using Symposium Call Center Server.
ACD Protocol	Select MLS.	The ACD Protocol option used by your TS configured for the Nortel Meridian switch using Symposium Call Center Server.
Switch Name	Enter the name or IP address of the Symposium (directory) to which the switch connects through MLS.	This setting is defined when the switch administrator configures the Symposium Call Center Server.
Switch Port	Enter the port number used by the switch.	Default is 8000.

3. Select **OK**.

Configuring the TSQS server for Ericsson MD110

Tip:
This section includes only the basic required properties. For information about the advanced properties, see *IC Administration Volume 1: Servers & Domains*.

To configure the TSQS for Ericsson MD110:

1. If you have not already done so, double-click the TSQS server in the list of servers.
2. Select the **TSQS** tab and complete the fields as shown in the following table.

Field	Recommended entry	Notes
ACD Name	Select an ACD Name.	The name of the ACD (switch) that this TSQS is serving. Provides a pick list of name(s) assigned to the switch during system configuration. Each TSQS on the system must have a unique ACD Name.
Site	Select the site where the TSQS is located.	The site used by your TS configured for your Ericsson MD110 switch using Application Link Server.
ACD Type	Select CSTA	The ACD Type option used by the TS when configured for the Ericsson MD110 switch using Application Link Server.
ACD Model	Select Generic	The ACD Model option used by the TS when configured for the Ericsson MD110 switch using Application Link Server.
ACD Protocol	Select CSTA1	The protocol used between the TS and the PBX.
CTC Server Name	Enter the name of the server where CT Connect is running.	The node needs to translate to an IP address via DNS or host table.
CTC Link Name	The logical identifier in the server where CT Connect is running.	This link establishes a path between a CT Connect client and a given PBX.

3. Select **OK**.

Creating a voice queue

The sample Incoming Call workflow uses the DefaultVoiceQueue@DefaultTenant voice queue. Avaya recommends that you create this queue and additional queues, including a queue for each possible route (transfer) point where the Incoming Call workflow can route a voice contact.

Avaya IC uses voice queues for the following:

To gather statistics information: The TSQueueStatistics server monitors the queues and maintains statistics in the ADU server. These statistics can then be processed by, for example, Avaya OA. For more information, see Creating the Telephony Queue Statistics server on page 158.

To provide a literal translation for a switch device: With this literal translation, you can reference a destination in the switch. For example, you can reference VDN 1234 as queue_sales. Avaya IC displays queue_sales as a destination in the Unified Agent Directory.

To provide support for multi-site heterogeneous switches: Avaya IC uses the information you enter in the Voice tab of the queue to support multi-site heterogeneous switches. For more information, see *IC Telephony Connectors Programmer Guide*.

To integrate with routing hints: You add the ID of the voice queue to the RoutingHint table when you configure the routing hints used by the Incoming Call workflow. For more information, see Creating routing hints for the Incoming Call workflow on page 172.

The following procedure explains how to create a simple voice queue. For more information, including queues for transfers and multi-site heterogeneous switches, see *IC Administration Volume 2: Agents, Customers, & Queues* and *IC Telephony Connectors Programmer Guide*.

To create a simple voice queue:

1. In IC Manager, select the **Device** tab.
2. Select **Device** > **New Device**.
3. In the **New Device** dialog box, select **Voice Queue**. Select **OK**.
4. In the **Device Editor (Voice)** dialog box:
   a. Select the **General** tab and complete the fields shown in the following table.

Field	Recommended entry	Description
Id	The device number known to the PBX (or ACD).	The ID is the VDN or vector identifier that your PBX or ACD uses for the queue. The ID must be a numeric value. For a Nortel Meridian switch with Symposium, the ID must be the name of the SkillSet defined in the PBX or ACD.

Field	Recommended entry	Description
Site	Select the site of your Telephony server.	
ACD Name	Select the name of the ACD.	This is the ACD Name that you confirmed in Configuring the ACD name parameter on page 148,
Name	Type a name for the voice queue.	For the default voice queue, type DefaultVoiceQueue @DefaultTenant. Queue names can have up to 256 characters, including special characters and spaces. Queue names cannot: • Start with a digit, such as zero (0) • Start with an asterisk "*" or a pound sign "#" • Contain "@" (except default queue) The Unified Agent Directory displays this name to agents.
Media	Voice	Automatically set by IC Manager. You cannot change this field.
Priority	Assign a priority to the queue.	For example, type 1.
Service Level	Type the number of hours, minutes, and seconds in the format HH:MM:SS	The service level defines the time within which all voice contacts in the queue must be answered. Type the time in the format HH:MM:SS.
Minimum agents	1	Type the minimum number of agents who must be active to use the queue.
Addressable	Check this box.	Determines whether the queue is displayed in the Unified Agent Directory.

b. Select the **Voice** tab and complete the fields in the following table.

Field	Recommended entry	Description
Enable EDU Tracking		If selected, the first Telephony server in the TS Set monitors this queue internally. Select this option only under one of the following conditions: ● The switch and CTI link cannot make a call-to-data association. ● The switch supports queue monitoring. ● The environment is configured to ensure that new contacts are pre-processed by one Telephony server, where all the queues reside, but all agents are handled by another Telephony server. (Usually the pre-process has to do with call routing and queue monitoring.) **Note:** In addition to selecting this check box, make sure that the associated Telephony server is the first one in the TS Set list.
Wait Treatment Style	Leave this field blank.	The numeric value associated with the wait treatment configuration on the switch. For more information, contact your switch administrator.
TS Set	Select the **Ellipsis (…)** button and in the dialog box: ● Select **New**. ● Select the Telephony server that handles voice contacts for this queue from the drop-down list. ● After you have added all of the Telephony servers, select **OK**.	Defines the Telephony servers that can be used to deliver voice contacts to this queue, and the order that the Multi-Site Heterogeneous Switch (MSHS) mechanism follows when attempting to deliver contacts to specific queues. In order to do this, the MSHS uses the ADU for its central data store. The TS Set can only include Telephony servers that handle contacts from the switch where the queue resides **Note:** Queue names are kept in cache for 24 hours.

5. Select **OK**.

Starting the Telephony servers

Important:
Create the voice queues before you start the Telephony server and the TSQS server.

To start Telephony servers:

1. Start the Telephony server:
   a. Select the Telephony server.
   b. Right-click on the Telephony server.
   c. Select **Start** from the drop-down list.

   After the Alarm Monitor displays a message confirming that the server has started correctly, continue with the next step.
2. Start the TSQS server:
   a. Select the TSQS server.
   b. Right-click on the TSQS server.
   c. Select **Start** from the drop-down list.

   After the Alarm Monitor displays a message confirming that the server has started correctly, continue with the next step.
3. Set your Telephony server to start automatically:
   a. Double-click the Telephony server in the list of servers.
   b. Select the **General** tab.
   c. Check the **Autostart** box.
   d. Select **OK**.
4. Set your TSQS server to start automatically:
   a. Double-click the TSQS server in the list of servers.
   b. Select the **General** tab.
   c. Check the **Autostart** box.
   d. Select **OK**.

Configuring a Workflow server for Telephony

To create and configure a Workflow server for Telephony, perform the steps in the following topics:

1. Creating a Workflow server for Telephony on page 168
2. Configuring the voice channel for the Workflow server on page 169

If the Avaya IC system includes multiple Workflow servers, perform these steps on each Workflow server that processes voice contacts.

Creating a Workflow server for Telephony

These instructions only provide information about those parameters you need to set when you create a Workflow server to handle voice contacts. For more information about other parameters in the Workflow server, see Configuring multiple Workflow servers on page 109 and *IC Administration Volume 1: Servers & Domains*.

To create a Workflow server for Telephony:

1. In IC Manager, select **Server** > **New**.
2. Select **Workflow** from the list of servers.
3. Select **OK**.
4. Select the **General** tab, and complete the fields shown in the following table.

Field	Recommended entry	Notes
Name	Workflow_<*domain*>	Include the domain in the server name to identify the server.
Domain	Select the Avaya IC domain for the server from the drop-down list.	For example, select `Voice1` to use the preconfigured domain for Telephony.
Host	Select the machine's IP address from the drop-down list, or type the IP address if it is not in the list.	When you select the host, IC Manager fills in the fields for Directory, Port, and Executable.

5. Select the **Workflow** tab.
6. From the **IC Data Source** drop-down list, select the Interaction Center data source.

   The default name for this data source is interaction_center. This is the data source that you created in Generating the Interaction Center application on page 84.
7. Select **Synchronous Startup Flows.**

8. If the following row does not exist, add it to the Synchronous Startup Flows:
   a. Select **New**.
   b. In the new row, type `web_routing.update_qw_cache`
   c. Select **OK**.
9. Continue with Configuring the voice channel for the Workflow server on page 169.

Configuring the voice channel for the Workflow server

To configure the voice channel for the Workflow server:

1. In the Server Editor for the Workflow server, select the **Channels** tab.
2. Select **New Channel**.
3. In the **Channel Editor** dialog box, complete the fields as shown in the following table. Select **OK**.

Field	Recommended entry	Notes
Global	Do not check this field.	Do not check this field to create a create a channel for a specific server or media, such as Telephony.
By Server	• Do not check this field if you want this channel to handle events from all servers of the type that you select from the **Service** drop-down list. • Check this field if you want this channel to handle events from only one specific server that you select from the **Service** drop-down list.	If you check this field, and you need this Workflow server to communicate with more than one server, you must create another channel for that server. **Warning:** If you check this field and the Telephony server is named "TS", the Workflow server will not be able to communicate with the Telephony server.
Channel Range	No entry necessary.	Completed by IC Manager

Field	Recommended entry	Notes
Service	Select **TS** or a specific Telephony server from the drop-down list.	Whether you can select a server or a type of server, depends up whether or not you checked the **By Server** field.
Criteria	Type the criteria you want the workflow to use for the event.	For example, you can enter a criteria for the workflow to route calls that arrive at a routing point. For a detailed description of the criteria for each server and server type, see the description of the `Assign` method in the Programmer Guide for that server. For example, to see criteria for the Telephony server, see *IC Telephony Connectors Programmer Guide*.

4. Select the channel that you created in the step above.
5. Select **New Association**.
6. In the **Channel Association** dialog box, complete the fields as shown in the following table. Select **OK**.

Field	Recommended entry
Channel Range	Completed by IC Manager
Service Interface	Completed by IC Manager
Event	TS.IncomingCall **Note:** This field is case-sensitive.
Flow	Type `<workflow_project>.<routing_workflow>` For example, if you use the sample Incoming Call workflow, type `ts.incomingcall` **Note:** This field is case-sensitive.

7. Select **OK**.
8. Select **OK**.
9. In the Server tab of IC Manager, select the Workflow server that handles voice contacts.
10. Right-click the Workflow server and select **Start**.

Building and loading workflows for Telephony

You can use the sample workflows to configure and test your Telephony servers. When you move into production, modify the properties of the sample workflows to meet your system needs and configuration. For more information about the sample workflows and ways to customize them, see *Avaya IC Media Workflow Reference*.

For each workflow project, perform the steps in the following topics:

1. Building the Incoming Call workflow on page 171.
2. Loading workflows in the Workflow server on page 172.

Building the Incoming Call workflow

You do not need to configure any blocks to use the sample Incoming Call flow.

To build the Incoming Call workflow:

1. In Workflow Designer, select **File** > **Open Project** and open the TS project.

   You can find the TS project in the following directory: `IC_INSTALL_DIR\IC71\design\IC\Flows\Avaya\TS\TS.prj`
2. Double-click incomingcall.qfd in the **Project** pane.
3. Select **Project** > **Settings**.
4. Select the **Database** tab and type the following values:
   - Interaction Center Data Source name in the **IC Data Source** field
   - Valid Avaya IC Administrator account in the **Login ID** field

     The default account is Admin.
   - Password for the account in the **Password** field
5. Select **OK**.
6. Select **Build** > **Build Flowset**.

   Workflow Designer verifies and compiles the flows. All error messages, including the block name, script name, and offending line, are displayed in the Output bar.
7. Select **File** > **Exit** to exit Workflow Designer.

Loading workflows in the Workflow server

When you build a flowset, Workflow Designer does not automatically load and run the workflows in the Workflow server. You can reload workflows without restarting the Workflow server.

Tip:
Test the workflows and confirm that they work correctly. If the Workflow server is not running the new workflows, stop and restart the server.

To reload workflows in the Workflow server:

1. In IC Manager, select the **Servers** tab and double-click the Workflow server.
2. In the **Workflow server** settings dialog box, select the **Workflow** tab.
3. Select **Reload Flows**.
4. In the **Reload Flows** dialog box:
   a. Select **Force Immediate Reload**.
   b. Select **OK** to reload all currently loaded workflows even if the version numbers are the same.
5. Select **OK**.

Creating routing hints for the Incoming Call workflow

The Add Routing Hints (DNIS) block in the Incoming Call workflow uses the routing hints in the RoutingHint table of the Directory server to route incoming voice contacts. The sample Incoming Call workflow requires at least one routing hint for the main incoming DNIS number. Assign this routing hint to a voice queue that you created in Creating a voice queue on page 164.

You can create routing hints for one or more additional DNIS numbers, if required by your contact center.

Important:
Routing hints must be in lower case. Do not use mixed upper and lower case in your routing hints. If the routing hint is not in all lower case, the workflow cannot locate the routing hint, and Avaya IC cannot correctly route the contact.

Each row in the routing hint table contains the following:

- A routing hint
- The name of the voice queues where contacts that match the routing hint should be routed

For more information about how workflows use routing hints, see *Avaya IC Media Workflow Reference*.

To create routing hints:

1. In IC Manager, select the **Configuration** tab.
2. In the left pane, select **Tables** > **Workflow** > **RoutingHint**.
3. Select **New**.
4. In the right pane, complete the fields shown in the following table:

Parameter	Recommended entry	Description
Routing Hint	Type a routing hint.	For the sample Incoming Call workflow, create a routing hint with the DNIS for the incoming calls. For example, if the DNIS is 21000, type 21000 in this field. The routing hint must be a single word in all lower case or a series of numbers. Do not use special characters.
Voice Queue ID	Type the name of a voice queue.	Avaya recommends that you do not use DefaultVoiceQueue@DefaultTenant for routing hints. For information on how to create a voice queue, see Creating a voice queue on page 164.
Category/Qualifier	Leave this field blank.	Business Advocate uses this field.
Tenant	Leave this field blank.	Telephony does not use tenancy.

5. Select **OK**.
6. Select **Manager** > **Refresh**.

Chapter 7: Configuring Web Management

Web Management is a Web-based marketing, sales, and service application that personalizes and manages Web transactions for Avaya Interaction Center. Configure Web Management if your Avaya IC system includes Web Management or Email Management.

This section includes the following topics that describe Web Management and the steps that you must perform to complete the configuration of Web Management:

This section includes the following topics about optional Web Management configurations:

For information on how to set up RONA for Web Management, see *IC Administration Volume 2: Agents, Customers, & Queues*.

Web Management support for media channels

The following table shows the integrated functionality that Web Management provides and the support that the functionality provides for the chat channel and the email channel.

Feature or component	Chat channel	Email channel
Customer management	X	X
Self-service to provide suggested responses for agents	X	X
Chat escalation	X	–
Web scheduled calls	X	–
Email escalation	–	X
Survey	X	–
WebACD server administration	X	X
Web page multi-tenancy and multi-tenancy administration	X	X
DataWake and DataWake administration	X	X
Chat server and client components	X	–

Before you configure Web Management

Before you configure Web Management, make sure that you:

1. Install and configure all prerequisite software and hardware, including a Web server and a JDK.

   For information on which prerequisites you need for each machine, see *IC Installation Planning and Prerequisites*.

2. Copy the Avaya IC server files to the target machines, as described in Installing Avaya IC server and administration components on page 29.
3. Configure a secondary server environment, as described in Configuring the ORB server environment on page 33.
4. Perform all the steps to configure the Avaya IC core servers, databases, and related components, described in Configuring core servers on page 99.

Configuring servers for Web Management

You must add and configure Web Management servers to use Web Management and Email Management. These instructions include only those properties required to get the servers up and running. For information about other server properties, see *IC Administration Volume 1: Servers & Domains*.

This section describes the Web Management servers and how to configure them. Topics include:

Note:
Add and configure the servers in the order in which they are presented in the following topics. Avaya IC systems that include the email channel, but not the chat channel, do not require the Attribute server.

1. Creating the WebACD server on page 177.
2. Creating the Attribute server on page 181.
3. Creating the ComHub server on page 182.
4. Creating the Paging server on page 184.
5. Starting the Web Management servers on page 186.

Creating the WebACD server

The WebACD server performs as a call distributor for chat and email contacts. This server assigns tasks to agents and tracks the different states of the agent interactions. This server uses the Attribute server, Paging server, IC Email server, and ComHub server to complete support operations such as managing agent states and administering agent and contact interactions. This server is also known as the Web Agent Automatic Call Distributor server.

The Avaya IC installation program does not automatically add this server. Web Management and Email Management require this server.

If your Avaya IC system includes multiple domains, ensure that the failover strategy for the WebACD server includes the following:

- The domain that includes your IC Email server must failover to the domain that includes your WebACD server.
- The domain that includes your WebACD server must failover to the domain that includes your IC Email server.

Tip:
On your development system, or if you encounter issues with the WebACD server, Avaya recommends that you set the WACD trace levels on the **Debug** tab to 10,000 or 100,000.

To create the WebACD server:

1. Select **Server** > **New** in IC Manager.
2. Select **WACD** from the list of servers. Select **OK**.
3. Select the **General** tab and complete the fields in the following table.

Field	Recommended entry	Notes
Name	WebACD_<*domain*>	Include the domain in the server name to identify the server.
Domain	Select the Avaya IC domain for the server from the drop-down list.	For example, select `Web` from the drop-down list.
Host	Enter or select the machine's IP address from the drop-down list.	When you select the host, IC Manager fills in Directory, Port, and Executable.

4. Select the **WACD** tab and complete the fields in the following table.

Field	Recommended entry	Notes
Host Name	Enter the name of the machine that hosts the WebACD server.	For example, enter TESTBOX.
Domain	Enter the domain of the machine that hosts the WebACD server.	For example, enter xyzcorp.com.
Service Port	4010	If you must change this port, see *IC Installation and Configuration* for a list of the default port numbers used by the other Avaya IC servers. Port conflicts can cause serious problems within the Avaya IC system.
IC Data Source	Select the Interaction Center Data Source.	If you used the default name, select `interaction_center`.
WACD Webserver	Enter the name and domain of the machine that hosts the Web Administration pages.	For example, enter TEXTBOX.xyzcorp.com.

Field	Recommended entry	Notes
Port	Enter the port that the WebACD server uses for connections with Web applications.	Default port is 80 unless you plan to configure SSL for your website. If you must change this port, see *IC Installation and Configuration* for a list of the default port numbers used by the other Avaya IC servers. Port conflicts can cause serious problems within the Avaya IC system.
Protocol	Select the protocol that you use to connect to the Website.	Select `http` unless you plan to configure SSL for your Website. For more information on SSL, see *IC Installation and Configuration*.
Comhub Host Name	Enter the fully-qualified domain name of the machine that hosts the ComHub server.	For example, enter TESTBOX.xyzcorp.com.
Comhub Port	Enter the service port for the Comhub server.	Default service port is 4001. If you must change this port, see *IC Installation and Configuration* for a list of the default port numbers used by the other Avaya IC servers. Port conflicts can cause serious problems within the Avaya IC system.
Website Context	Enter the name of the Web application used for Web Management.	The default website context is `website`.
Agent Timeout (secs)	100	If the WebACD assigns a contact to an agent who has turned on the "Wait for agent confirmation before accepting a contact" option in Avaya Agent, then this value specifies the number of seconds that the WebACD server will wait for confirmation from that agent before it reassigns the contact to another available agent. For details about setting this option, see the *Avaya Agent User Guide*.
Max Display Tasks	*No recommended entry*	Enter the number of currently active tasks to display per request in the WebACD administration pages.

Field	Recommended entry	Notes
Task Wrap Timeout (secs)	*No recommended entry*	The WebACD server automatically wraps and completes a task after an customer or agent has timed out. For example, if the Avaya Agent shuts down and the user is forced to end the consultation, the WebACD server waits until the amount of time specified in the wrap-up timeout parameter has passed, then wraps and completes the task.
Interval Between Cleanup (mins)	*No recommended entry*	Enter the period of time that the WebACD should wait between cleaning up threads from timed out and abandoned chat tasks.
Max Allowed Queue Time (mins)	*No recommended entry*	Enter the maximum time that a chat task can stay in a queue before it is considered to be dead or abandoned.
Summary Interval (mins)	*No recommended entry*	Enter the period of time that the WebACD should wait between creating summary records. This interval must be an even divisor of 60 (for example, you can use 4, 5, 6, 10, 12, or 15, but you cannot use 8 or 9.) If you set the interval to 5 minutes, then the WebACD will write summaries at 12:00, 12:05, 12:10, etc.
Requalify Contacts	*No recommended entry*	Enable this option if you want the WebACD server to re-run the Qualify workflow on unassigned tasks.

5. Select **OK** to save your configuration settings.

Creating the Attribute server

The Attribute server acts as a communications bridge between the ICM server and the WebACD server for chats. This server provides:

- Tracking of user web page browsing sessions for DataWake.
- Website property event notifications between the website and the ICM server.

If your Avaya IC system includes DataWake, or you are concerned with performance issues on the Website, you can host a second Attribute server on the Website machine in the DMZ. If your Avaya IC system includes this deployment, configure the secondary ORB server on the machine to start automatically.

The Avaya IC installation program does not automatically add this server. Web Management requires this server.

To create the Attribute server:

1. Select **Server** > **New** in IC Manager.
2. Select **Attribute** from the list of servers. Select **OK**.
3. Select the **General** tab and complete the fields in the following table.

Field	Recommended entry	Notes
Name	Attribute_<*domain*>	Include the domain in the server name to identify the server in the list of servers.
Domain	Select the Avaya IC domain for the server from the drop-down list.	For example, select `Web` from the drop-down list if the server is in the Web domain.
Host	Select the machine's IP address from the drop-down list, or enter the IP address if it is not in the list.	When you select the host, IC Manager fills in the fields for Directory, Port, and Executable.

4. Select the **Attribute** tab and complete the fields in the following table.

Field	Recommended entry
Port	If you must change the default, see Changing the service port for the Attribute server on page 439. Port conflicts can cause serious problems within the Avaya IC system.
Enable DataWake Recording	Check this field if: ● The Avaya IC system includes DataWake ● You want this Attribute server to track the Web pages browsed by a Website customer.

Field	Recommended entry
Enable ICM Bridge	Check this field.
IC Login	By default, this field uses the **icmbridge** account that is provided with Avaya IC. If you have not already done so, change the default password for this account. **Important:** Do not use the Administrative account for IC Manager or any account for which the password may change.
IC Password	Type the password for the account in the IC Login field.
ICM Servers	• Select the **Ellipsis (…)** button. • In the ICM Servers dialog box: – Select **New**. – Check **Enabled**. – Type the name and domain of the machine that hosts the ICM server. For example, TESTBOX.xyzcorp.com. – Accept the default port number or change to an available port. – Select **OK**.

5. Select **OK** to save your configuration settings.

Creating the ComHub server

The ComHub server provides a communications hub for the Web Management and Email Management servers. This server also assists in passing information from a web-based interface to the WebACD server, and helps the WebACD server to respond to agent requests, such as logon or logoff.

The Avaya IC installation program does not automatically add this server. Web Management and Email Management require this server.

To create the ComHub server:

1. Select **Server** > **New** in IC Manager.
2. Select **ComHub** from the list of servers. Select **OK**.

3. Select the **General** tab and complete the fields in the following table.

Field	Recommended entry	Notes
Name	Comhub_<*domain*>	Include the domain in the server name to identify the server.
Domain	Select the Avaya IC domain for the server from the drop-down list.	For example, select `Web` from the drop-down list if the server is in the Web domain.
Host	Select the machine's IP address from the drop-down list, or enter the IP address if it is not in the list.	When you select the host, IC Manager fills in the fields for Directory, Port, and Executable.

4. Select the **ComHub** tab and complete the fields in the following table.

Field	Recommended entry	Notes
Host Name	Enter the fully-qualified domain name of the machine that hosts the ComHub server.	For example, enter TESTBOX.xyzcorp.com.
Service Port	Accept the default port of 4001 or enter a new port.	If you must change the default, see Changing the service port for the ComHub server on page 438. Port conflicts can cause serious problems within the Avaya IC system.
IC Data Source	Select the Interaction Center Data Source.	If you used the default name, select `interaction_center`.
Threads	Accept the default or enter a number of threads.	The default entry is 10. The number of threads that can be constructed to handle communication tasks.

5. Select **OK** to save your configuration settings.

Creating the Paging server

The Paging server serves as a communications bridge between Avaya Agent and the WebACD server. This server brokers messages to ensure they are sent to the correct agents and to the WebACD server.

Important:
When you create Avaya IC accounts for agents who handle chat contacts, make sure that the domain for those agents fails over to the domain that includes the Paging server.

The Avaya IC installation program does not automatically add this server. Web Management and Email Management require this server.

To create the Paging server:

1. Select **Server** > **New** in IC Manager.
2. Select **Paging** from the list of servers. Select **OK**.
3. Select the **General** tab and complete the fields in the following table.

Field	Recommended entry	Notes
Name	Paging_<*domain*>	Include the domain in the server name to identify the server.
Domain	Select the Avaya IC domain for the server from the drop-down list.	For example, select `Web` from the drop-down list if the server is in the Web domain.
Host	Select the machine's IP address from the drop-down list, or enter the IP address if it is not in the list.	When you select the host, IC Manager fills in the fields for Directory, Port, and Executable.

4. Select the **Paging** tab and complete the fields in the following table.

Field	Recommended entry	Notes
Host Name	Enter the name of the machine that hosts the Paging server.	For example, enter TESTBOX. **Important:** The Avaya IC agent desktop application uses this host name without the "Domain" name to connect to the Paging server. Configure the agent machine to use the host name without the domain name suffix to communicate with the machine that hosts the Paging server.
Domain	Enter the domain of the machine that hosts the Paging server.	For example, enter xyzcorp.com. **Important:** The Avaya IC agent desktop application does not use this Domain field to connect to the Paging server. For more information, see the Notes for **Host Name** above.
Service Port	4200	If you must change the default, see Changing the service port for the Paging server on page 439. Port conflicts can cause serious problems within the Avaya IC system.
ComHub Host Name	Enter the fully-qualified domain name of the machine that hosts the ComHub server.	For example, enter TESTBOX.xyzcorp.com.

5. If you changed the default service port of 4001 for the Comhub server, perform the following steps:
   a. Right-click on a blank space of the **Paging** tab.
   b. Check the box next to **Show Advanced Properties**.
   c. In the **Comhub Port** field, type the service port for the Comhub server.
6. Select **OK** to save your configuration settings.

Starting the Web Management servers

Before you configure your media channels, Avaya recommends that you start the Avaya IC servers, including the Web Management servers. When you start the Attribute server, the WebACD server will start automatically.

To start the Web Management servers:

1. Select the server.
2. Right-click on the server and select **Start**.

For more information about the correct order for starting and stopping Web Management and other Avaya IC servers, see Starting and stopping Avaya IC servers on page 120.

Setting startup options for servers in IC Manager

Set the following Web Management servers to autostart:

- Attribute server
- ComHub server
- Paging server
- Workflow server that processes chat contacts

To set startup options for servers in IC Manager:

1. Double-click the server in the **Server** tab.
2. Select the **General** tab.
3. Check the **Auto Start** box.

Configuring Web Management services

This section describes how to install and configure Web Management services for each operating system that Avaya IC supports. This section includes the following topics:

Where to configure Web Management services

Configure Web Management services on the following:

- Machines that host Web Management Websites
- Machines that host the WebACD server and Attribute servers to configure database access for:
  - Suggested Response feature of the WebACD server
  - DataWake recording feature of the Attribute server

Hosting multiple Web applications on one machine

If the Avaya IC system includes more than one Web application on the same machine as the WebLM, Avaya recommends that you configure all of the Web applications on the target machine at the same time.

Important:
If you do not configure all of the Web applications simultaneously, leave the options for all Web applications on the target machine checked when you re-run the Configuration Tool to create the new Web applications. If you do not leave the options for the previously created Web applications checked, the Configuration Tool may delete those Web applications.

Setting memory allocation for Web Management services

The Web tab also includes advanced properties for the Java Virtual Machine. Only configure the advanced properties if you expect a high volume of contacts on the Website. For more information, see Configuration Tool advanced properties on page 447.

The advanced properties use the following format:

```
-<initial_Java_heap> -<maximum_Java_heap>
```

If you expect a high volume of chat contacts, increase the default settings for the advanced properties. For example, you can use the advanced properties to increase the memory allocations for the Website JVM and ICM JVM should be adjusted upward. For high volumes, Avaya recommends that you configure each of these properties to:

```
-Xms128m -Xmx512m
```

Configuring Web Management services on Windows

Use these instructions if you plan to host Web Management services on a Windows machine.

You do not need to stop the IIS Web server on Windows machines.

To configure Web Management services to run on a Windows machine:

1. To start the Configuration Tool, select **Start** > **Programs** > **Avaya Interaction Center 7.1** > **Configuration Tool**.

   If the Configuration Tool is already open, close and re-open it to ensure that the Configuration Tool includes all system changes, such as new servers.
2. Log in with your IC Manager login ID and password.
3. Select the **Web** tab.
4. Complete the general fields in the following table.

Field	Description	Sample entry
JDK Home	The path to the directory where the Java SDK is installed. For more information about the Java SDK, see *IC Installation Planning and Prerequisites*.	`C:\j2sdk1.4.2_08`
Tomcat Base Port	The port used to configure the following ports: ● Tomcat HTTP ports for Web applications ● Tomcat AJP (Web server connector) ports	Default: 9600
IIS Website	The name of the IIS Web server that the Web application will use. **Tip:** For a localized version of IIS, type the localized name for the IIS Web server.	Default Web Site
Web Server Host	The name of the machine that hosts the Web server. Do not include the DNS domain.	testbox
DNS Domain	The network (DNS) domain of the machine that hosts your Web server. Do not enter an Avaya IC domain. **Note:** Verify the default DNS domain carefully to ensure that it is correct.	xyzcorp.com

Field	Description	Sample entry
Web Server Port	The port that your Web server uses for communication. Make sure that the port matches the protocol used by your Web server for communication. The default ports are: ● HTTP port is 80. ● HTTPS port is 443. Do not change the default port unless you assign a different port to the Web server.	Default: 80
IC Test	Optional. IC Test is a Web application that you can use to test your Tomcat configuration. If you install multiple versions of Tomcat, the Configuration Tool creates an IC Test application on each version of Tomcat. The Configuration Tool also creates a separate Tomcat server to host IC Test. To access IC Test, use the Tomcat HTTP port in the URL. For example, type: http://<*server*>.<*domain*>.com:9606/ictest **Note:** The port number is not required if you install a single version of Tomcat, or access IC Test from the separate Tomcat server for IC Test.	Checkmark in box

5. Complete the Web Management fields in the following table.

Field	Description	Sample entry
Configure Web Management	Check this box if you want to configure Web Management services on the target machine. After you check this box, the Configuration Tool automatically: ● Displays the other Web Management fields ● Checks the following boxes: – Website – ICM – CIRS – Attribute - DataWake recording (PDM)	Checkmark in box

Field	Description	Sample entry
Website	Creates the Website Web application and performs other tasks that are required to configure a Web Management Website on the target machine. After you check this box, the Configuration Tool displays the following required fields for the Website: ● Website Virtual Directory Name ● WebACD ● Attribute Server	Checkmark in box
Website Virtual Directory Name	The name of the virtual directory for the Website.	website
WebACD	The WebACD server in your Avaya IC system. You must create the WebACD server before the Configuration Tool can include the server in the drop-down list. If the list does not include the server, close the Configuration Tool and create the server. For more information, see Creating the WebACD server on page 177.	WebACD_web
Attribute Server	The Attribute server that the DataWake plug-in uses. You must create the Attribute server before the Configuration Tool can include the server in the drop-down list. If the list does not include the server, close the Configuration Tool and create the server. For more information, see Creating the Attribute server on page 181.	Attribute_web
ICM Service	Configures the ICM server and related components on the target machine. For more information, see Configuring the ICM server on page 211.	Checkmark in box
CIRS Service	Configures the CIRS server and related components on the target machine. For more information, see Configuring the Central Internet Routing service on page 213. **Important:** Only configure a CIRS server if your Avaya IC system includes more than one ICM server.	Checkmark in box
Attribute - DataWake recording (PDM)	Configures the DataWake recording feature of the Attribute server.	Checkmark in box

Field	Description	Sample entry
IC Login	Use the website account that you imported into the database with the seed data. If you have not already done so, change the default password for this account. For more information, see *IC Administration Volume 2: Agents, Customers, & Queues*. **Note:** Do not use the Administrator account for IC Manager or any other account for which the password may change.	website
IC Password	The password used by the IC Login.	website
IC Data Source	The Interaction Center data source that you create with the Interaction Center application for the CallCenterQ database. For more information, see Generating the Interaction Center application on page 84.	interaction_center
Repository Data Source	The Repository data source that you create with the repository application for the IC Repository database. For more information, see Generating the IC Repository application on page 73.	repository
Database Login	Type a DBA login ID for the database server.	*SQL Server*: sa *Oracle*: sys
Database Password	The password for the DBA login ID.	admin
Oracle Home	*Oracle databases only.* The home directory of the Oracle client on the machine that hosts the Web Management servers.	*SQL Server*: leave empty *Oracle*: `C:\Oracle\Ora9`

6. Select **Apply Settings**.
7. Select **OK** in the **Success** dialog box.
8. Select **Exit**.
9. To complete the configuration, perform the following steps to ensure that all Web Management services start properly:
   a. Open the Windows Services control panel.
   b. Start Avaya IC Web Management Service 7.1, as described in Starting and stopping Avaya IC services on page 127.

Configuring Web Management services on Solaris

Use these instructions if you plan to host Web Management services on a Solaris machine.

Important:
To configure Web Management services on Solaris, log in as a user with write permissions on the Web server directories and the Avaya IC installation directories. The root user usually has these write permissions.

To configure Web Management services to run on a Solaris machine:

1. Stop the Sun ONE server that hosts the Website application, as described in Starting and stopping Sun ONE Server Web server on page 130.
2. If the Configuration Tool is already open, close it to ensure that the Configuration Tool includes all system changes, such as new servers.
3. Start the Configuration Tool:
   a. Navigate to `IC_INSTALL_DIR/IC71/bin`
   b. Run **`./configure`**
4. Log in with your IC Manager login ID and password.
5. Select the **Web** tab.
6. Complete the general fields in the following table.

Field	Description	Sample entry
JDK Home	The path to the directory where the Java SDK is installed. For more information about the Java SDK, see *IC Installation Planning and Prerequisites*.	`/opt/j2sdk1_4_2_08`
Tomcat Base Port	The port used to configure the following ports: • Tomcat HTTP ports for Web applications • Tomcat AJP (Web server connector) ports	Default: 9600
Web Server Home	The installation path for the Sun ONE Server that hosts the Web application.	`/opt/SUNWwbsvr`
Web Server Name	The root name of the server as found in the Sun ONE Server home directory. **Note:** Do not include **`https-`** in the Web server name.	testbox.xyzcorp.com
Web Server Host	The name of the machine that hosts the Web server. Do not include the DNS domain.	testbox

Field	Description	Sample entry
DNS Domain	The network (DNS) domain of the machine that hosts your Web server. Do not enter an Avaya IC domain. **Note:** Verify the default DNS domain carefully to ensure that it is correct.	xyzcorp.com
Web Server Port	The port that your Web server uses for communication. Make sure that the port matches the protocol used by your Web server for communication. The default ports are: ● HTTP port is 80. ● HTTPS port is 443. Do not change the default port unless you assign a different port to the Web server.	Default: 80
IC Test	Optional. IC Test is a Web application that you can use to test your Tomcat configuration. If you install multiple versions of Tomcat, the Configuration Tool creates an IC Test application on each version of Tomcat. The Configuration Tool also creates a separate Tomcat server to host IC Test. To access IC Test, use the Tomcat HTTP port in the URL. For example, type: http://<*server*>.<*domain*>.com:9606/ictest **Note:** The port number is not required if you install a single version of Tomcat, or access IC Test from the separate Tomcat server for IC Test.	Checkmark in box

7. Complete the Web Management fields in the following table.

Field	Description	Sample entry
Configure Web Management	Check this box if you want to configure Web Management services on the target machine. After you check this box, the Configuration Tool automatically: ● Displays the other Web Management fields ● Checks the following boxes: – Website – ICM – CIRS – Attribute - DataWake recording (PDM)	Checkmark in box
Website	Creates the Website Web application and performs other tasks that are required to configure a Web Management Website on the target machine. After you check this box, the Configuration Tool displays the following required fields for the Website: ● Website Virtual Directory Name ● WebACD ● Attribute Server	Checkmark in box
Website Virtual Directory Name	The name of the virtual directory for the Website.	website
WebACD	The WebACD server in your Avaya IC system. You must create the WebACD server before the Configuration Tool can include the server in the drop-down list. If the list does not include the server, close the Configuration Tool and create the server. For more information, see Creating the WebACD server on page 177.	WebACD_web
Attribute Server	The Attribute server that the DataWake plug-in uses. You must create the Attribute server before the Configuration Tool can include the server in the drop-down list. If the list does not include the server, close the Configuration Tool and create the server. For more information, see Creating the Attribute server on page 181.	Attribute_web

Field	Description	Sample entry
ICM Service	Configures the ICM server and related components on the target machine. For more information, see Configuring the ICM server on page 211.	Checkmark in box
CIRS Service	Configures the CIRS server and related components on the target machine. For more information, see Configuring the Central Internet Routing service on page 213. **Important:** Only configure a CIRS server if your Avaya IC system includes more than one ICM server.	Checkmark in box
Attribute - DataWake recording (PDM)	Configures the DataWake recording feature of the Attribute server.	Checkmark in box
IC Login	Use the website account that you imported into the database with the seed data. If you have not already done so, change the default password for this account. For more information, see *IC Administration Volume 2: Agents, Customers, & Queues*. **Note:** Do not use the Administrator account for IC Manager or any other account for which the password may change.	website
IC Password	The password used by the IC Login.	website
IC Data Source	The Interaction Center data source that you create with the Interaction Center application for the CallCenterQ database. For more information, see Generating the Interaction Center application on page 84.	interaction_center
Repository Data Source	The Repository data source that you create with the repository application for the IC Repository database. For more information, see Generating the Interaction Center application on page 84.	repository
Database Login	Type a DBA login ID for the database server. **Note:** Do not use the DBA login for a database client on a DB2 database.	*Oracle*: sys
Database Password	The password for the DBA login ID.	admin
Database Host	The host name of the machine that hosts your database server.	testbox.xyzcorp.com

Field	Description	Sample entry
Oracle SID	The Oracle SID of your database. **Note:** The Oracle SID field is case-sensitive.	icutf8db

8. Select **Apply Settings**.
9. Select **OK** in the **Success** dialog box.
10. Select **Exit**.
11. To complete the configuration, perform the following steps to ensure that all Web Management services start properly:
    a. In the Sun ONE Server installation directory:
    - Open the https-admserv directory.
    - If the directory includes a file called start-ICEnv.backup, execute the following command to rename the file:

      ```
      mv start-ICEnv.backup oldstart-ICEnv
      ```

    b. Start the Sun ONE server that hosts the Website application, as described in Starting and stopping Sun ONE Server Web server on page 130
    c. Navigate to the *IC_INSTALL_DIR*/IC71/bin directory and use the following script to start Tomcat:

    ```
    nohup ./ictomcat.sh start website
    ```

Important:
For Solaris and AIX only, the Configuration Tool changes the ownership of the implementation file (vesp.imp) and the interface file (vespidl.pk) to root. If you do not want to run Avaya IC as root, you must change the ownership of these files as described in Changing ownership for Avaya IC - Solaris and AIX only on page 38.

Configuring Web Management services on AIX

Use these instructions if you plan to host Web Management services on an AIX machine.

Important:
To configure Web Management services on AIX, log in as a user with write permissions on the Web server directories and the Avaya IC installation directories. The root user usually has these write permissions.

To configure Web Management services to run on an AIX machine:

1. Stop the IBM HTTP Server that hosts the Website application, as described in Starting and stopping IBM http Web server on page 130.
2. If the Configuration Tool is already open, close it to ensure that the Configuration Tool includes all system changes, such as new servers.
3. Start the Configuration Tool:
   a. Navigate to `IC_INSTALL_DIR/IC71/bin`
   b. Run **`./configure`**
4. Log in with your IC Manager login ID and password.
5. Select the **Web** tab.
6. Complete the general fields in the following table.

Field	Description	Sample entry
JDK Home	The path to the directory where the Java SDK is installed. For more information about the Java SDK, see *IC Installation Planning and Prerequisites*.	`/usr/java142`
Tomcat Base Port	The port used to configure the following ports: • Tomcat HTTP ports for Web applications • Tomcat AJP (Web server connector) ports	Default: 9600
Web Server Home	The installation path for the IBM HTTP server instance that hosts the Web application.	`/usr/HTTPServer`
Web Server Host	The name of the machine that hosts the Web server. Do not include the DNS domain.	testbox

Field	Description	Sample entry
DNS Domain	The network (DNS) domain of the machine that hosts your Web server. Do not enter an Avaya IC domain. **Note:** Verify the default DNS domain carefully to ensure that it is correct.	xyzcorp.com
Web Server Port	The port that your Web server uses for communication. Make sure that the port matches the protocol used by your Web server for communication. The default ports are: ● HTTP port is 80. ● HTTPS port is 443. Do not change the default port unless you assign a different port to the Web server.	Default: 80
IC Test	Optional. IC Test is a Web application that you can use to test your Tomcat configuration. If you install multiple versions of Tomcat, the Configuration Tool creates an IC Test application on each version of Tomcat. The Configuration Tool also creates a separate Tomcat server to host IC Test. To access IC Test, use the Tomcat HTTP port in the URL. For example, type: http://<*server*>.<*domain*>.com:9606/ictest **Note:** The port number is not required if you install a single version of Tomcat, or access IC Test from the separate Tomcat server for IC Test.	Checkmark in box

7. Complete the Web Management fields in the following table.

Field	Description	Sample entry
Configure Web Management	Check this box if you want to configure Web Management services on the target machine. After you check this box, the Configuration Tool automatically: ● Displays the other Web Management fields ● Checks the following boxes: – Website – ICM – CIRS – Attribute - DataWake recording (PDM)	Checkmark in box
Website	Creates the Website Web application and performs other tasks that are required to configure a Web Management Website on the target machine. After you check this box, the Configuration Tool displays the following required fields for the Website: ● Website Virtual Directory Name ● WebACD ● Attribute Server	Checkmark in box
Website Virtual Directory Name	The name of the virtual directory for the Website.	website
WebACD	The WebACD server in your Avaya IC system. You must create the WebACD server before the Configuration Tool can include the server in the drop-down list. If the list does not include the server, close the Configuration Tool and create the server. For more information, see Creating the WebACD server on page 177.	WebACD_web
Attribute Server	The Attribute server that the DataWake plug-in uses. You must create the Attribute server before the Configuration Tool can include the server in the drop-down list. If the list does not include the server, close the Configuration Tool and create the server. For more information, see Creating the Attribute server on page 181.	Attribute_web

Field	Description	Sample entry
ICM Service	Configures the ICM server and related components on the target machine. For more information, see Configuring the ICM server on page 211.	Checkmark in box
CIRS Service	Configures the CIRS server and related components on the target machine. For more information, see Configuring the Central Internet Routing service on page 213. **Important:** Only configure a CIRS server if your Avaya IC system includes more than one ICM server.	Checkmark in box
Attribute - DataWake recording (PDM)	Configures the DataWake recording feature of the Attribute server.	Checkmark in box
IC Login	Use the website account that you imported into the database with the seed data. If you have not already done so, change the default password for this account. For more information, see *IC Administration Volume 2: Agents, Customers, & Queues*. **Note:** Do not use the Administrator account for IC Manager or any other account for which the password may change.	website
IC Password	The password used by the IC Login.	website
IC Data Source	The Interaction Center data source that you create with the Interaction Center application for the CallCenterQ database. For more information, see Generating the Interaction Center application on page 84.	interaction_center
Repository Data Source	The Repository data source that you create with the repository application for the IC Repository database. For more information, see Generating the IC Repository application on page 73.	repository
Database Login	Type a DBA login ID for the database server. **Note:** Do not use the DBA login for a database client on a DB2 database.	*DB2*: db2inst1
Database Password	The password for the DBA login ID.	admin

Field	Description	Sample entry
Database Host	The host name of the machine that hosts your database server.	testbox.xyzcorp.com
DB2 Port	The port that the target machine uses to communicate with the DB2 database.	Default: 50,000

8. Select **Apply Settings**.
9. Select **OK** in the **Success** dialog box.
10. Select **Exit**.
11. To complete the configuration, perform the following steps to ensure that all Web Management services start properly:
    a. Start the IBM HTTP Server that hosts the Website application, as described in Starting and stopping IBM http Web server on page 130.
    b. Navigate to the *IC_INSTALL_DIR*/IC71/bin directory.
    c. Use the following script to start Tomcat:

```
nohup ./ictomcat.sh start website
```

Important:
For Solaris and AIX only, the Configuration Tool changes the ownership of the implementation file (vesp.imp) and the interface file (vespidl.pk) to root. If you do not want to run Avaya IC as root, you must change the ownership of these files as described in Changing ownership for Avaya IC - Solaris and AIX only on page 38.

Integrating Web Management Administration

Web Management Administration is a set of Web pages that you use to administer and configure Web Management and Email Management. You open Web Management Administration from IC Manager. Before you use Web Management Administration, you must integrate it with IC Manager.

Note:
Complete only those properties listed in this section to integrate Web Management administration. You do not need to complete the other properties available in the System/Configuration list.

This section includes the following topics:

Integrating Web Management Administration with IC Manager

To integrate Web Management Administration with IC Manager:

1. In IC Manager, select **Tools** > **Groups**.
2. Select the **Properties** tab.
3. Select the **IC** node in the left pane.
4. In the **Sections** list, select **System/Configuration**.
5. Double-click the **Value** column next to ChatLoginServer in the list of properties and complete the following fields:
   a. In the **Property Value** field, type the fully-qualified domain name of the machine that hosts the Tomcat server for the Web Management Administration Website. For example, type support.xyzcorp.com.
   b. Select **OK**.
6. Double-click the **Value** column next to ChatLoginServerWebsite in the list of properties and complete the following fields:
   a. Type the name of the Tomcat web application for the Web Management Administration Website.

      This is the name that you specified when you configured the website Tomcat application in Configuring Web Management services on page 186. The Web Management Administration Website must be on the machine that you specified for the ChatLoginServer property.
   b. Select **OK**.
7. If you serve your Web Management Administration pages from a secure web server, you must also modify the properties shown in the following table:

Property	Recommended entry	Notes
ChatLoginServerProtocol	Type the protocol that your Web server uses.	For secure server protocol, type **https**. For non-secure server protocol, type **http**.
ChatLoginServerPort	Type the following ports: • HTTP - 80 • HTTPS - 443	Do not change the default port.

8. Select **OK**.
9. Exit and restart IC Manager.

Setting the ServerName property - AIX only

The default installation of the IBM http server does not include the fully qualified domain name for the `ServerName` property in the `httpd.conf` file. If this property is incorrect, the Web Management Administration pages can loop indefinitely on the opening page.

To set the ServerName property:

1. In a text editor, open the `.../HTTPServer/conf/httpd.conf` file.
2. Search for the `ServerName` entry and ensure that the value includes the fully qualified domain name of the server.
3. Save the file.
4. Restart the IBM http server, as described in Starting and stopping IBM http Web server on page 130.

Configuring a Workflow server for Web Management

To configure the Workflow server for Web Management, perform the steps in the following topics:

1. Creating a Workflow server for Web Management on page 204.
2. Creating the chat channel for the Workflow server on page 205.

If your Avaya IC system includes multiple Workflow servers, perform these steps on each Workflow server that processes chat contacts.

Creating a Workflow server for Web Management

These instructions only provide information about those parameters you need to set when you create a Workflow server to handle chat contacts. For more information about other parameters in the Workflow server, see Configuring multiple Workflow servers on page 109 and *IC Administration Volume 1: Servers & Domains*.

CAUTION:
If you do not configure the Workflow server with synchronous startup flows, the Qualify Chat workflow cannot resolve the pkey of the queue where a contact is to be routed. If this occurs, Avaya IC cannot route chat contacts.

To create a Workflow server for Web Management:

1. In IC Manager, select **Server** > **New**.
2. Select **Workflow** from the list of servers.
3. Select **OK**.
4. Select the **General** tab, and complete the fields shown in the following table.

Field	Recommended entry	Notes
Name	Workflow_<*domain*>	Include the domain in the server name to identify the server.
Domain	Select the Avaya IC domain for the server from the drop-down list.	For example, select `Web` to use the preconfigured domain for Web Management.
Host	Select the machine's IP address from the drop-down list, or type the IP address if it is not in the list.	When you select the host, IC Manager fills in the fields for Directory, Port, and Executable.

5. Select the **Workflow** tab.
6. From the **IC Data Source** drop-down list, select the Interaction Center data source.

   The default name for this data source is interaction_center. This is the data source that you created in Generating the Interaction Center application on page 84.
7. Select **Synchronous Startup Flows.**
8. If the following rows do not exist, add them to the Synchronous Startup Flows:
   a. Select **New**.
   b. In the new row, type **`web_routing.update_qw_cache`**
   c. Select **OK**.
9. Continue with Creating the chat channel for the Workflow server on page 205.

Creating the chat channel for the Workflow server

To create the chat channel for the Workflow server:

1. In the Server Editor for the Workflow server, select the **Channels** tab.
2. Select the **Channels** tab.
3. Select **New Channel**.
4. In the **Channel Editor** dialog box:
   a. Complete the fields as shown in the following table.

Field	Recommended entry	Notes
Global	Do not check this field.	Do not check this field to create a create a channel for a specific server or media, such as Chat.
By Server	• Do not check this field if you want this channel to handle events from all servers of the type that you select from the **Service** drop-down list. • Check this field if you want this channel to handle events from only one specific server that you select from the **Service** drop-down list.	If you check this field, and you need this Workflow server to communicate with more than one server, you must create another channel for that server. **Warning:** If you check this field and the WebACD server is named "WACD", the Workflow server will not be able to communicate with the WebACD server.
Channel Range	No entry necessary.	Completed by IC Manager
Service	Select **WACD** or the WebACD server from the drop-down list.	Whether you can select a server or a type of server, depends up whether or not you checked the **By Server** field.
Criteria	Type **media=chat**	

   b. Select **OK**.
5. Select the channel that you created in the step above.
6. Select **New Association**.

7. In the **Channel Association** dialog box, complete the fields as shown in the following table. Select **OK**.

Field	Recommended entry
Channel Range	Completed by IC Manager
Service Range	Completed by IC Manager
Event	WACD.QualifyChat **Note:** This field is case-sensitive and must follow the format `<flow_project>.<flow_name>`
Flow	`<flow_project>.<flow_name>` For example, to use the sample workflow, type `wacd.qualifychat`

8. Select **OK**.
9. In the **Server** tab of IC Manager, select the Workflow server that handles chat contacts.
10. Right-click the Workflow server and select **Start**.

Using workflows for Web Management

You can use the sample workflows to configure and test your Web Management servers. When you move into production, modify the sample workflows to meet your system needs and configuration. For more information, see *Avaya IC Media Workflow Reference*.

Note:
If you add a queue to route chat contacts, you must re-run the update_qw_cache workflow in the Web_Routing project. If you do not want to stop and start the Workflow server that processes chat contacts, select **Run Flows** on the General tab of the Workflow server.

This section includes the following topics:

Workflows required by Web Management

Web Management requires the following sample and system workflows:

- Qualify Chat workflow in the WACD project
- All workflows in the WebRouting project
- All workflows in the WebCenter project

The Avaya IC seed data includes compiled sample workflows for these projects. When you created the CCQ database, you imported the compiled workflows with the seed data and stored them in the database.

For a complete list of the workflows in these projects, including the directories where Avaya IC installs the workflows, see *Avaya Workflow Designer User Guide*.

Important:
Make sure that no workflows use a formatted telephone number to look up customer records. For example, confirm that your Qualify Chat workflow does not use a formatted telephone number in the Customer Lookup block.

Reloading the customer management workflows

The customer management workflows in the WebCenter project require file-based IC Scripts. By default, the `include` property contains the names of the required file-based IC Scripts.

Before you compile the workflows in the WebCenter project, add the following IC Script directory to the project:

IC_INSTALL_DIR\IC71\design\IC\Flows\Avaya\WebCenter

To add the IC Script directory:

1. With the project open in Workflow Designer, select **Project** > **Settings**.
2. In the **Directories** tab of the **Project Settings** dialog box, select **New Folder**.
3. In the **Open** dialog box:
   a. Navigate to the following IC Script folder:

      IC_INSTALL_DIR\IC71\design\IC\Flows\Avaya\WebCenter

   b. Select **OK** to add the IC Script folder to the **Directories** tab.
4. If you have not already done so, in the **Project Settings** dialog box:
   a. Select the **Database** tab.
   b. Verify that the **IC Data Source** field includes the name of the Interaction Center data source.

c. In the **Login Id** field, enter an administrative account for Avaya IC.

d. In the **Password** field, enter the password for the administrative account.

5. In the **Project Settings** dialog box, select **OK**.

   You can now compile and load the customer management workflows.

Configuring routing hints for the Qualify Chat workflow

The Fetch Routing Hints (chat) block in the Qualify Chat workflow uses the routing hints in the RoutingHint table of the Directory server to route incoming chat contacts. The following table shows the routing hints used in the sample Qualify Chat workflow.

Category	Sample routing hint values
language	This category requires ISO-639-1 values, such as: • en • sp • fr • de • zh
intent	• sales • support

To route chat contacts with the sample Qualify chat workflow, create these hints, then assign them to the default chat queue.

Important:
Routing hints must be in lower case. Do not use mixed upper and lower case in your routing hints. If the routing hint is not in all lower case, the workflow cannot locate the routing hint, and Avaya IC cannot correctly route the contact.

To configure routing hints, perform the steps in the following topics:

1. Creating routing hints on page 209.
2. Associating routing hints with Web Self-Service documents on page 210.

Creating routing hints

Use the Configuration tab of IC Manager to create routing hints and add them to the RoutingHint table. The Qualify Chat workflow uses hints from the RoutingHint table to route incoming chat contacts.

Each row in the routing hint table contains the following:

- A routing hint
- The IDs of the queues where contacts that match the routing hint should be routed

Tip:
The default chat queue is DefaultChatQueue@DefaultTenant. You can create and use additional chat queues for routing chat contacts. For more information, see *IC Administration Volume 2: Agents, Customers, & Queues*.

To create routing hints:

1. In IC Manager, select the **Configuration** tab.
2. In the left pane, select **Tables** > **Workflow** > **RoutingHint**.
3. Select **New**.
4. In the right pane, complete the fields shown in the following table.

Parameter	Recommended entry	Description
Routing Hint	Type a routing hint.	For the sample Qualify Chat workflow, enter a value for the language or intent category. For language, type a value such as: – en – sp – fr – de – zh For intent, type a value such as: – sales – support The routing hint must be a text string in all lower case. The text string cannot contain any special characters.

Parameter	Recommended entry	Description
Chat Queue ID	Type `DefaultChatQueue@DefaultTenant`.	DefaultChatQueue@DefaultTenant is the default chat queue. For more information about chat queues, see *IC Administration Volume 2: Agents, Customers, & Queues*.
Category/Qualifier	Leave this field blank.	Used only for routing hints for chat contacts in Business Advocate.
Tenant	Select `DefaultTenant` from the queue from the drop-down list.	Select the tenant used by the queue. For the DefaultChatQueue, select DefaultTenant to ensure that the routing hint uses the correct queue.

5. Select **OK**.

   Repeat Steps 3 through 6 to create the second routing hint.

6. Select **Manager** > **Refresh**.

Associating routing hints with Web Self-Service documents

After you add the routing hints to the Directory server tables, you can associate the routing hints with documents in the Web Self-Service database.

When a customer requests a chat contact with an agent, Web Management records the last document that the customer viewed on the Website. If that document has an associated routing hint, the Qualify Chat workflow uses that routing hint to determine the correct queue for the chat contact.

You need to create at least one document for that database to fully test the Qualify Chat workflow. For more information about the Web Self-Service database, see *IC Administration Volume 2: Agents, Customers, & Queues*.

To associate routing hints with Web Self-Service documents:

1. In IC Manager, select **Services** > **Web Response Unit**.
2. In the left frame, select **Web Self-Service Console**.
3. In the Web Self-Service Console page:
   a. Select a tenant from the drop-down list.
   b. In the left frame, select **Manage FAQ**.
4. In the Manage FAQ page:
   a. Select the document in the list of documents.
   b. Select **Update**.

5. In the document, scroll down to the **Routing Attributes** section.
6. Select one routing hint from the **Routing Hint** drop-down lists.
7. Select **Update**.

Configuring the ICM server

The ICM server is a service that hosts text conferencing for Web Management. The ICM server does not run in IC Manager. For information about how to stop and restart the ICM server, see Starting and stopping Avaya IC services on page 127.

> **Important:**
> The steps in *Configuring the ICM server* are optional. Do not perform these steps if the ICM server requires only the default functionality. For example, perform these steps if you want to increase the logging level from the default logging level of "1".

Do not enter a value or change the default values in the fields available through **Advanced Properties** unless a property needs to be explicitly changed from the default value calculated by the ICM server during its initialization. Most Avaya IC systems do not require setting any of the advanced properties. For more information about the advanced properties, see *IC Administration Volume 1: Servers & Domains*.

To configure the ICM Server:

1. In IC Manager, select the **Configuration** tab.
2. From the **Tables** list in left pane, select **Chat** > **ICM**.
3. Select **New**.
4. In the right pane, type a name for the ICM server in the **Global ICM Name** field.

   If your Avaya IC system includes multiple ICM servers, type a name that allows you to easily identify the ICM server. For example, for an ICM server on the TESTBOX machine, type **`icm_TESTBOX`**.

   > **Important:**
   > The ICM server name is case-sensitive.

   The ICM server uses the global name to determine which ICM record to read for configuration. The global name in this field must match the **`dsObject`** parameter in the following file on the machine that hosts the ICM server:
   `IC_INSTALL_DIR/IC71/etc/systemParms.txt`

5. In the right pane, review the fields as shown in the following table.

Note:
Do not enter a value or change a default value in these fields unless a property needs to be explicitly changed from the default value calculated by the ICM server during initialization. Most Avaya IC systems do not require changing any of these fields.

Parameter	Description
ICM Active	External clients use this parameter to determine which ICMs to use.
ICM Server Name	The fully-qualified domain name of the machine that hosts this ICM server.
SMTP Host	The fully-qualified domain name of the machine that hosts the SMTP server. For example, **`SMTPSVR.xyzcorp.com`**.
Chat Transcript Directory	The directory where Avaya IC stores the chat transcripts. The default directory is *`IC_INSTALL_DIR`*`\IC71\comp\icm\transcript`
Style Sheet Directory	The directory where Avaya IC stores the style sheets used to format emails that include chat transcripts. If you use the default installation directory, IC Manager automatically enters the following directory: `../comp/icm/transcriptxsl`
CIRS Host	The name of the machine that hosts the CIRS server used for load balancing.
ICM Property Management Debug Level	A number from 0 to 4 that represents the debug level for ICM components. Level 0 provides no debugging information in the logs, and level 4 provides full debugging information.
ICM Toolkit Debug Level	A number from 0 to 4 that represents the debug level for ICM toolkit components. Level 0 provides no debugging information in the logs, and level 4 provides full debugging information.
ICM Debug Level	A number from 0 to 4 that represents the debug level for the ICM server. Level 0 provides no debugging information in the logs, and level 4 provides full debugging information.

6. Select **OK**.
7. Restart the ICM server.

Configuring the Central Internet Routing service

If your Avaya IC system includes multiple ICM servers, you must configure a Central Internet Routing service (CIRS server) to balance the load between the ICM servers. Repeat the following steps for each CIRS server in your Avaya IC system.

The CIRS server does not run in IC Manager. For information about how to stop and restart the CIRS server, see Starting and stopping Avaya IC services on page 127.

> **Important:**
> The steps in *Configuring the Central Internet Routing service* are optional. Do not perform these steps if the CIRS server requires only the default functionality. For example, perform these steps if you want to increase the logging level from the default logging level of "1".

Do not enter a value or change the default values in the fields available through **Advanced Properties** unless a property needs to be explicitly changed from the default value calculated by the CIRS server during its initialization. Most Avaya IC systems do not require setting any of the advanced properties. For more information about the advanced properties, see *IC Administration Volume 1: Servers & Domains*.

To configure the CIRS server:

1. In IC Manager, select the **Configuration** tab.
2. From the **Tables** list in left pane, select **Chat** > **CIRS**.
3. Select **New**.
4. In the right pane, type a name for the CIRS server in the **Global CIRS Name** field.

   The CIRS server name is case-sensitive.

   If your Avaya IC system includes multiple CIRS servers, type a name that allows you to easily identify this CIRS server. For example, for a CIRS server on the TESTBOX machine, type **`cirs_TESTBOX`**.

   The CIRS server uses the global name to determine which CIRS record to read for configuration. The global name in this field must match the **`dsObjectName`** parameter in the following file on the machine that hosts the CIRS server:
   `IC_INSTALL_DIR``/IC71/etc/cirsSystemParms.txt`

5. In the right pane, review the fields as shown in the following table.

Note:
Do not enter a value or change the default values in these fields unless a property needs to be explicitly changed from the default value calculated by the CIRS server during its initialization. Most Avaya IC systems do not require changing any of these fields.

Parameter	Description
CIRS Active	External clients use this parameter to determine which ICMs to use. This box must be checked for the CIRS server to function.
IC Site	Automatically lists all sites in your Avaya IC system. This field contains the site where this CIRS server is located.

6. Select **OK**.
7. Restart the CIRS server.

Configuring the Website

Before you configure the website, create the website application in the Configuration Tool. For more information, see Configuring Web Management services on page 186.

If you are configuring a localized version, you can specify a supported language for the Website. For more information, see Configuring the Website for supported languages on page 392.

Important:
The steps in *Configuring the Website* are optional. Do not perform these steps if the Website requires only the default functionality. For example, perform these steps to create a separate administration Website and to disable access to the administration pages on the customer Website.

Do not enter a value or change the default values in the fields available through **Advanced Properties** unless a property needs to be explicitly changed from the default value calculated by the Website during its initialization. Most Avaya IC systems do not require setting any of the advanced properties. For more information about the advanced properties, see *IC Administration Volume 1: Servers & Domains*.

To configure the Website:

1. In IC Manager, select the **Configuration** tab.
2. From the **Tables** list in the left pane, select **Website** > **Website Context**.

3. Select **New**.
4. In the right pane, type a name for the Website in the **Global Name** field.

   The Website name is case-sensitive.

   Type a name that allows you to easily identify the Website. For example, for a Website on the TESTBOX machine, type **`website_TESTBOX`**.

   The Website uses this parameter to determine which website context record to read. This value must match the **`dsObject`** parameter in the following file on the machine that hosts the Website:
   `IC_INSTALL_DIR``\IC71\comp\website\WEB-INF\web.xml`
5. In the right pane, review the fields as shown in the following table.

Note:
Do not enter a value or change the default values in these fields unless a property needs to be explicitly changed from the default value calculated by the Website during its initialization. Most Avaya IC systems do not require changing any of these fields.

Parameter	Description
Context Active	External clients use this parameter to determine which website context to use. This box must be checked for the Website to function.
CIRS Name	This is the CIRS server to which the ICM CIRS servlet connects to perform load-balancing for chat contacts.
Website Debug Level	A number from 0 to 4 that represents the debug level for the website. Level 0 provides no debugging information in the logs, and level 4 provides full debugging information.
Default hostname for context	The name of the machine that hosts the Website. Used by external clients to determine the location of your customer-facing Website. If you enter a value in this field, Web Management uses this as the default ***`machine_name`*** in the URL for the customer-facing Website. If you leave this field blank, Web Management uses the value that you use in the URL when you access the customer-facing website for the first time. For example, if you use localhost in the URL the first time, the URL will be **`http://localhost/website/public`**.
IC Site	This property is not currently used.

Parameter	Description
Servlet context name	The name of your Website servlet. For example, **`website`**. This is the web application name in the Tomcat server. Used by external clients to determine website context name. This value is part of the URL used to access the customer-facing Website. For example, if you enter support for a customer support Website, the URL will be: **`http://<hostname>/support/public`**
Default internet protocol	Either HTTP or HTTPS protocol. Used by external clients to determine website protocol.
Default port for context	This is the HTTP connection port that the website uses. The defaults are: ● 80 for HTTP ● 443 for HTTPS

6. Select **OK**.
7. Restart the Tomcat server that hosts the Website, as shown in the following table:

Operating system	Step
Windows	From the Services Control Panel, restart the Tomcat server.
Solaris or AIX	Run the following command: **`nohup ./ictomcat.sh start`**

Configuring Avaya Full Text Search Engine

Avaya Full Text Search Engine (Avaya FTSE) is the full text search engine for Avaya IC. Avaya FTSE supports the Web Self-Service database, including the FAQs and Suggested Email Responses.

This section includes the following topics:

Configuring Avaya FTSE for Windows

This section includes the following topics:

Configuring full text searches for Microsoft Windows

You must configure full text searches on every machine that hosts one or more of the following:

- Customer Website
- Administrative Website
- WebACD server

To configure full text searches for Microsoft Windows:

1. Restart the Avaya IC Website service, as described in Starting and stopping services on Windows on page 128.
2. Open a DOS command prompt window.
3. In the command prompt window, navigate to the following directory: `IC_INSTALL_DIR\IC71\etc\wru_sql\`

4. Run the set up command for your database:

Database	Set up command
SQL Server	fulcrum_setup.cmd sqlserver <*ccq_database_username*> <*ccq_database_password*>
Oracle	fulcrum_setup.cmd oracle <*ccq_database_username*> <*ccq_database_password*>

After the set up command executes, continue with Step 5.

5. Check the `IC_INSTALL_DIR\IC71\etc\wru_sql\wru_createview.err` file for errors.

   If the file is not present or is empty, the set up command executed correctly. Some messages that you might see in the error file do not indicate a problem. For more information, see Full text search configuration error messages on page 422.

6. Check the `IC_INSTALL_DIR\IC71\etc\wru_sql\fulcrum.err` file for errors.

   If the file is empty, the set up command executed correctly. Some messages that you might see in the error file do not indicate a problem. For more information, see Full text search configuration error messages on page 422. Correct these errors as indicated in the message and as required by the database, then re-run the set up command.

Updating the full text indices on Microsoft Windows

If you host your customer Website and WebACD server on different machines, or if your Avaya IC configuration includes multiple Websites, you must update the full text indices on those machines. The update ensures that the indices on these machines include all documents that you have added to the index.

You can run the update command as needed or schedule them to run at regular intervals. If you schedule an update to run at regular intervals, do not run the update more frequently than once per hour.

You must run this update command on every machine that hosts one or more of the following:

- Customer-facing Website
- WebACD server

Important:
Do not run this update command on the machine that hosts the Administrative Website. That machine automatically updates its own index.

To update the full text indices:

1. Open a DOS command prompt window.
2. In the command prompt window, navigate to the following directory: `IC_INSTALL_DIR\IC71\etc\wru_sql`
3. Run the following update command: **`fulcrum_updatendx.cmd`**
4. Check the `IC_INSTALL_DIR\IC71\etc\wru_sql\fulcrum_updatendx.err` file for errors.

   If the file is empty, the set up command executed correctly. All messages in this file indicate errors. Correct these errors as indicated in the message and as required by the database, then re-run the set up command.
5. Restart the Avaya IC Website service, as described in Starting and stopping services on Windows on page 128.

   After you update the full text indices, you must restart the Avaya IC Website service to ensure that the drivers for the fulcrum search are loaded.

Configuring for Avaya FTSE for Sun Solaris and IBM AIX

This section includes the following topics:

Changing ownership for the full text search directory

Only the root user has read permissions for some of the files in the following directory: `IC_INSTALL_DIR/IC71/etc/wru_sql`

You must change the ownership for this directory if you plan to run the Avaya FTSE components as a non-root user on any machine that hosts a Website or the WebACD server.

To change ownership for the full text search directory:

1. Log in as root user.
2. Navigate to `IC_INSTALL_DIR/IC71/etc`
3. Execute the following command:

   `chown -R <userid> wru_sql`

   where <*userid*> represents the non-root user that you use to run the Avaya FTSE components.

Configuring full text searches on Sun Solaris and IBM AIX

You must configure full text searches on every machine that hosts one or more of the following:

- Customer Website
- Administrative Website
- WebACD server

To configure full text searches on Sun Solaris or IBM AIX:

1. If you defined the following environment variable in your shell, unset that environment variable.

Operating system	Environment variable
Sun Solaris	ORACLE_HOME
IBM AIX	DB2DIR

2. Navigate to the following directory: *IC_INSTALL_DIR*/IC71/etc/wru_sql
3. Run the following command to create the indices for full text searching:

   ./fulcrum_setup.sh <*ccq_database_username*> <*ccq_database_password*>

   When this command executes, you may see the following output:

Error message	Description
ERROR at line 1: ORA-00955: name is already used by an existing object	You can ignore this error. It indicates that the view already exists.
DB21034E The command was processed as an SQL statement because it was not a valid Command Line Processor command. During SQL processing it returned: SQL0601N The name of the object to be created is identical to the existing name "CCQ.WRU_VIEW" of type "VIEW". SQLSTATE=42710	You can ignore this error. This message indicates that the view already exists.

Error message	Description
"Error : 666"	This error indicates a problem in the odbc.ini file. This error results from the `bind18` command used to create bind packages for the ODBC drivers. Verify that the entries in the odbc.ini file for the `ccq` datasource are correct. Incorrect values in this file typically result from incorrect values entered in the Configuration Tool. Repeat the configuration of Web Self-Service.
execsql: execute failed SQLSTATE: SGS00, Native error: 0, error text [Hummingbird][SearchServer] Invalid table name	You may see this error message twice in fulcrum.err. This error occurs because the script is attempting to drop a table that does not yet exist. You can ignore this error when you run the `fulcrum_setup` command for the first time on a machine. However, if you receive this error when you repeat the command on a machine, investigate why the script cannot access the database to perform the following tasks: • unprotect table qw_wru_en • drop table qw_wru_en

4. Check the *IC_INSTALL_DIR*/IC71/etc/wru_sql/fulcrum.err file for errors.

   If the file is not present or is empty, the set up command executed correctly. Some messages that you might see in the error file do not indicate a problem. For more information, see Full text search configuration error messages on page 422.

5. Verify that the command did not create a file with a **DIL** extension in the *IC_INSTALL_DIR*/IC71/etc/wru_sql/ directory.

   If such a file exists, check the contents for errors. If it contains errors, check the contents of `fulcrum_odbctrace.out` to see what went wrong. If there were problems with the database connection, confirm that the entries in the `odbc.ini` file are correct and that you invoked `fulcrum_setup.sh` with a valid username and password.

6. For IBM AIX only: verify that the wru_createview.sql script contains the correct values for username, password, and database name for the DB2 database.

   The Configuration Tool substitutes these values when you configure the Website Web application. Incorrect values in this file typically result from incorrect values entered in the Configuration Tool. If the file includes errors, re-configure the Website. For more information, see Configuring Web Management services on page 186.

7. If necessary, after you correct all errors, re-run the `fulcrum_setup.sh` command.

Updating full text indices on Sun Solaris and IBM AIX

If you host your customer Website and WebACD server on different machines, or if your Avaya IC configuration includes multiple Websites, you must update the full text indices on those machines. The update ensures that the indices on these machines include all documents that you have added to the index.

You can run the update command as needed or schedule them to run at regular intervals. If you schedule an update to run at regular intervals, do not run the update more frequently than once per hour.

You must run this update command on every machine that hosts one or more of the following:

- Customer-facing Website
- WebACD server

Important:
Do not run this update command on the machine that hosts the Administrative Website. That machine automatically updates its own index.

To update the full text indices:

1. Navigate to the following directory: *IC_INSTALL_DIR*/IC71/etc/wru_sql
2. Run the following update command:

   ./fulcrum_updatendx.sh

3. Check the *IC_INSTALL_DIR*/IC71/etc/wru_sql/fulcrum_updatendx.err file for errors.

   If the file is empty, the set up command executed correctly. All messages in this file indicate errors. Correct these errors as indicated in the message and as required by the database, then re-run the set up command.

4. For AIX only, verify that:
   - The odbc.ini file lists the IP address of the DB2 machine not the hostname.
   - Each IP address listed in /etc/hosts has only one entry.
5. Restart the Avaya IC Website service, as described in Starting and stopping services on Sun Solaris and IBM AIX on page 129.

   After you update the full text indices, you must restart the Avaya IC Website service to ensure that the drivers for the fulcrum search are loaded.

Configuring Web Scheduled Callback

Web Scheduled Callback uses the components of the Avaya IC chat channel to route and report on Website customer requests for an agent callback.

Tip:
If you want an agent to handle Web Scheduled Callback contacts, you must configure the agent to handle voice and chat contacts.

To configure Web Scheduled Callback:

1. Cautions and tips for configuring Web Scheduled Callback on page 223
2. Creating a Web Scheduled Callback server on page 224
3. Configuring the Website for Web Scheduled Callback on page 225

Cautions and tips for configuring Web Scheduled Callback

This section includes some important cautions and tips that you need to consider when you install the software for Avaya Agent Web Client on the server.

This section includes the following topics:

- Supported agent desktop applications on page 223
- Time zone requirements for Web Scheduled Callback on page 223
- Calendar requirements for Web Scheduled Callback on page 224

Supported agent desktop applications

Avaya Agent is the only agent desktop application that supports Web Scheduled Callback. If an Avaya IC system includes Web Scheduled Callback, that system cannot include agents who work in Avaya Agent Web Client or a custom application developed with the Client SDK.

Time zone requirements for Web Scheduled Callback

Web Scheduled Callback is a time-bound feature. For Web Scheduled Callback to work correctly, all Avaya IC servers and the database must be in the same time zone.

Important:
If the time on the machines that host Avaya IC servers and the database is not synchronized, a time lag may occur between the scheduled time for the callback and the exact time that a Web Scheduled Callback request is delivered to an agent.

Calendar requirements for Web Scheduled Callback

Web Scheduled Callback requires the Gregorian calendar. Web Scheduled Callback does not work with any other calendar. For example, Web Scheduled Callback does not support the Thai B. E. (Buddhist Era) calendar or date format.

Creating a Web Scheduled Callback server

The Web Scheduled Callback server retrieves the scheduled call from the database and delivers the call to the agent as a Chat&Callback task.

To create a Web Scheduled Callback server:

1. Select **Server** > **New** in IC Manager.
2. Select **WSCallback** from the list of servers. Select **OK**.
3. Select the **General** tab and complete the fields in the following table.

Field	Recommended entry	Notes
Name	WSCallback_<*domain*>	Include the domain in the server name to identify the server.
Domain	Select the Avaya IC domain for the server from the drop-down list.	For example, select `Website` from the drop-down list.
Host	Enter or select the machine's IP address from the drop-down list.	When you select the host, IC Manager fills in Directory, Port, and Executable.

4. Select the **WSCallback** tab and complete the fields in the following table.

Field	Recommended entry	Notes
ICM Server Name	Enter the name of the machine where the ICM server is installed.	The Web Scheduled Callback contacts are sent to the ICM server that you specify here.
Call Timeout Interval (sec)	Enter the number of seconds after which the request times out if it is not routed to an agent.	Default is 120.
IC Login	Enter the IC Login username.	Default is dcobridge1
IC Password	Select the Ellipsis (…) and specify the password for the IC Login.	

5. Select **OK** to save your configuration settings.

Configuring the Website for Web Scheduled Callback

You can configure the working hours of a contact center with the tenant properties for the Website. The default values for these properties assume that the contact center will open at 09:00 and close 18:00.

To configure the Website for Web Scheduled Callback:

1. In IC Manager, select **Services** > **MultiTenancy Administration**.
2. Select **Tenant Properties** in the **Tenant Admin** menu.
3. Select the tenant you want to customize from the **Select a Tenant** drop-down list.
4. Select **Customize Tenant**.
5. In the **Customize Tenant** page, select the language properties you want to set from the **Select Language** drop-down list at the top of the page.
6. Click the **Callback** link.
7. Update the properties in the following table, and then select **Update Data**.

Property	Default value	Notes
callback.checkcallbacktime	TRUE	When set to TRUE, enables Web Scheduled Callback.
callback.contactcenteropentime	09:00	Use a 24-hour clock and xx.xx format only.
callback.contactcenterclosetime	18:00	Use a 24-hour clock and xx.xx format only.

Refreshing IC Manager

After you complete your Web Management configuration, refresh IC Manager and verify that the configuration information is present.

To refresh IC Manager:

1. In IC Manager, select **Manager** > **Refresh**.
2. In the **Success** message, select **OK**.

   If you do not see a Success message, see Troubleshooting the refresh in IC Manager on page 406.
3. If desired, verify that the information on the **Configuration** tab is correct.

Configuring SSL security for Web servers (optional)

You can configure Web Management and Email Management to work with Secure Sockets Layer (SSL) to provide secure Internet sessions. SSL is optional.

SSL connections require additional work for the Web servers, because they encrypt and decrypt all communications. Therefore, if your system includes SSL, install an ICM server on a machine dedicated to text conferencing. If desired, this ICM server can be a second ICM server. To install an additional ICM server, see Deploying multiple ICM servers (optional) on page 237.

If all tenants will be using SSL, you can host all Web Management servers on one machine, but should still host the ICM server on a dedicated machine.

To configure SSL, perform the steps in the following topics:

Prerequisites for configuring SSL

Before you configure Web Management or Email Management to use SSL, you must complete the following steps:

- Install and properly configure SSL. This step requires you to:
  a. Generate SSL authentication keys and a certificate request.
  b. Submit the certificate request to a certifying authority such as VeriSign, Thawte, or GTE CyberTrust.
  c. Import the signed certificate and configure the Web server to use the signed certificate returned by the certifying authority.
- If your Avaya IC system includes a second Web Management server for SSL, configure SSL on the secure server and the machine that hosts the ComHub server.
- Install, configure, and test one of the following on the secure server machine:
  – A full set of Web Management servers or Email Management servers
  – An additional ICM server

Modifying the Website configuration

You must modify the configuration of the website to use SSL values.

To modify the website configuration:

1. In IC Manager, select the **Configuration** tab.
2. From the **Tables** list in left pane, select **Website** > **Website Context**.
3. In the right pane, select the entry for the website and select **Edit**.
4. Update the values as shown in the following table:

Property	Recommended entry
Default internet protocol	Select **https** from the drop-down list
Default port for context	Type **443**.

5. Select **OK**.
6. Select **Manager** > **Refresh**.

Configuring the WebACD server

To configure the WebACD server:

1. In IC Manager, double-click the WebACD server in the lists of servers.
2. Select the **WACD** tab.
3. In the **WACD Webserver** field, update the values as shown in the following table:

Property	Recommended entry
Default internet protocol	Select **https** from the drop-down list
Default port for context	Type **443**.

4. Select **OK**.

Editing the configuration file

To edit the configuration file:

1. In Notepad or another text editor, open **`webadmin.cfg`**.
2. Change the value of the attribute **`serverPort`** to 443.
3. Add the new attribute-value pair shown in the following table:

Attribute	Value
protocol	https://

4. Save and close the file.

Modifying the SSL properties

To modify the SSL properties:

1. In IC Manager, select **Tools** > **Groups**.
2. Select the **Properties** tab.
3. Select **IC** in the left pane of the **Group Manager**.
4. Select **System/Configuration** in the Sections list.
5. Select the following properties.
6. Select **Edit** and set values for the properties, as shown in the following table:

Property	Recommended entry
ChatLoginServerProtocol	Type **https**.
ChatLoginServerPort	Type **443**.

7. Select **OK**.

Configuring SSL for specific tenants

The values that you set in the previous steps become the default values for all tenants. All tenants are not configured for SSL by default. You can override this default behavior by setting a tenant specific property.

To set the website.pages.public property:

1. In IC Manager, select **Services** > **MultiTenancy Administration**.
2. Select **Tenant Properties** in the **Tenant Admin** menu.
3. Select the tenant you want to customize from the **Select a Tenant** drop-down list.
4. Select **Customize Tenant**.
5. In the **Customize Tenant** page, select the language properties you want to set from the **Select Language** drop-down list at the top of the page.
6. Select the website properties.
7. Change the **`website.pages.public`** property to an absolute URL with the protocol specified as http for non SSL and https for SSL.

   For example, type `https://mymachine.company.com/website/public`.
8. Select **Update Data** at the bottom of the page.

Modifying tenant properties for SSL

You must modify some tenant properties for SSL to function properly in your Website.

Tip:
This section describes the tenant properties that you typically need to modify. Some properties may not be required for all Avaya IC systems.

To modify the tenant properties for SSL:

1. In IC Manager, select **Services** > **MultiTenancy Administration**.
2. Select **Tenant Properties** in the **Tenant Admin** menu.
3. Select the tenant you want to customize from the **Select a Tenant** drop-down list.
4. Select **Customize Tenant**.
5. In the **Customize Tenant** page, select the language properties you want to set from the **Select Language** drop-down list at the top of the page.
6. If the customer Website uses SSL, do the following:
   a. Click the **wru** link.

b. Update the properties in the following table.

In the recommended entries, *server* is the fully-qualified domain name of the machine that hosts the customer Website.

Property	Recommended entry
wru.stylesheets.display	https://*server*/website/public/xsl/displayxsl
wru.stylesheets.displayparts	https://*server*/website/public/xsl/displaypartsxsl
wru.stylesheets.grouping	https://*server*/website/public/xsl/groupingxsl
wru.stylesheets.search	https://*server*/website/public/xsl/search.xsl

c. Select **Update Data**.

7. If the administration Website uses SSL, do the following:

a. Scroll to the top of the page and click the **wruadmin** link.

b. Update the properties in the following table.

In the recommended entries, *server* is the fully-qualified domain name of the machine that hosts the administration Website.

Property	Recommended entry
wruadmin.stylesheets. approve	https://*server*/website/admin/wru/xsl/edit.xsl
wruadmin.stylesheets. approvelist	https://*server*/website/admin/wru/xsl/ approvelist.xsl
wruadmin.stylesheets. display	https://*server*/website/website/admin/wru/xsl/ display.xsl
wruadmin.stylesheets. displayparts	https://*server*/website/admin/wru/xsl/ displayparts.xsl
wruadmin.stylesheets.edit	https://*server*/website/admin/wru/xsl/edit.xsl
wruadmin.stylesheets. grouping	https://*server*/website/admin/wru/xsl/ grouping.xsl
wruadmin.stylesheets. search	https://*server*/website/admin/wru/xsl/search.xsl
wruadmin.stylesheets. submit	https://*server*/website/admin/wru/xsl/edit.xsl

c. Select **Update Data**.

Setting up a separate administration Website (optional)

You can configure a web server to serve as an administration website only. The administration Website will not contain any accessible external or customer-facing content, and the chat functions will be disabled.

These instructions assume that you have already configured Web Management.

Note:
If your Avaya IC system includes multiple Attribute servers, all Websites and ICM servers must use the same Attribute server, so that their Tenant customization properties remain synchronized.

To set up a separate administration website, complete the steps in the following topics:

1. Creating the Web application for the administration website on page 231.
2. Configuring an administration Website on page 231.
3. Configuring the WebACD server on page 232.
4. Integrating the administration Website on page 233.

Creating the Web application for the administration website

Create the Web application for the administration website, as described in Configuring Web Management services on page 186.

Configuring an administration Website

Create a separate entry for the administration Website in IC Manager.

To configure the administration website:

1. In IC Manager, select the **Configuration** tab.
2. From the **Tables** list in left pane, select **Website** > **Website Context**.
3. Select **New**.
4. Right-click in the right pane, and check the box next to **Show Advanced Properties**.

5. Complete the fields in the right pane, as shown in the following table:

Field	Recommended entry
Global Name	Type a name for the website. For example, type AdminWebsite. **Note:** The Global Name is case-sensitive. The Global Name must match the `dsObject` parameter in the following file on the machine that hosts the administration Website: *IC_INSTALL_DIR*\IC71\comp\website\WEB-INF\web.xml
Context Active	Check this box.
Admin Pages Active	Check this box.
Public Pages Active	Do not check this box.
ICM Servlets Active	Do not check this box.

For more information about these fields, see Configuring the Website on page 214

6. Select **OK**.
7. Select **Manager** > **Refresh**.
8. Restart the Tomcat server that hosts the Administration website.

Configuring the WebACD server

The administration and customer Websites share the WACD Webserver property in the WebACD server. If you install separate administration and customer Websites, you must configure this property and create a new name-value pair in the WebACD server for Sametime to function correctly.

For information on how to set up Sametime, see *IC Administration Volume 2: Agents, Customers, & Queues*.

To configure the WebACD server for the administration website:

1. In IC Manager, double-click the WebACD server in the lists of servers.
2. Select the **WACD** tab.
3. In the **WACD Webserver** field, type the fully-qualified domain name of the machine that hosts the administration website.
4. Select **Apply**.
5. Select the **Configuration** tab.

6. Select **New**
7. In the **CTI Type Editor** dialog box:
   a. Complete the fields as shown in the following table:

Field	Recommended entry
CTI Type	Couple
Name	collaborationRootURL
Value	`http://<customer_webserver>/icm/aimagentcl.hta`

   These entries are case-sensitive.

   b. Select **OK**.
8. If your Web Management system includes the Sametime feature:
   a. Select **New**.
   b. In the **CTI Type Editor** dialog box, complete the fields as shown in the following table:

Field	Recommended entry
CTI Type	Couple
Name	sametimeurl
Value	URL of the "schedule a meeting" page on the sametime server.

   c. Select **OK**.

   You do not need to complete this step if your Web Management system does not include the Sametime feature.
9. Select **OK**.

Integrating the administration Website

To integrate the administration website:

1. In IC Manager, select **Tools** > **Groups**.
2. Select the **Properties** tab.
3. Select **IC** in the left pane of the **Group Manager**.
4. Select **System/Configuration** in the Sections list.

5. Select the following properties:
   a. Select **Edit**.
   b. Set values for the properties, as shown in the following table:

Property	Recommended entry
ChatLoginServer	Type the fully-qualified domain name of the machine that hosts the administration website.
ChatLoginServerWebsite	Type the servlet context name that you gave to this website in Configuring an administration Website on page 231.

Note:
If the columns in the right pane are Name, Entity, Value, and Overridable, select the **- (minus)** button on the toolbar to view and edit these properties.

6. Select **OK**.

Setting up a separate customer Website (optional)

You can configure a web server to serve as a customer Website only. The customer Website will not contain any accessible administration functions. These instructions assume that you have already configured Web Management.

Note:
If the Avaya IC system includes multiple Attribute servers, all Websites and ICM servers must use the same Attribute server, so that their Tenant customization properties remain synchronized.

To set up a separate customer Website, complete the steps in the following topics:

1. Creating the Web application for the customer Website on page 235.
2. Configuring the customer Website on page 235.
3. Configuring the WebACD server on page 236.

Creating the Web application for the customer Website

Create the Web application for the customer website, as described in Configuring Web Management services on page 186.

Configuring the customer Website

Create a separate entry for the customer website in IC Manager.

To configure the customer Website:

1. In IC Manager, select the **Configuration** tab.
2. From the **Tables** list in left pane, select **Website** > **Website Context**.
3. Select **New**.
4. Right-click in the right pane, and check the box next to **Show Advanced Properties**.
5. Complete the fields in the right pane, as shown in the following table:

Field	Recommended entry
Global Name	Type a name for the Website, for example, type CustomerWebsite.
Context Active	Check this box.
Admin Pages Active	Do not check this box.
Public Pages Active	Check this box.
ICM Servlets Active	Check this box.

   For more information about these fields, see Configuring the Website on page 214

6. Select **OK**.
7. Select **Manager** > **Refresh**.
8. Restart the Tomcat server that hosts the customer website.

Configuring the WebACD server

If you install separate administration and customer websites, you must configure this property and create a new name-value pair in the WebACD server for Collaboration and Sametime to function correctly. These entries are case-sensitive.

To configure the WebACD server for the customer website:

1. In IC Manager, double-click the WebACD server in the lists of servers.
2. Select the **Configuration** tab.
3. Select **New**.
4. In the **CTI Type Editor** dialog box:
   a. Complete the fields as shown in the following table:

Field	Recommended entry
CTI Type	Couple
Name	collaborationRootURL
Value	`http://<`*customer_webserver*`>/icm/aimagentcl.hta`

   These entries are case-sensitive.

   b. Select **OK**.
5. If your Web Management system includes the Sametime feature:
   a. Select **New**.
   b. In the **CTI Type Editor** dialog box, complete the fields as shown in the following table:

Field	Recommended entry
CTI Type	Couple
Name	sametimeurl
Value	URL of the "schedule a meeting" page on the sametime server.

   c. Select **OK**.

   You do not need to complete this step if your Web Management system does not include the Sametime feature.
6. Select **OK**.

Deploying multiple ICM servers (optional)

The ICM server hosts the Web Management conferences between agents and customers. You can deploy additional ICM servers, for one or both of the following reasons:

- To increase the capacity or load sharing of chat functionality.
- To use a secure server for chat escalations from one site but not another.

Tip:
The procedures in this section describe how to deploy one additional ICM server. To deploy more than one additional ICM servers, follow these instructions for each additional ICM server.

This section includes the following topics:

Deployment guidelines for an additional ICM server

The following guidelines describe the two ways that you can deploy an ICM server:

Deploying an additional ICM server with a CIRS server: With a CIRS server for load balancing. In this configuration, users enter the Website on the primary machine and are redirected to an ICM server on a different machine based on the load. For more information, see Configuring an additional ICM server with a CIRS server on page 239.

Deploying an additional ICM server without a CIRS server: Without a CIRS server. In this configuration, each combination of ICM server and Website is independent. For more information, see Configuring an independent additional ICM server.

Tip:
If you're setting up a secure ICM server, follow the instructions in the section Configuring SSL security for Web servers (optional) on page 226, as well as the instructions below.

Before you configure an additional ICM server

This section includes information that you need to know and steps you must perform before you configure an additional ICM server.

This section includes the following topics:

Location of an additional ICM server

Deploy an additional ICM server on a dedicated machine for scalability. Do not install the additional ICM server on the machine that hosts your database software.

Installing and configure prerequisites

Install and configure all prerequisites for a Website machine, including a database client. For more information, see *IC Installation Planning and Prerequisites*.

Installing the ICM server software

The software for the ICM server is included in the Avaya IC installer for Avaya IC servers. To install the ICM server software, follow the instructions in Installing Avaya IC server and administration components on page 29.

Setting the startup options for the secondary ORB server

If you do not plan to host other Avaya IC servers on the same machine as the additional ICM server, then the secondary ORB server does not need to be started. Set the startup options on the secondary ORB server to **Manual**.

If the machine also hosts an Avaya IC server, such as an Attribute server, the secondary ORB server must be started. Set the startup options for the secondary ORB server to **Automatic**.

For more information on how to set the startup options, see Starting and stopping the ORB server on page 123.

Configuring an additional ICM server with a CIRS server

To configure an additional ICM server to work with a CIRS server and the website, you must designate one machine that hosts an ICM server and Website combination as the primary ICM server machine.

After you determine which machine will be the primary ICM server machine, perform the steps in the following topics:

1. Configuring the primary ICM server on page 239.
2. Configuring the additional ICM server on page 240.
3. Configuring the CIRS server on page 240.
4. Configuring the CIRS servlet for Website on page 241.
5. Adding ICM servers to the ICM Bridge on page 243.

Configuring the primary ICM server

These instructions assume that you have already installed and configured the primary ICM server and the CIRS server.

To configure the primary ICM server:

1. In IC Manager, select the **Configuration** tab.
2. From the **Tables** list in left pane, select **Chat** > **ICM**.
3. Select the ICM table with the same name as the **`dsObjectName`** in *`IC_INSTALL_DIR`*`/IC71/etc/SystemParms.txt`

   If the table does not exist, create a new table. For more information, see Configuring the ICM server on page 211.
4. Update the fields in the right pane shown in the following table:

Property	Recommended entry
Global ICM Name	Type the value of **`dsObjectName`**.
ICM Server Name	Type the fully-qualified domain name of the machine that hosts the primary ICM server.
CIRS Host	Type the hostname of the machine that hosts the primary ICM server.
CIRS Port	Type the port for the CIRS server.

   For information on all other fields, see Configuring the ICM server on page 211.
5. Select **OK**.

6. Restart the ICM server
7. Start the CIRS server.
8. Add the ICM server to the ICM Bridge. For more information, see Adding ICM servers to the ICM Bridge on page 243.

Configuring the additional ICM server

To configure the additional ICM Server:

1. In IC Manager, select the **Configuration** tab.
2. From the **Tables** list in left pane, select **Chat** > **ICM**.
3. Select **New**.
4. Update the following fields in the right pane shown in the following table:

Property	Recommended entry
Global ICM Name	Type a name for the additional ICM server. For example, type **icm2**.
ICM Server Name	Type the fully-qualified domain name of the machine that hosts the additional ICM server.
CIRS Host	Type the hostname of the machine that hosts the primary ICM server.
CIRS Port	Type the port for the CIRS server.

For information on all other fields, see Configuring the ICM server on page 211.

5. Select **OK**.
6. Restart the ICM server
7. Start the CIRS server.
8. Add the ICM server to the ICM Bridge. For more information, see Adding ICM servers to the ICM Bridge on page 243.

Configuring the CIRS server

To configure the CIRS server:

1. In IC Manager, select the **Configuration** tab.
2. From the **Tables** list in left pane, select **Chat** > **CIRS**.

3. Select the CIRS table with the same name as the **dsObjectName** in *IC_INSTALL_DIR*/IC71/etc/cirsParms.txt

   If the table does not exist, create a new table. For more information, see Configuring the Central Internet Routing service on page 213.

4. In the **Global CIRS Name** field in the right pane, type the value of **dsObjectName** in *IC_INSTALL_DIR*/IC71/etc/cirsParms.txt

   For information on all other fields, see Configuring the Central Internet Routing service on page 213.

5. Select the **CIRS Active** box and place a checkmark in that box.

   This box must be checked for the CIRS server to function.

6. Select **OK**.
7. Start the CIRS server.

Configuring the CIRS servlet for Website

For more information about Website applications, see Configuring the Website on page 214.

To configure the CIRS servlet for website:

1. In IC Manager, select the **Configuration** tab.
2. From the **Tables** list in left pane, select **Website** > **Website Context**.
3. Create or update the websitecontext record for each Web Management application that chat users must access.
   a. Right-click in the right pane and check the box next to **Show Advanced Properties**.
   b. Complete the fields as shown in the following table:

Property	Recommended entry
Global Name	Type the value of dsObjectName in *IC_INSTALL_DIR*/IC71/comp/website/WEB-INF/web.xml.
ICM Servlets Active	Check this box.
ICM CIRS Servlet Active	Check this box.

   For information on all other fields, see Configuring the Central Internet Routing service on page 213.

4. Select **OK**.
5. Restart each server that hosts a Website application.
6. Start the ICM server.

Configuring an independent additional ICM server

After you designate one machine as the primary ICM server machine, perform the steps in the following topics:

1. Configuring an additional ICM server on page 242.
2. Disabling the CIRS servlet for Website on page 242.
3. Adding ICM servers to the ICM Bridge on page 243.

Configuring an additional ICM server

To configure an independent additional ICM server:

1. In IC Manager, select the **Configuration** tab.
2. From the **Tables** list in left pane, select **Chat** > **ICM**.
3. Select **New**.
4. Type a name for the additional ICM server in the **Global ICM Name** field.

   For information on all other fields, see Configuring the ICM server on page 211.
5. Select **OK**.
6. Restart the ICM server
7. Add the ICM server to the ICM Bridge. For more information, see Adding ICM servers to the ICM Bridge on page 243.

Disabling the CIRS servlet for Website

For more information about Website applications, see Configuring the Website on page 214.

To disable the CIRS servlet for website:

1. In IC Manager, select the **Configuration** tab.
2. From the **Tables** list in left pane, select **Website** > **Website Context**.
3. Create or update the websitecontext record for each Web Management application that chat users must access.
   a. Right-click in the right pane and check the box next to **Show Advanced Properties**.

b. Complete the fields as shown in the following table:

Property	Recommended entry
Global Name	Type the value of `dsObjectName` in *`IC_INSTALL_DIR`*`/IC71/comp/website/WEB-INF/web.xml`.
ICM CIRS Servlets Active	Do not check this box.

4. Select **OK**.
5. Restart each server that hosts a Website application.
6. Start the ICM server.

Adding ICM servers to the ICM Bridge

You add ICM servers to the ICM bridge in the Attribute server configuration. For more information, see Creating the WebACD server on page 177.

To add an additional ICM server to the ICM Bridge:

1. In IC Manager, double-click the Attribute server in the list of servers.
2. Select the **Attribute** tab.
3. Select the **Ellipsis** (**…**) next to the **ICM Servers** field.
4. In the **ICM Servers** dialog box:
   a. Select **New**.
   b. Check **Enabled**.
   c. In the Host field, type the name and domain of the machine that hosts the ICM server. For example, type TESTBOX.xyzcorp.com.
   d. Accept the default port number (8103) or change to an available port.
   e. Select **OK**.

   Repeat these steps for each ICM server in your Avaya IC system.
5. Select **OK**.
6. Restart the Attribute server.

Chapter 8: Configuring Email Management

Email Management is part of the email channel for Avaya Interaction Center (Avaya IC).

To configure Email Management, perform the steps in the following topics:

Your Avaya IC system can also include optional Email Management features, such an approval process or email message loop detection. For more information on how to configure these features, see *IC Administration Volume 1: Servers & Domains*.

Tip:
For information on how to set up RONA for Email Management, see *IC Administration Volume 2: Agents, Customers, & Queues*.

Before you configure Email Management

Before you configure Email Management, you must:

1. Verify that all required third party software, including SMTP servers, POP3 servers, and email accounts are installed and configured and accessible through the network. For more information, see *IC Installation Planning and Prerequisites*.
2. Copy the Avaya IC server files to the target machines, as described in Installing Avaya IC server and administration components on page 29.
3. Configure a secondary server environment, as described in Configuring the ORB server environment on page 33.
4. Perform all the steps to configure the Avaya IC servers, databases, and related components, described in Configuring core servers on page 99.
5. Configure Web Management, as set out in Configuring Web Management on page 175.

Configuring an IC Email server

The IC Email server interacts with SMTP and POP3 servers. This server also manages all polling and forwarding of emails into the Avaya IC system from customer to agent. Through workflows, this server also handles the filtering of spam, the delivery of automatic replies, and the management of traffic flow to external agents and approval agents.

This section includes the following topics:

Guidelines for an IC Email server

Ensure that the failover strategy for your Avaya IC domains includes the following:

- The domain that includes your IC Email server must failover to the domain that includes your WebACD server.
- The domain that includes your WebACD server must failover to the domain that includes your IC Email server.

Creating the IC Email server

The Avaya IC installation program does not automatically add this server. Email Management requires this server.

To create the IC Email server:

1. Select **Server** > **New** in IC Manager.
2. Select **Email** from the list of servers. Select **OK**.
3. Select the **General** tab and complete the fields in the following table.

Field	Recommended entry	Notes
Name	Email_<*domain*>	Include the domain in the server name to identify the server.
Domain	Select the Avaya IC domain for the server from the drop-down list.	For example, select `Email` from the drop-down list if the server is in the Email domain.
Host	Select the machine's IP address from the drop-down list, or enter the IP address if it is not in the list.	When you select the host, IC Manager fills in the fields for Directory, Port, and Executable.

4. Select the **ICEMail** tab and complete the fields in the following table.

Field	Recommended entry	Notes
IC Data Source	Select the Interaction Center Data Source.	If you used the default name, select `interaction_center`.
SMTP Server Name	Enter the name of the machine that hosts the SMTP server.	This is the server that Avaya IC uses for outbound email. For example, enter MailSrvExchange.
SMTP Helo Domain Name	Enter the domain of the machine that hosts the SMTP server.	For example, enter xyzcorp.com.
HTTP Timeout (sec)	*No recommended entry*	This field is no longer used by Avaya IC.

Field	Recommended entry	Notes
Duplicate Message Checking	Check this field, if desired.	Checks to make sure that duplicate messages are not received. Does not check outbound email contacts. An incoming email contact is considered to be a duplicate if all of the following parts of the contact are identical to those in a previous contact: ● From address ● To address ● Subject ● Body
Maximum Messages Retrieved per POP3 Cycle	240	Determines the maximum number of email contacts retrieved from a POP3 server over a single connection. The default entry assumes that the server takes approximately 1 second to download an email contact from the POP3 server. Thus, the server can process 240 contacts before the next polling cycle, 240 seconds later.
POP3 Cycle Wait Time (sec)	240	Specifies the default number of seconds that the server waits between checking for new contacts on a POP3 server. You can override this property per mail account. Increase this cycle if you expect to receive: ● Large email contacts that take longer to download, such as contacts with big attachments. ● A relatively low volume of email contacts to avoid an unnecessary drain on system and network resources. If you increase wait time, there will be a delay in when agents receive email contacts, since contacts are downloaded less frequently.

Field	Recommended entry	Notes
Detect Message Loops	Check this field, if desired.	If you are using workflows to analyze incoming emails, select this field to have the IC Email server set the `emailcount` field in the EDU. The Analyze flow can then be customized to look at `emailcount` and bypass the SmartAck block when the value is higher than the desired limit, thus preventing an autoresponse loop if both your system and your customer's system is set to respond to every email. If you are *not* using workflows to analyze your incoming emails, select this option to have the IC Email server stop sending acknowledgements to the same customer if the number of acknowledgements in a 24 hour period exceeds the value specified in **Message Loop Count**. 24 hours after the first acknowledgement is sent, the IC Email server resets the clock and starts sending acknowledgements to that customer again. **Tip:** If you want the customer to receive a different acknowledgement stating that a loop has been detected, create an email template for this purpose and specify its name in the **Loop Template Id** field.

Field	Recommended entry	Notes
Message Loop Count	Accept the default or change, if desired.	Email Management can be configured to acknowledge every email received from a customer. This field specifies the maximum number of acknowledgements that should be sent to a specific customer in any 24 hour period. The IC Email server starts counting when the first email acknowledgement is sent. It continues to count the number of acknowledgements sent until 24 hours have past, at which point it resets the count. If the **Message Loop Count** value is exceeded during that 24 hour period, the IC Email server stops sending further acknowledgements to that particular customer until the 24 hour period is over. For example, if you set this value to 5, Avaya IC returns the New Message template to the first five email contacts from the customer. The customer does not receive an acknowledgement for the sixth email contact unless you have specified an Autoresponse Loop Detection template in the **Loop Template Id** field.
Loop Detection Type	Select a number from the drop-down list.	Loop detection is based on "originator", "from address", "reply to address" or "both". You can select: ● 0 for Originator (first looks for Reply-To, if not set then looks for "from") ● 1 for "from" address ● 2 for "reply to" address ● 3 for Both
Loop Template Id	Select the Ellipsis (…) button and navigate to the template ID you want to use.	ID of the template used to send a final message to a customer after the message loop count is exceeded. Create this template in Email Template Administration.

Field	Recommended entry	Notes
Blank Message Template Id	Select the Ellipsis (…) button and navigate to the template ID you want to use.	Determines the ID of the template that is sent when a blank message (for example, and email with no body text) is received from a contact. Create this template in Email Template Administration.
Bounced Message Email Address	Enter an email address. For example, enter bounce@xyzcorp.com.	Determines the email address to which "bounce" messages are sent, including messages returned as undeliverable, bounced by Avaya IC workflows, or filtered out by your email filters. A supervisor or administrator should monitor this account using an external email client. **Important:** Make sure that the IC Email server does not poll this email address, or the server will retrieve all the bounce emails and enter them into the Avaya IC system.
Database Query Retries	Accept the default or change, if desired.	Determines the maximum number of times that the IC Email server will retry database queries if they fail. If this number of retries is exceeded, the IC Email server will shut itself down.
Store All Messages	Check this field, if desired.	Determines whether Email Management stores the message body of acknowledgements sent because of "New message template" configuration. If this option is set then all the bounce messages will also get stored in the database. Email Management stores these messages in the database, and agents can view them in the history browser. If you do not check this field, the agent can see that a message was sent, but cannot see the body of the message. **Note:** Email acknowledgements initiated by workflows are always stored in the database.
Validate Agent Reply	Do not check this field.	This field is no longer used.

Field	Recommended entry	Notes
Directory for Stored Messages	Enter a directory path.	The directory that the IC Email server should use to store messages larger than 1 MB in size. (The file path must be relative to the machine that hosts the IC Email server.) **Note:** If you do not specify a path, the files will be stored in `IC_INSTALL_DIR\IC71\MessageCenter\messages`.
Port for HTTP Requests	Accept the default of 19114.	Specifies the port on which the built-in HTTP server will listen. This is the port that is used if the specific server ports are not set. If this value is 0, the port defaults to the value set in the advanced property: HTTP Port for Admin Interface. If you must change this port, see *IC Installation Planning and Prerequisites* for a list of the default port numbers used by the other Avaya IC servers. Port conflicts can cause serious problems within the Avaya IC system.

5. Select the **Analysis** tab and complete the fields in the following table.

Field	Recommended entry	Notes
Run Analyze Flow	Check this field.	Check this field if you want: ● The IC Email server to invoke an email analysis workflow to assist in the routing of incoming email contacts. ● To use Analyze with Keywords or Content Analyzer to process incoming email. You must also complete all steps to configure Email workflows to use email analysis. For details, see Using workflows for Email Management on page 267 and the *Avaya IC Media Workflow Reference*.
Run Outbound Email Flow	For the initial installation of Avaya IC, clear this field.	Select this field if you want to: ● Have Avaya IC analyze outbound email. ● Have a supervisor approve outbound email. ● Use Analyze with Keywords or Content Analyzer to process outbound email. You must also complete all steps to configure Email workflows to use email analysis.

Even if you check the fields in the **Analysis** tab, email analysis will not work if you do not perform the steps in the following topics:

- Configuring a Workflow server for Email Management on page 261
- Using workflows for Email Management on page 267
- Creating routing hints for email workflows on page 269

6. Select **OK** to save your configuration settings.
7. Start the IC Email server:
   a. Select the IC Email server in the **Server** tab.
   b. Right-click on the IC Email server and select **Start**.

For more information about the correct order for starting and stopping Avaya IC servers, see Starting and stopping Avaya IC servers on page 120.

Configuring Email Template Administration

Email Template Administration requires a Web application. You configure Email Template Administration on the **Web** tab of the Avaya IC Configuration Tool.

This section describes how to install and configure Email Template Administration for each operating system that Avaya IC supports. This section includes the following topics:

Important:
The Configuration Tool overwrites all manual edits that you make to an Avaya IC configuration file.

Where to configure Email Template Administration

Configure Email Template Administration on the machine that hosts the templates for Email Management and the Web pages for Email Template Administration.

Hosting multiple Web applications on one machine

If the Avaya IC system includes more than one Web application on the same machine as the WebLM, Avaya recommends that you configure all of the Web applications on the target machine at the same time.

Important:
If you do not configure all of the Web applications simultaneously, leave the options for all Web applications on the target machine checked when you re-run the Configuration Tool to create the new Web applications. If you do not leave the options for the previously created Web applications checked, the Configuration Tool may delete those Web applications.

Advanced properties for Email Template Administration

The Web tab also includes advanced properties for the Java Virtual Machine.

Only configure the advanced properties if you expect a high volume of access to Email Template Administration. For more information, see Configuration Tool advanced properties on page 447.

Configuring Email Template Administration on Windows

Use these instructions if you plan to host Email Template Administration on a Windows machine.

You do not need to stop the IIS Web server on Windows machines.

To configure Email Template Administration to run on a Windows machine:

1. To start the Configuration Tool, select **Start** > **Programs** > **Avaya Interaction Center 7.1** > **Configuration Tool**.

   If the Configuration Tool is already open, close and re-open it to ensure that the Configuration Tool includes all system changes, such as new servers.
2. Log in with your IC Manager login ID and password.
3. Select the **Web** tab.
4. Complete the general fields in the following table.

Field	Description	Sample entry
JDK Home	The path to the directory where the Java SDK is installed. For more information about the Java SDK, see *IC Installation Planning and Prerequisites*.	`C:\j2sdk1.4.2_08`
Tomcat Base Port	The port used to configure the following ports: ● Tomcat HTTP ports for Web applications ● Tomcat AJP (Web server connector) ports	Default: 9600
IIS Website	The name of the IIS Web server that the Web application will use. **Tip:** For a localized version of IIS, type the localized name for the IIS Web server.	Default Web Site
Web Server Host	The name of the machine that hosts the Web server. Do not include the DNS domain.	testbox

Field	Description	Sample entry
DNS Domain	The network (DNS) domain of the machine that hosts your Web server. Do not enter an Avaya IC domain. **Note:** Verify the default DNS domain carefully to ensure that it is correct.	xyzcorp.com
Web Server Port	The port that your Web server uses for communication. Make sure that the port matches the protocol used by your Web server for communication. The default ports are: ● HTTP port is 80. ● HTTPS port is 443. Do not change the default port unless you assign a different port to the Web server.	Default: 80
IC Test	Optional. IC Test is a Web application that you can use to test your Tomcat configuration. If you install multiple versions of Tomcat, the Configuration Tool creates an IC Test application on each version of Tomcat. The Configuration Tool also creates a separate Tomcat server to host IC Test. To access IC Test, use the Tomcat HTTP port in the URL. For example, type: http://<*server*>.<*domain*>.com:9606/ictest **Note:** The port number is not required if you install a single version of Tomcat, or access IC Test from the separate Tomcat server for IC Test.	Checkmark in box

5. Check the **Configure Email Template Administration** box.
6. Select **Apply Settings**.
7. Select **OK** in the **Success** dialog box.
8. Select **Exit**.
9. To complete the configuration, perform the following steps to ensure that Email Template Administration services start properly:
   a. Open the Windows Services control panel.
   b. Start Avaya IC Email Template Management Service 7.1.

   For more information about how to start and stop Web application services, see Starting and stopping Avaya IC services on page 127.

Configuring Email Template Administration on Solaris

Use these instructions if you plan to host Email Template Administration on a Solaris machine.

Important:
To configure Email Template Administration on Solaris, you must log in as a user with write permissions on the Web server directories and the Avaya IC installation directories. The root user usually has these write permissions.

To configure Email Template Administration to run on a Solaris machine:

1. Stop the Sun ONE server that hosts the Website application, as described in Starting and stopping Sun ONE Server Web server on page 130.
2. If the Configuration Tool is already open, close it to ensure that the Configuration Tool includes all system changes, such as new servers.
3. Start the Configuration Tool:
   a. Navigate to `IC_INSTALL_DIR/IC71/bin`
   b. Run **`./configure`**
4. Log in with your IC Manager login ID and password.
5. Select the **Web** tab.
6. Complete the general fields in the following table.

Field	Description	Sample entry
JDK Home	The path to the directory where the Java SDK is installed. For more information about the Java SDK, see *IC Installation Planning and Prerequisites*.	`/opt/j2sdk1_4_2_08`
Tomcat Base Port	The port used to configure the following ports: ● Tomcat HTTP ports for Web applications ● Tomcat AJP (Web server connector) ports	Default: 9600
Web Server Home	The installation path for the Sun ONE™ Server that hosts the Web application.	`/opt/SUNWwbsvr`
Web Server Name	The root name of the server as found in the Sun ONE™ Server home directory. **Note:** Do not include `https-` in the Web server name.	testbox.xyzcorp.com
Web Server Host	The name of the machine that hosts the Web server. Do not include the DNS domain.	testbox

Field	Description	Sample entry
DNS Domain	The network (DNS) domain of the machine that hosts your Web server. Do not enter an Avaya IC domain. **Note:** Verify the default DNS domain carefully to ensure that it is correct.	xyzcorp.com
Web Server Port	The port that your Web server uses for communication. Make sure that the port matches the protocol used by your Web server for communication. The default ports are: ● HTTP port is 80. ● HTTPS port is 443. Do not change the default port unless you assign a different port to the Web server.	Default: 80
IC Test	Optional. IC Test is a Web application that you can use to test your Tomcat configuration. If you install multiple versions of Tomcat, the Configuration Tool creates an IC Test application on each version of Tomcat. The Configuration Tool also creates a separate Tomcat server to host IC Test. To access IC Test, use the Tomcat HTTP port in the URL. For example, type: http://<*server*>.<*domain*>.com:9606/ictest **Note:** The port number is not required if you install a single version of Tomcat, or access IC Test from the separate Tomcat server for IC Test.	Checkmark in box

7. Check the **Configure Email Template Administration** box.
8. Select **Apply Settings**.
9. Select **OK** in the **Success** dialog box.
10. Select **Exit**.
11. To complete the configuration, perform the following steps to ensure that all Email Template Administration services start properly:
    a. In the Sun ONE Server installation directory:
    - Open the https-admserv directory.
    - If the directory includes a file called start-ICEnv.backup, execute the following command to rename the file:

```
mv start-ICEnv.backup oldstart-ICEnv
```

b. Start the Sun ONE server that hosts the Website application, as described in Starting and stopping Sun ONE Server Web server on page 130

c. Navigate to the *IC_INSTALL_DIR*/IC71/bin directory.

d. Use the following script to start Tomcat:

```
nohup ./ictomcat.sh start rlmanager
```

Important:
For Solaris and AIX only, the Configuration Tool changes the ownership of the implementation file (vesp.imp) and the interface file (vespidl.pk) to root. If you do not want to run Avaya IC as root, you must change the ownership of these files as described in Changing ownership for Avaya IC - Solaris and AIX only on page 38.

Configuring Email Template Administration on AIX

Use these instructions if you plan to host Email Template Administration on an AIX machine.

Important:
To configure Email Template Administration on AIX, you must log in as a user with write permissions on the Web server directories and the Avaya IC installation directories. The root user usually has these write permissions.

To configure Email Template Administration to run on an AIX machine:

1. Stop the IBM HTTP Server that hosts the Website application with the stop script packaged with the Web server: **./httpserver.sh stop**
2. Start the Configuration Tool:
   a. Navigate to *IC_INSTALL_DIR*/IC71/bin
   b. Run **./configure**

   If the Configuration Tool is already open, close and re-open it to ensure that the Configuration Tool includes all system changes, such as new servers.
3. Log in with your IC Manager login ID and password.
4. Select the **Web** tab.
5. Complete the general fields in the following table.

Field	Description	Sample entry
JDK Home	The path to the directory where the Java SDK is installed. For more information about the Java SDK, see *IC Installation Planning and Prerequisites*.	/usr/java142

Field	Description	Sample entry
Tomcat Base Port	The port used to configure the following ports: ● Tomcat HTTP ports for Web applications ● Tomcat AJP (Web server connector) ports	Default: 9600
Web Server Home	The installation path for the IBM HTTP server instance that hosts the Web application.	`/usr/HTTPServer`
Web Server Host	The name of the machine that hosts the Web server. Do not include the DNS domain.	testbox
DNS Domain	The network (DNS) domain of the machine that hosts your Web server. Do not enter an Avaya IC domain. **Note:** Verify the default DNS domain carefully to ensure that it is correct.	xyzcorp.com
Web Server Port	The port that your Web server uses for communication. Make sure that the port matches the protocol used by your Web server for communication. The default ports are: ● HTTP port is 80. ● HTTPS port is 443. Do not change the default port unless you assign a different port to the Web server.	Default: 80
IC Test	Optional. IC Test is a Web application that you can use to test your Tomcat configuration. If you install multiple versions of Tomcat, the Configuration Tool creates an IC Test application on each version of Tomcat. The Configuration Tool also creates a separate Tomcat server to host IC Test. To access IC Test, use the Tomcat HTTP port in the URL. For example, type: http://<*server*>.<*domain*>.com:9606/ictest **Note:** The port number is not required if you install a single version of Tomcat, or access IC Test from the separate Tomcat server for IC Test.	Checkmark in box

6. Check the **Configure Email Template Administration** box.
7. Select **Apply Settings**.
8. Select **OK** in the **Success** dialog box.

9. Select **Exit**.
10. To complete the configuration, perform the following steps to ensure that all Email Template Administration services start properly:
    a. Start the IBM HTTP Server that hosts the Website application, as described in Starting and stopping IBM http Web server on page 130.
    b. Navigate to the *IC_INSTALL_DIR*/IC71/bin directory.
    c. Use the following script to start Tomcat:

    ```
    nohup ./ictomcat.sh start rlmanager
    ```

    Important:
    For Solaris and AIX only, the Configuration Tool changes the ownership of the implementation file (vesp.imp) and the interface file (vespidl.pk) to root. If you do not want to run Avaya IC as root, you must change the ownership of these files as described in Changing ownership for Avaya IC - Solaris and AIX only on page 38.

Configuring a Workflow server for Email Management

To configure the Workflow server for Email Management, perform the steps in the following topics:

1. Creating a Workflow server for Email Management on page 262.
2. Creating the email channels for the Workflow server on page 263.
3. Starting the Workflow server on page 267.

If your Avaya IC system includes multiple Workflow servers, perform these steps on each Workflow server that handles pre-qualification for email contacts and routes email contacts.

Creating a Workflow server for Email Management

These instructions only provide information about those parameters you need to set when you create a Workflow server to handle email contacts. For more information about other parameters in the Workflow server, see Configuring multiple Workflow servers on page 109 and *IC Administration Volume 1: Servers & Domains*.

CAUTION:
If you do not configure the Workflow server with synchronous startup flows, the Qualify Email workflow cannot resolve the pkey of the queue where a contact is to be routed. If this occurs, Avaya IC cannot route email contacts.

To create a Workflow server for Email Management:

1. In IC Manager, select **Server** > **New**.
2. Select **Workflow** from the list of servers.
3. Select **OK**.
4. Select the **General** tab, and complete the fields shown in the following table.

Field	Recommended entry	Notes
Name	Workflow_<*domain*>	Include the domain in the server name to identify the server.
Domain	Select the Avaya IC domain for the server from the drop-down list.	For example, select `Email` to use the preconfigured domain for Email Management.
Host	Select the machine's IP address from the drop-down list, or type the IP address if it is not in the list.	When you select the host, IC Manager fills in the fields for Directory, Port, and Executable.

5. Select the **Workflow** tab.
6. From the **IC Data Source** drop-down list, select the Interaction Center data source.

   The default name for this data source is interaction_center. This is the data source that you created in Generating the Interaction Center application on page 84.
7. Select **Synchronous Startup Flows.**
8. If the following rows do not exist, add them to the Synchronous Startup Flows:
   a. Select **New**.
   b. In the new row, type `web_routing.update_qw_cache`
   c. Select **OK**.
9. Continue with Creating the email channels for the Workflow server on page 263.

Creating the email channels for the Workflow server

You must add email channels and associations with the workflows for each channel. You create separate channels for email qualification and for email analysis. If the Avaya IC system uses different Workflow servers to handle each task, create these channels in the appropriate Workflow server.

This section includes the following topics:

- Creating the email channel for email qualification on page 263.
- Creating the email channel for email analysis on page 264.

Creating the email channel for email qualification

Perform these steps in each Workflow server that will run the Qualify Email workflow.

To create an email channel for a Workflow server that qualifies emails:

1. In the Server Editor for the Workflow server, select the **Channels** tab.
2. Select **New Channel**.
3. In the **Channel Editor** dialog box, complete the fields as shown in the following table.

Field	Recommended entry	Notes
Global	Do not check this field.	Do not check this field to create a create a channel for a specific server or media, such as Email.
By Server	• Do not check this field if you want this channel to handle events from all servers of the type that you select from the **Service** drop-down list. • Check this field if you want this channel to handle events from only one specific server that you select from the **Service** drop-down list.	If you check this field, and you need this Workflow server to communicate with more than one server, you must create another channel for that server. **Warning:** If you check this field and the WebACD server is named "WACD", the Workflow server will not be able to communicate with the WebACD server.
Channel Range	No entry necessary.	Completed by IC Manager
Service	Select **WACD** or the WebACD server from the drop-down list.	Whether you can select a server or a type of server, depends up whether or not you checked the **By Server** field.
Criteria	Type **media=email**	

4. Select **OK** in the **Channel Editor** dialog box.
5. Select the channel that you created in the step above.
6. Select **New Association**.
7. In the **Channel Association** dialog box, complete the fields as shown in the following table.

Field	Recommended entry
Channel Range	Completed by IC Manager
Service Interface	Completed by IC Manager
Event	WACD.QualifyEmail **Note:** This field is case-sensitive and must follow the format `<flow_project>.<flow_name>`
Flow	`<flow_project>.<flow_name>` For example, type `wacd.qualifyemail`

8. Select **OK** in the **Channel Association** dialog box.
9. Perform one of the following steps:
   - Select **OK** in the Server Editor to complete the Workflow server configuration.
   - If the Workflow server will also run email analysis workflows, continue with Creating the email channel for email analysis on page 264.

Creating the email channel for email analysis

Perform these steps in each Workflow server that will run the email analysis workflow.

To create an email channel for a Workflow server that analyzes emails:

1. In the Server Editor for the Workflow server, select the **Channels** tab.
2. Select **New Channel**.

3. In the **Channel Editor** dialog box, complete the fields as shown in the following table.

Field	Recommended entry	Notes
Global	Do not check this field.	Do not check this field to create a create a channel for a specific server or media, such as Email.
By Server	• Do not check this field if you want this channel to handle events from all servers of the type that you select from the **Service** drop-down list. • Check this field if you want this channel to handle events from only one specific server that you select from the **Service** drop-down list.	If you check this field, and you need this Workflow server to communicate with more than one server, you must create another channel for that server. **Warning:** If you check this field and the WebACD server is named "WACD", the Workflow server will not be able to communicate with the WebACD server.
Channel Range	No entry necessary.	Completed by IC Manager
Service	Select **ICEMail** from the drop-down list.	Whether you can select a server or a type of server, depends up whether or not you checked the **By Server** field.
Criteria	Type *****.	

4. Select **OK** in the **Channel Editor** dialog box.
5. Select the channel that you created in the step above.
6. Select **New Association**.

7. In the **Channel Association** dialog box, complete the fields as shown in the following table to create an inbound and an outbound association for the email channel.

Channel or Association	Field	Recommended entry
Association 1	Channel Range	Completed by IC Manager
	Service Interface	Completed by IC Manager
	Event	ICEmail.Analyze **Note:** This field is case-sensitive and must follow the format *<flow_project>.<flow_name>*
	Flow	*<flow_project>.<flow_name>* For example, enter one of the following: ● **icemail.analyzenoca** if your system does not include Content Analyzer ● **icemail.analyzeca** if your system includes Content Analyzer
Association 2	Channel Range	Completed by IC Manager
	Service Interface	Completed by IC Manager
	Event	ICEmail.OutboundEmail **Note:** This field is case-sensitive and must follow the format *<flow_project>.<flow_name>*
	Flow	*<flow_project>.<flow_name>* For example, enter one of the following: ● **icemail.outboundnoca** if your system does not include Content Analyzer ● **icemail.outboundca** if your system includes Content Analyzer

8. Select **OK** in the **Channel Association** dialog box.
9. Select **OK** in the Server Editor to complete the Workflow server configuration.

Starting the Workflow server

To start the Workflow server:

1. In IC Manager, select the Workflow server that handles email contacts.
2. Right-click the Workflow server and select **Start**.

Using workflows for Email Management

You can use the sample workflows to configure and test your Email Management servers. The Avaya IC seed data includes compiled sample workflows. When you imported seed data into the CCQ database, you stored the compiled workflows in the database.

Email Management uses the following sample workflows:

- An incoming and outbound Email Analysis workflows from the ICEmail project
- The Qualify Email workflow in the WACD project
- All Web Management workflows, see Using workflows for Web Management on page 206

Before your Avaya IC system moves into production, you can modify the properties of the sample workflows to meet your contact center's needs. For example, you can route an outbound email to an approval queue or to an approving agent.

For more information, see *Avaya IC Media Workflow Reference*.

Configuring Outbound Email Analysis workflows

The ICEmail project contains two sample Outbound Email Analysis flows. The sample Outbound with Keywords workflow (outboundnoca) performs analysis on outbound email in Avaya IC systems that do not include Content Analyzer. The sample Outbound with Content Analyzer workflow (outboundca) performs analysis on outbound email in Avaya IC systems with Content Analyzer.

The sample Outbound Email Analysis flows depend on settings in the following:

- Outbound settings in the IC Email server
- Email channel in the Workflow server
- Group properties in IC Manager
- Blocks in the Qualify Email workflow
- Blocks in the Outbound Email Analysis workflow

You must know the configuration of your production environment before you can configure the Outbound Email Analysis flows to work in your Avaya IC system. Therefore, until you have tested your Email Management system and know the configuration of your production environment, you should not run any Outbound Email Analysis flows. For more information on this setting, see Creating the IC Email server on page 247.

If you want to run an Outbound Email Analysis workflow in your Email Management system, you must configure and test your system carefully.

To configure Outbound Email Analysis:

1. In Workflow Designer, open the appropriate Outbound Email Analysis workflow in the ICEmail project, as shown in the following table:

Workflow	Avaya IC system configuration
outboundca	Avaya IC systems with Content Analyzer.
outboundnoca	Avaya IC systems without Content Analyzer.

2. Double-click the GetAgentQuota block and in the Property Sheet:
   a. Select the **Basic** tab.
   b. Set the value of `DefaultQuotaValue` to 0 (zero).

      The default value is 0 (zero), no review of outbound email contacts.
3. Save and recompile the workflow.
4. In IC Manager, set the group properties for agents
   a. Select **Groups** > **Properties** to open the **Group Properties** dialog box:
   b. Select Email/Agent and set the value of the ReviewQuota property.

      The default value is 0 (zero), no review of outbound email contacts.
   c. Apply and save the changes.

   For more detailed instructions, see Setting global properties for all agents on page 293.
5. In IC Manager, if you configured any agents not to cascade their properties from the global properties, set the value of ReviewQuota to 0 (zero) for those agents also. For more detailed instructions, see Setting properties for individual agents and workgroups on page 294.

Creating routing hints for email workflows

The sample email workflows contain blocks that use routing hints from the RoutingHint table in the Directory server to analyze and route email contacts. These blocks include:

- Fetch Routing Hints (email) block in the Qualify Email workflow
- Set Routing Hint blocks in each of the Email Analysis workflows

Important:
Routing hints must be in lower case. Do not use mixed upper and lower case in your routing hints. If the routing hint is not in all lower case, the workflow cannot locate the routing hint, and Avaya IC cannot correctly route the contact.

For more information about the sample email workflows and how the workflows use routing hints, see *Avaya IC Media Workflow Reference*.

The email workflows use hints from the RoutingHint table to route email contacts.

Each row in the routing hint table contains the following:

- A routing hint
- The IDs of the queues where contacts that match the routing hint should be routed

Tip:
The default email queue is DefaultEmailQueue@DefaultTenant. You can create and use additional email queues for routing email contacts. For more information, see *IC Administration Volume 2: Agents, Customers, & Queues*.

The routing hints that you need to create for the sample email workflows depend upon your Avaya IC system. The following table describes the routing hints required by the different sample email workflows.

Avaya IC deployment	Email workflow	Routing hints
Email contact routing	wacd.qualifyemail	If deployment includes email analysis, no additional hints required. If no email analysis, create a routing hint for the To address of email. For example, incomingemail@ic.avaya.com

Avaya IC deployment	Email workflow	Routing hints
Email Analysis with Keywords	icemail.analyzenoca	Create a routing hint with a value such as: • sales • support • printers
	icemail.outboundnoca	Create a routing hint with a value of: • approvalrequired
Email Analysis with Content Analyzer	icemail.analyzeca	Create a routing hint with a value such as: • home computing • desktop Also, create routing hints for language with an ISO-639-1 value such as: • en • sp • fr • de • zh
	icemail.outboundca	Create a routing hint with a value of: • approvalrequired • suspectcontent

To create routing hints:

1. In IC Manager, select the **Configuration** tab.
2. In the left pane, select **Tables** > **Workflow** > **RoutingHint**.
3. Select **New**.
4. In the right pane, complete the fields shown in the following table:

Parameter	Recommended entry	Description
Routing Hint	Type a routing hint.	Type the name of a routing hint required by a sample email workflow. The routing hint must be a single word in all lower case, and cannot contain any special characters.
Email Queue ID	Type `DefaultEmailQueue@DefaultTenant`.	DefaultEmailQueue@DefaultTenant is the default email queue. For more information about email queues, see *IC Administration Volume 2: Agents, Customers, & Queues*.

Parameter	Recommended entry	Description
Category/Qualifier	Leave this field blank.	
Tenant	Select `DefaultTenant` from the queue from the drop-down list.	Select the tenant used by the queue. For the DefaultEmailQueue, select DefaultTenant to ensure that the routing hint uses the correct queue.

5. Select **OK**.
6. Select **Apply**.

   Repeat Steps 3 through 6 until you create all required routing hints.
7. Select **Manager** > **Refresh**.

Configuring the WebACD server for Email Management

If you install the WebACD server and IC Email server on different machines, you must configure the WebACD server for Email Management.

To configure the WebACD server for Email Management:

1. In IC Manager, double-click the WebACD server in the lists of servers.
2. Select the **Configuration** tab.
3. Select **New**.
4. In the **CTI Type Editor** dialog box:
   a. Complete the fields as shown in the following table:

Field	Recommended entry
CTI Type	Couple
Name	emailservername This field is case-sensitive.
Value	Fully-qualified domain name or IP address of the machine that hosts the IC Email server. Make sure this name can be resolved to the correct machine from all agent machines.

   b. Select **OK**.
5. Select **OK**, then stop and restart the WebACD server.

Integrating Email Template Administration

Perform these steps to launch the Email Template Administration Tool from IC Manager.

Tip:
You need to complete only those properties listed in this section to integrate Email Management administration.

To configure Email Template Administration:

1. In IC Manager, select **Tools** > **Groups**.
2. Select the **Properties** tab.
3. Select **IC** in the left pane of the **Group Manager**.
4. Select **System/Configuration** in the **Sections** list.
5. Select the following properties:
   a. Select **Edit**.
   b. Set values for the properties, as shown in the following table:

Property	Recommended entry
EmailLoginServer	Type the fully-qualified domain name of the server that hosts the Email Template Administration pages. For example, type **ICEmail.xyzcorp.com**.
EmailLoginServerPort	Type one of the following ports for the IC Email server web port: ● HTTP - 80 ● HTTPS - 443 Do not change the default port.
EmailLoginServerWebsite	Type **rlmanager** as the name of the Response Library Manager web application. The Configuration Tool defined this application name when you configured Email Template Administration.
EmailServer	Type the fully-qualified domain name of the machine that hosts the IC Email server.
EmailServerPort	Type the IC Email server HTTP port. For example, the default is 19114.

If one of these properties is not available, select **Property Insert** and select the property name from the drop-down menu.

Tip:
If the columns in the right pane are Name, Entity, Value, and Overridable, select the **- (minus)** button on the toolbar to view and edit these properties.

6. Select **Apply**.
7. Select **OK**.
8. Start the IC Email server, if necessary.

Configuring email accounts

You must configure Email Management to use your mail accounts to:

- Retrieve inbound email from customers
- Send outbound agent replies

The following table describes the email accounts that must exist before you configure Email Management to use email accounts.

Required email accounts	Description
Email Management mail accounts	These accounts must exist as mailboxes on the POP3 server. Note the login ID and password. IC Manager can only link to an existing mailbox. IC Manager cannot create mailboxes on a POP3 server.
At least one email account for the Customer account for inbound customer messages	Web Management uses customer email accounts to send email from the Customer Web site to your contact center. Use this email address for mailto: links on your website and wherever you plan to make email addresses available to customers.

Required email accounts	Description
Bounced email account	Email Management uses this account as the destination address for emails sent by the IC Email server that the SMTP server bounces or rejects. All filtered spam and other junk emails also get forwarded to this bounced email. You include this account in your IC Email server configuration.
Disabled accounts (optional)	You can set up Disabled accounts to test or troubleshoot the following servers: ● Web Management servers ● IC Email server ● Tomcat server where you install the website application Email Management does not retrieve messages for disabled accounts.

Email Management can manage mailboxes in any number of domains so long as it has the necessary information to log onto the POP3 server.

Tip:
The IC Email server generates the "to address" for an incoming email from the **Name** and **Domain** fields on the **General** tab of the server. As a result, the logon account does not need to match the first part of the email address, and the "to address" is independent of the logon account used to poll the POP3 server.

To add a POP3 email account to Email Management:

1. In IC Manager, select **Services** > **Email Accounts**.
2. In the **Email Accounts** dialog box, select **New**.

3. In the **New Email Account** property sheet, complete the fields as shown in the following table.

Tab	Field	Description
General tab	Name	Type the mailbox name exactly as it is configured in your POP3 server. For example, type **`agent`**.
	Domain	Type the mailbox domain exactly as it is configured in your POP3 server. For example, type **`xyzcorp.com`**.
	Tenant	Select the tenant that should be associated with this email account from the drop-down list.
	Return address	This address appears in the "From" field in an email response sent to the customer from this account. IC Manager automatically completes this field with **`name@domain`**. To use a different return address, select it from the Return Address drop-down list.
Server tab	Outgoing Email	Type the network address for the SMTP email server you would like to use here.
	Incoming Email	Type the network address of the POP3 server where the email accounts are configured, the logon account, and password in the appropriate field. **Note:** If any of these settings are incorrect, Email Management will not be able to connect to the POP3 email server.
	Logon account	Enter the name of the email account. You do not need to enter the domain.
	Password / Confirm	Enter the password for the email account in both of these fields.
	Log on using Secure Password Authentication	Secure Password Authentication is a challenge-response protocol used by the Windows security subsystem to prevent passwords from being sent through the network in plain text. Your POP3 server must support Secure Password Authentication to use this option.

Tab	Field	Description
Templates tab	—	The **Templates** tab allows you to specify the following templates: ● Header template specifies the text to be inserted at the top of any email to a customer. ● Footer template specifies the text to be appended to the end of any email to a customer. ● New Message template specifies the text to be be automatically sent to a customer when a new email is received from that customer. ● Follow Up template specifies the basic acknowledgement message to be sent when a customer replies to a message sent from Avaya IC. Email Management sends this template whether the message to the customer was an automated outbound or an agent reply. Create these templates in Email Template Administration.
Miscellaneous tab	Validate incoming email addresses	Select this check box if you want to limit the addresses that can send email to this account.
	Valid email addresses	Select the button following this field to specify which addresses can send email to this account. If a message comes in from a different email address, it will be rejected by Email Management. You must check **Validate incoming email addresses** to use this field.
	Override global email checking scheduler	Check this box if you want this account to check for new messages either more or less frequently than the global setting that was specified for the IC Email server.
	New email check frequency	Type the number of seconds between email checks in this field. You must check **Override global email checking scheduler** to use this field.

4. Select **Test** to test your incoming and outbound accounts with your POP3 server or SMTP server.
5. Select **OK**.

For more information about how to create Avaya IC email accounts, see *IC Administration Volume 1: Servers & Domains*.

Creating an email status

An agent can select an email status from a scrollable list in Avaya Web Agent. The agent selects a status to resolve an email contact. You use IC Manager to create the different types of email status that appear in the list.

Important:
You must create at least one email status of Dismiss and check the **Messages set to this status should be treated as answered** field for that status. Email Management requires this Dismiss status when tasks are cancelled in IC Website Administration Tool. If you do not create a Dismiss status, and a task is cancelled from IC Website Administration Tool, the IC Email server server will generate an alarm.

For more information on how to create an email status, see *IC Administration Volume 1: Servers & Domains*.

To create an email status:

1. In IC Manager, select **Services** > **Mail Template Administration**.

   If prompted, log in to Email Template Administration with the same login ID and password that you used for IC Manager.

2. Select **New**.
3. Select **New Status**.
4. In the **New Status Properties** dialog box, complete the following fields:
   a. Type a name for the status in the **Name** field.

      This text is displayed on the list of statuses available to agents in Avaya Agent.

   b. Check the boxes shown in the following table, if desired:

Check box	Recommended entry
Messages set to this status should be treated as answered	Check this box if the status indicates a resolution of the issue that requires no further action by the agent.
Send template for this status	Check this box if you want to send an auto-response message to the user when an agent assigns this status to a message. Choose a template to send. If you do not know the location of the template, select **Browse** and navigate to the desired template.

5. Select **OK** to close the **Status Properties** dialog box.

Configuring Avaya Content Analyzer (optional)

The Avaya IC server installation automatically installs Content Analyzer files on the server machine. For more information, see Installing Avaya IC server and administration components on page 29.

Before you can configure and use Content Analyzer, you must create and configure the Content Analyzer servers.

To configure Content Analyzer, perform the steps in the following topics:

1. Creating the Administrative Content Analyzer server on page 278.
2. Creating the Operations Content Analyzer server on page 279.
3. Adding a Knowledge Base on page 281.

For more detailed information about Content Analyzer, see:

- *Avaya Workflow Designer User Guide* for an overview of Content Analyzer and information about how to customize workflows for Content Analyzer
- *IC Administration Volume 1: Servers & Domains* to administer Content Analyzer, including how to set up and maintain Knowledge Bases and how to train Content Analyzer

Creating the Administrative Content Analyzer server

For more information about the Administrative Content Analyzer server, see *IC Administration Volume 1: Servers & Domains*.

To create the Administrative Content Analyzer server:

1. Select **Server** > **New** in IC Manager.
2. Select **CAAdmin** from the list of servers. Select **OK**.
3. Select the **General** tab and complete the fields shown in the following table.

Field	Recommended entry	Notes
Name	CAADmin_<*domain*>	Include the domain in the server name to identify the server.

Field	Recommended entry	Notes
Domain	Select the Avaya IC domain for the server from the drop-down list.	This server should be in the same domain as the IC Email server. For example, select `Email` from the drop-down list if the server is in the Email domain.
Host	Select the machine's IP address from the drop-down list, or enter the IP address if it is not in the list.	When you select the host, IC Manager fills in the fields for Directory, Port, and Executable.

4. Select the **CAAdmin** tab and complete the fields shown in the following table.

Field	Recommended entry	Notes
IC Data Source	Select the Interaction Center Data Source.	If you used the default name, select `interaction_center`.
Path to NLP Data	Type the directory path to the NLP data.	Windows: *IC_INSTALL_DIR*`\IC71\oem\banter\nlpdata` Solaris or AIX: *IC_INSTALL_DIR*`/IC71/oem/banter/NLPData/`

5. Select **OK**.
6. Start the Administrative Content Analyzer server.

Creating the Operations Content Analyzer server

For more information about the Operations Content Analyzer server, see *IC Administration Volume 1: Servers & Domains*.

Note:
Do not start the Operations Content Analyzer server. You must configure at least one trained and validated Knowledge Base before you start this server.

To create the Operations Content Analyzer server:

1. Select **Server** > **New** in IC Manager.
2. Select **CAServer** from the list of servers. Select **OK**.

3. Select the **General** tab and complete the fields shown in the following table.

Field	Recommended entry	Notes
Name	OperationCA_<*domain*>	Include the domain in the server name to identify the server.
Domain	Select the Avaya IC domain for the server from the drop-down list.	This server should be in the same domain as the IC Email server. For example, select `Email` from the drop-down list if the server is in the Email domain.
Host	Select the machine's IP address from the drop-down list, or enter the IP address if it is not in the list.	When you select the host, IC Manager fills in the fields for Directory, Port, and Executable.

4. Select the **CA Server** tab and complete the fields shown in the following table.

Field	Recommended entry	Notes
IC Data Source	Select the Interaction Center Data Source.	If you used the default name, select `interaction_center`.
Path to NLP Data	Type the directory path to the NLP data.	Windows: *IC_INSTALL_DIR*\IC71\oem\banter\nlpdata Solaris or AIX: *IC_INSTALL_DIR*/IC71/oem/banter/NLPData/
Knowledge Base	Type the name of the Knowledge Base associated with this server.	Select **Knowledge Base** to display the **Knowledge Base** dialog box. For details about entering a Knowledge Base, see below.

5. Select **OK**.

Adding a Knowledge Base

Before you add a Knowledge Base to your Operations Content Analyzer server, perform the following steps in the Content Analyzer Administration tab:

1. Create the Knowledge Base.
2. Train the Knowledge Base.
3. Validate the Knowledge Base.
4. Save the trained and validated Knowledge Base.

For detailed information on how to perform these steps, see *IC Administration Volume 1: Servers & Domains*.

You need the following information about the Knowledge Bases before you add them to the Operations Content Analyzer server:

- Name
- File path
- Threshold
- Language codes

This information is available in IC Manager for all saved Knowledge Bases. You can find this information in the **KB Management** pane of the **Content Analysis** window.

To add a Knowledge Base to the Operations Content Analyzer server:

1. Double-click the Operations Content Analyzer server in the list of servers.
2. Select the **CAServer** tab.
3. Select the **Ellipsis (…)** button next to **Knowledge Base**.
4. In the **Knowledge Base** dialog box:
   a. Select **New**.
   b. Type the name of the Knowledge Base in the **Name** column.

      This name must be the same as the name of the Knowledge Base in the **KB Name** column of the **KB Management** pane in the **Content Analysis** window.

c. Type the directory path to the Knowledge Base in the **KB File Location** column.

   This path must be the same as the path in the **File Path** column of the **KB Management** pane in the **Content Analysis** window.

   If the Administrative Content Analyzer server and the Operations Content Analyzer server are hosted on the same physical machine, this path must match the **File Path** column of the **KB Management** pane in the **Content Analysis** window.

   If the Administrative Content Analyzer server and the Operations Content Analyzer server are hosted on different physical machines, make sure that this file path accesses the same Knowledge Base as the one pointed to by the **File Path** column of the **KB Management** pane in the **Content Analysis** window.

d. Type a threshold in the **Threshold** column, if desired.

   You can leave this column blank or type the same threshold that you specified when you validated the Knowledge Base.

e. Select the **Ellipsis** (**…**) button in the **Languages** column.

5. In the **Languages** dialog box:

   a. Select **New**.

   b. Type a language code.

      Repeat Steps a and b for each language code you want to add. All available language codes are in the **Languages** column of the **KB Management** pane in the **Content Analysis** window. The language codes are listed in a single string, separated by semicolons.

   c. Select **OK**.

6. Select **OK** in the **Knowledge Base** dialog box.

7. Select **OK** in the **CAServer** tab.

Chapter 9: Configuring agent accounts

You must create and configure Avaya IC accounts for all agents who will use Avaya Agent, Avaya Agent Web Client, or a custom application developed with the Client SDK.

After you create the agent accounts, you also need to configure the:

- Unified Agent Directory for agents who work with Avaya Agent
- Address Book for agents who work with Avaya Agent Web Client
- Address Book agents who work with a custom application created with the Client SDK

The Unified Agent Directory and the Address Book allow agents to interact with other agents in the Avaya IC system.

Tip:
This section includes basic information about how to create test agents for a development Avaya IC system. A customized system or a production system may require that you configure additional properties. For more information about agent properties that you can configure for agent accounts, see *IC Administration Volume 2: Agents, Customers, & Queues*.

This section includes the following topics:

Required permissions for agents

Agents can run Avaya IC agent desktop applications with limited permissions over certain directories on their desktops. Agents do not require administrator privileges.

The following table describes the permissions and allowable restrictions on Avaya IC directories for agent desktop applications.

Directory	Required permissions	Allowable restrictions
IC_INSTALL_DIR\IC71\bin	Modify permissions (includes Read, Write, Execute)	Delete
IC_INSTALL_DIR\IC71\etc	Modify permissions (includes Read, Write, Execute)	Delete
IC_INSTALL_DIR\IC71\apps	Modify permissions (includes Read, Write, Execute)	Delete
IC_INSTALL_DIR\IC71\logs	Modify permissions (includes Read, Write, Execute)	Delete

Cautions and tips for creating agent accounts

You must create an account in IC Manager for each agent, supervisor, and other employees who need to use Avaya IC. Each user account requires that you configure permissions, media channels, and other requirements.

This manual contains only the information that you require to create agent and other user accounts for testing, including the minimal permissions and configuration settings. For more information, see *IC Administration Volume 2: Agents, Customers, & Queues*.

This section includes some important cautions and tips that you need to consider when you create agents for your Avaya IC system. Additional information is available in *IC Administration Volume 2: Agents, Customers, & Queues*.

This section includes the following topics:

Agent domains

All Avaya IC agent accounts must belong to a User domain. You must create all User domains before you create your agents. If you create agents first, you must assign all agents to the Default domain, and then create the User domains and reassign the agents.

If your User domain does not include a secondary ORB server, the domain must failover to a domain that includes an ORB server, such as the Default domain.

Agent workgroups and tenants

Avaya strongly recommends that you organize your agent population into sets of tenants and workgroups that mirror the organization of your contact center. A tenant is a set of workgroups that fulfill a particular business function. You can use tenants to define the security and administrative boundaries around data, queues, and content resources. A workgroup is a set of agents or queues that form a logical grouping.

A workgroup can only belong to one tenant. However, you can share agents across tenants by assigning them to multiple workgroups. To use workgroups, create workgroups and tenants before you create agents.

Tenants, workgroups, and agents inherit properties from parent to child entities. By default, if you assign a property value to a tenant, the workgroups in that tenant inherit that property value from the tenant, and the agents in the workgroups inherit the property value from the workgroups. When you assign agents to workgroups, and workgroups to agents, you can specify the order of inheritance. The inheritance order controls which property value IC Manager uses for an agent if an entity inherits multiple values for the same property.

Agent login IDs

Each agent must have a separate and unique login ID.

If an agent or supervisor needs to monitor multiple Avaya IC devices, the agent or supervisor must have a separate and unique Avaya IC login ID for each device.

Avaya IC does not support simultaneous logins with the same login ID.

Important:
Simultaneous logins with the same login ID can cause serious issues with the performance of Avaya IC.

Avaya IC does not support:

- Two agents logging in with the same login ID.
- One agent simultaneously logging in to more than one machine with the same login ID.
- One agent simultaneously logging in to more than one Avaya IC desktop application with the same login ID.

Agent password requirements

To prevent access to Avaya IC by unauthorized users, agents are assigned passwords that are required when they log into Avaya IC.

Tip:
Password requirements (such as the required length and duration) are controlled by the properties in the Agent/Security section. For information about these properties, see *IC Administration Volume 2: Agents, Customers, & Queues*.

Creating an agent account

You must create at least one agent account to test the Avaya IC system and make sure that all features and media channels function correctly. When you create your production system, you must create an Avaya IC agent account for each agent who will work with an Avaya IC agent application.

Tip:
Avaya recommends that you create at least one agent in each User domain. Configure these agents to handle all applicable media channels.

The procedures in this section contain information on how to set basic properties for agent accounts, so you can test your system. If you want to set additional properties for your test agents, see *IC Administration Volume 2: Agents, Customers, & Queues*.

To create an agent, perform the tasks in the following topics:

1. Creating an agent account on page 287.
2. Configuring an agent for media channels on page 290.

After you create an agent account, you must configure the agent properties, as described in Setting agent properties on page 293.

Creating an agent account

This procedure assumes that you will create the agent account in the Default tenant.

To create an agent account:

1. In IC Manager, select the **Agent** tab.
2. Expand the **DefaultTenant** node in the left pane.

   If you want to create the agent account in a different tenant, select that node in the left pane.
3. Select **Agent** > **New**.
4. Select the **General** tab and complete the fields as shown in the following table:

Field	Description
First Name	Required field Type agent's first name.
Last Name	Required field Type agent's last name.
Preferred Name	Required field Type agent's preferred name.
Employee ID	Type the agent's company employee ID (if available).
Domain	Required field Select domain for the agent from the list. **Note:** If the agent will handle chat contacts, the agent domain must failover to the domain that includes the Paging server.
Site	Select a site from the drop-down list. Note: Avaya IC uses the Site to compile statistics for groups or agents or queues.

5. In the **System Information** group of the **General** tab, complete the fields as shown in the following table:

Field	Description
Login ID	Required field Type a login ID that the agent uses for all Avaya IC applications. Each agent account must have a separate and unique login ID. For more information, see Agent login IDs on page 285.
Options	1. Select the **Ellipsis (…)** button next to **Options**. 2. Check the **User Addressable** box to make the agents visible for transfers. 3. Select **OK**.
Task Load	Required field Set this field to no more than 6 concurrent tasks. Use the arrow keys to set the maximum number of contacts that the agent can handle concurrently. These contacts can come from any of the media channels used by the agent. For example, if you plan to configure the test agent to use Email and Voice media channels, and to set the task load on Email to 2 and the task load on Voice to 1, set this Task Load property to 3.
Task Ceiling	Required field. Use the arrow keys to set the limit of the task load across all of the media channels. The task load must be less than or equal to the task ceiling. **Note:** The Task Load can vary according to your system conditions, such as number of tasks, agents, or time of day. The Task Ceiling is an upper limit on the Task Load.

6. In the **Membership Information** group of the **General** tab, complete the fields as shown in the following table:

Field	Recommended entry
Domain	Required field Select your User domain from the drop-down list.
Workgroup	1. Select the **Ellipsis (…)** button next to **Workgroup**. 2. Expand the **DefaultTenant** node in the Workgroups list. 3. Select the **Default** workgroup. 4. Select **>>** to add the agent to the Default workgroup. 5. Select **OK**. **Note:** Agents can belong to more than one workgroup. Agents who work with chat contacts or email contacts must have the Default workgroup as their primary workgroup.
Site	Select a site from the drop-down list. **Note:** Avaya IC uses the Site to compile statistics for groups or agents or queues.

Tip:
If you want this agent to be a Supervisor who can monitor chats between other agents and customers, configure this agent as the Supervisor for the Workgroup.

7. Select the **Email** tab in the center of the **General** tab, and complete the fields as shown in the following table:

Field	Recommended entry
Primary	Type the email address assigned to the agent by the contact center. This address is configured at the mail server. If you specify that the agent is user addressable on the System tab, Avaya IC lists this email address for the agent in the Agent Directory.
Internal	Type the email address assigned to the agent for internal email messages only. This address is not intended to be used outside of the contact center.
Personal	Type the email address assigned to the agent for personal, non-business communication from the agent.
Mobile Device	Type the email address assigned to the agent for use with their mobile device.

8. Select **OK**.

9. Select the **Security** tab and complete the fields as shown in the following table to set agent security:

Field	Recommended entry
Password	Type the password that the agent uses to log in to Avaya IC applications. For example, type agent1.
Confirm	Type the password a second time to confirm.
Roles	Check one or more boxes to select the agent's security level.

10. Select **OK**.

Configuring an agent for media channels

When you set Task Load and Task Ceiling for the media channels, make sure that:

- The total of all Task Load values does not exceed the Task Load that you set for the agent on the **General** tab.
- The total of all Task Ceiling values does not exceed the Task Ceiling set on the **General** tab.

Important:
If you want an agent to handle Web Scheduled Callback contacts, you must configure the agent to handle voice and chat contacts.

This section includes the following topics:

- Configuring an agent to handle chat contacts on page 290.
- Configuring an agent to handle email contacts on page 291.
- Configuring an agent to handle voice contacts on page 292.

Configuring an agent to handle chat contacts

If you want the agent to receive and handle Web Scheduled Callback contacts, you must also configure the agent to handle voice contacts.

Tip:
This step continues from the previous step and assumes that the agent account remains open in IC Manager.

To configure an agent to handle chat contacts:

1. Select the **Channels** tab.
2. Select **Chat** from the **Channel** drop-down list.
3. Complete the fields as shown in the following table:

Field	Recommended entry
Disable Chat Channel	Clear this box.
Task Load	Set the maximum number of chat contacts an agent can handle at one time.
Task Ceiling	Set the maximum value for the chat Task Load.

4. Select **Apply**.

Configuring an agent to handle email contacts

Tip:
This step continues from the previous step and assumes that the agent account remains open in IC Manager.

To configure an agent to receive handle email contacts:

1. In the **Channels** tab, select **Email** from the **Channel** drop-down list.
2. Complete the fields as shown in the following table:

Field	Recommended entry
Disable Email Channel	Clear this box.
Show Full Headers	Check this box if you want the agent to see the full header of each email contact.
From Address	Type the email address that you want recipients to see in emails from this agent.
Task Load	Set the maximum number of email contacts an agent can handle at one time.
Task Ceiling	Set the maximum value for the email Task Load.

3. Configure the primary email address for the agent, as described in Step 7 of Creating an agent account on page 286.
4. Select **Apply**.

Configuring an agent to handle voice contacts

If you want the agent to receive and handle Web Scheduled Callback contacts, you must also configure the agent to handle chat contacts.

Tip:
This step continues from the previous step and assumes that the agent account remains open in IC Manager.

To configure an agent to handle voice contacts:

1. Select **Voice** from the **Channel** drop-down list.
2. Complete the fields as shown in the following table:

Field	Recommended entry
Disable Voice Channel	Clear this box.
Phone ID	Type the logical extension number for the agent's phone. For example, type 34181.
Password	Type the password for agent login to the ACD.
Phone Type	Type the type of phone that the agent uses. The switch requirement for agent login determines the phone type. Some supported switches support both phone types. Other supported switches only support one phone type. ● Type EAS if the configuration controls the queue structure. You can only type EAS for Avaya DEFINITY/Communication Manager, or Aspect. ● Type ACD if the switch requires a queue. You can type ACD for all supported switches.
Equipment	Type the physical extension number for the agent's phone. For example, type 24181.
Queue	Type the default voice queue for this agent.
Task Load	Set the maximum number of voice contacts an agent can handle at one time.
Task Ceiling	Set the maximum value for the voice Task Load.

3. Select **Apply**.

Setting agent properties

By default, Avaya IC provides default values for most agent properties. You can use these default values to ensure that the agent applications function correctly.

As you customize the Avaya IC system, you may need to configure different values for these agent properties. For example, you need to configure different values for the agent properties if you want the agent desktop applications to include wrapup functionality. For information about the agent properties or how to enable other features, see *IC Administration Volume 2: Agents, Customers, & Queues*.

This section includes the following topics that describe how to set properties for agents:

- Setting global properties for all agents on page 293.
- Setting properties for individual agents and workgroups on page 294.

Setting global properties for all agents

The procedures in this topic assume that the property already exists in the property section. If a property does not exist, click **Add Property** and select that property from the **Assign Property** dialog box. For more information on adding properties to a property section, see *IC Administration Volume 2: Agents, Customers, & Queues*.

To set global properties that affect all agents in Avaya IC:

1. In IC Manager, select **Tools** > **Groups**.
2. Select the **Properties** tab.
3. Select the IC node in the left pane.
4. In the **Sections** list, select the property section that includes the property you want to set.
5. In the right pane, double-click the property that you want to set.
6. In the **Edit Property** dialog box:
   a. In the **Property** drop-down list, verify that the correct property is selected.
   b. In the **Property Value** field, set the value for the property.
   c. Clear the **Descendants May Override** checkbox.
   d. Select **OK**.
7. Select **Apply**.
8. Select **OK**.

Setting properties for individual agents and workgroups

The procedures in this topic assume that the property already exists in the property section. If a property does not exist, click **Add Property** and select that property from the **Assign Property** dialog box. For more information on adding properties to a property section, see *IC Administration Volume 2: Agents, Customers, & Queues*.

To set properties for individual agents and workgroups:

1. In IC Manager, select the **Agent** tab.
2. Select the desired agent or workgroup:
   - To select a workgroup, navigate to and select the desired workgroup in the left pane.
   - To select an agent, navigate to the workgroup that includes the agent in the left pane, then double-click the agent in the list of agents.
3. Select the **Properties** tab.
4. In the **Sections** list, select the desired property section.
5. In the right pane, double-click the property that you want to set.
6. In the **Edit Property** dialog box:
   a. If necessary, select the property name from the **Property Name** drop-down list.
   b. In the **Property Value** field, set the value for the property.
   c. Clear the **Descendants May Override** checkbox.
   d. Select **OK**.
7. Select **Apply**.
8. Select **OK**.

Configuring agents for Avaya Agent

For agents who will work in Avaya Agent, these agent properties ensure that Avaya Agent and the Unified Agent Directory include the functions required by the agent. For example, you specify which Avaya Agent layout the agent will use.

For information about properties that configure additional features available for agents who work with Avaya Agent, including wrapup, see *IC Administration Volume 2: Agents, Customers, & Queues*.

This section includes the following topics:

Setting agent properties for Avaya Agent

The agent properties that you must set for Avaya Agent include the Avaya Agent layout that an agent will use and the home directory for agents who handle chat contacts and email contacts.

You can change some or all of these default values to ensure that the functionality available to your agents matches the configuration of your Avaya IC system. Before you move to a production environment, review these properties to determine whether you need to change any of the default values. For more information about the additional agent properties, see *IC Administration Volume 2: Agents, Customers, & Queues*.

Configuring the agent layout property

By default the agent layout property is configured for the out-of-the-box, English Avaya Agent layout. If the Avaya IC system includes a custom or non-English Avaya Agent layout, you must configure the Agent/Desktop/Layout property for that layout.

Configuring the home directory property

The home directory property is always configured from the perspective of Avaya Agent. The syntax that you use to configure the home directory property depends upon how the machine that hosts Avaya Agent will access the directory. Since Avaya Agent is only supported on Windows, the syntax for the home directory must be in a format that Windows can use to access another network machine.

Important:
Even if the home directory uses the same shared directory as the working directory, you may need to use a different syntax for the home directory property.

For more information about the home directory property, including recommended deployments of the home directory for Avaya Agent and the working directory of Avaya Agent Web Client, see *IC Administration Volume 2: Agents, Customers, & Queues*.

To configure the home directory:

1. If it does not already exist, create the shared directory for the home directory on a network machine.
2. Ensure that all agent workstations that host Avaya Agent:
   - Can access the shared directory for the home directory through either a mapped drive or UNC notation in Windows Explorer.
   - Have the required Read, Write, and Execute permissions for that directory
3. Configure the `Agent/Desktop/WAC.HomeDir` as described in Setting agent properties on page 293.

   The following table provides examples of the syntax used to configure the home directory property. These examples use the `AgentResource` directory on a machine named `resource.xyzcorp.com` as the shared directory.

Avaya Agent access to shared directory	Syntax for home directory
You map the Z: drive on each agent workstation to the shared directory folder hosted on a Windows network machine. **Note:** Do not use this syntax if the shared directory is on a UNIX machine.	`Z:\AgentResource`
Each agent workstation uses UNC notation in Windows Explorer to access the shared directory. **Note:** You can use this syntax if the shared directory is on a Windows or UNIX machine.	`\\resource.xyzcorp.com\AgentResource`

Configuring agents for the Unified Agent Directory

The Unified Agent Directory contains resources for your contact center, including:

- Queues
- Agents
- Supervisors
- Subject Matter Experts
- Non-human resources, such as Interactive Voice Response units (IVRs)

You must configure queues and agents as Addressable if you want them to be visible in the Unified Agent Directory. For agents, set the ShowAgentsOnStartup property to be True to display the Directory tab in the Unified Agent Directory. Agents use the Directory tab to view individual agents in the contact center.

Agents can filter their view of the Unified Agent Directory to see only agents or queues that meet specified criteria. You can change this setting to force agents to view all of the agents and queues in your contact center, if desired.

For information on how to set other properties related to the Unified Agent Directory, see *IC Administration Volume 2: Agents, Customers, & Queues*. For information on how to use the Unified Agent Directory, see *Avaya Agent User's Guide*.

Note:
You do not need to perform these steps if the Avaya IC system does not include Avaya Agent.

The following table describes the properties that you need to set for agents to display in and use the Unified Agent Directory. All properties for the Unified Agent Directory are in the Agent/Desktop/Directory section.

Property	Recommended entry	Notes
ShowAgentsOnStartup	Yes	Adds the Directory Tab to the Unified Agent Directory.
ShowAgentState	Yes	Displays agent's state in the Directory tree of the Unified Agent Directory.
ShowAllAgents	Yes	Shows the entire Directory tree for agents in the Unified Agent Directory.
SkillsSupport	Yes	Lets agents use skills as search criteria in the Unified Agent Directory.
TransferFlowName	Type the name of the workflow that retrieves the destination from the virtual queue.	

Property	Recommended entry	Notes
WorkflowServerName	Name of the Workflow server that runs the workflows for the Unified Agent Directory.	Use the Workflow server where you added the semaphore in Configuring a Workflow server for transfers and conferences on page 303.
UADStringFormat	Select the desired string format.	Determines how agents are displayed in the Unified Agent Directory. When you choose a string format, the Unified Agent Directory displays the following information in IC Manager: • Standard string format displays the Display Name for an agent. • ASCII string format displays the Full Name for an agent. • LoginID string format displays the Login Name for an agent.

Configuring agents for Avaya Agent Web Client

The only agent property that you must set for Avaya Agent Web Client is the working directory that an agent will use. IC Manager includes additional agent properties that have default values. You can change some or all of these default values to ensure that the functionality available to your agents matches the configuration of your Avaya IC system.

Before you move to a production environment, review the additional properties to determine whether you need to change any of the default values. For more information about the additional agent properties, see *IC Administration Volume 2: Agents, Customers, & Queues*.

Tip:
You must also create a separate agent account for each Java Application Bridge that communicates with Avaya Agent Web Client. For more information, see Configuring an agent account for the Java Application Bridge on page 333.

This section includes the following topics:

Configuring the working directory property

The working directory property is always configured from the perspective of IBM WAS. The syntax that you use to configure the working directory property depends upon the operating system of the machine that hosts IBM WAS for Avaya Agent Web Client and how that machine will access the shared directory.

Even if the working directory uses the same shared directory as the home directory, you may need to use a different syntax to configure the working directory property.

For more information about the home directory property, including recommended deployments of the working directory of Avaya Agent Web Client and the home directory for Avaya Agent, see *IC Administration Volume 2: Agents, Customers, & Queues*.

CAUTION:
If you do not use a valid directory path when you configure the working directory, Avaya Agent Web Client will not function properly. Avaya Agent Web Client displays an error message on the Status Bar, and the chat and email channels will be disabled.

To configure the working directory:

1. If it does not already exist, create the shared directory for the working directory on a network machine.
2. Ensure that all machines that host IBM WAS for Avaya Agent Web Client:
   - Can access the shared directory for the working directory through one of the following methods:
     - For a Windows machine: a mapped drive or UNC notation in Windows Explorer
     - For a UNIX machine, an NFS mount for the shared directory
   - Have the required Read, Write, and Execute permissions for that directory
3. Configure the `Agent/Desktop/WebClient.WorkingDirectory` as described in Setting agent properties on page 293.

   The examples in the following table use the `AgentResource` directory on a machine named `resource.xyzcorp.com` as the shared directory.

IBM WAS access to shared directory	Syntax for working directory
You map the Z: drive on the IBM WAS machine to the shared directory folder hosted on a Windows network machine. **Note:** Do not use this syntax if IBM WAS is on a UNIX machine.	`Z:\AgentResource`

IBM WAS access to shared directory	Syntax for working directory
The IBM WAS machine uses UNC notation in Windows Explorer to access the shared directory. **Note:** Do not use this syntax if IBM WAS is on a UNIX machine.	`\\resource.xyzcorp.com\AgentResource`
You perform an NFS mount for the shared directory on the IBM WAS machine. **Note:** Do not use this syntax if IBM WAS is on a Windows machine.	/opt/AgentResource

Configuring agents for the Address Book

You do not need to configure any agent properties for the Address Book to work in Avaya Agent Web Client. However, if you want an agent to be visible in the Address Book, you must also configure the agent for the Address Book.

To configure agents for the Address Book in Avaya Agent Web Client:

1. Enable the **User Addressable** field in the **System Information** group of the **General** tab for each agent who:
   - Will work in Avaya Agent Web Client
   - Must be visible in the Address Book

   For more information on how to enable the User Addressable field, see Options in Creating an agent account on page 287.
2. Configure the primary email address for each agent who:
   - Will need to receive emails in Avaya Agent Web Client or from agents who work in Avaya Agent Web Client
   - Must be visible in the Address Book

   For more information, see Step 7 of Creating an agent account on page 286.

Creating agents for a Client SDK custom application

The only agent property that you must set for a custom application developed with the Client SDK is the working directory that an agent will use. IC Manager includes additional agent properties that have default values. You can change some or all of these default values to ensure that the functionality available to your agents matches the configuration of your Avaya IC system.

Before you move to a production environment, review the additional properties to determine whether you need to change any of the default values. For more information about the additional agent properties, see *IC Administration Volume 2: Agents, Customers, & Queues*.

Tip:
You must also create a separate agent account for each Java Application Bridge that communicates with the Client SDK server. For more information, see Creating an agent account for the Java Application Bridge on page 368.

This section includes the following topics:

Configuring the working directory property

The working directory property is always configured from the perspective of Tomcat. The syntax that you use to configure the working directory property depends upon the operating system of the machine that hosts Tomcat for the Client SDK server and how that machine will access the shared directory.

Even if the working directory uses the same shared directory as the home directory, you may need to use a different syntax to configure the working directory property.

For more information about the working directory property, including recommended deployments, see *IC Administration Volume 2: Agents, Customers, & Queues*.

CAUTION:
If you do not use a valid directory path when you configure the working directory, your custom application will not function properly. You should configure your custom application to display an error message on the Status Bar and to disable the chat and email channels.

To configure the working directory:

1. If it does not already exist, create the shared directory for the working directory on a network machine.
2. Ensure that all machines that host Tomcat for the Client SDK:
   - Can access the shared directory for the working directory through one of the following methods:
     - For a Windows machine: a mapped drive or UNC notation in Windows Explorer
     - For a UNIX machine, an NFS mount for the shared directory
   - Have the required Read, Write, and Execute permissions for that directory
3. Configure the `Agent/Desktop/WebClient.WorkingDirectory`.

   The following table provides examples of the syntax used to configure the working directory property. These examples use the `AgentResource` directory on a machine named `resource.xyzcorp.com` as the shared directory.

Tomcat access to shared directory	Syntax for working directory
You map the Z: drive on the Tomcat machine to the shared directory folder hosted on a Windows network machine. **Note:** Do not use this syntax if Tomcat is on a UNIX machine.	`Z:\AgentResource`
The Tomcat machine uses UNC notation in Windows Explorer to access the shared directory. **Note:** Do not use this syntax if Tomcat is on a UNIX machine.	`\\resource.xyzcorp.com\AgentResource`
You perform an NFS mount for the shared directory on the Tomcat machine. **Note:** Do not use this syntax if Tomcat is on a Windows machine.	/opt/AgentResource

Configuring agents for the Address Book

You do not need to configure any agent properties for the Address Book to work in your custom application. However, if you want an agent to be visible in the Address Book of your custom application, you must also configure that agent for the Address Book.

To configure agents for the Address Book in your custom application:

1. Enable the **User Addressable** field in the **System Information** group of the **General** tab for each agent who:
   - Will work in your custom application
   - Must be visible in the Address Book

   For more information on how to enable the User Addressable field, see *IC Administration Volume 2: Agents, Customers, & Queues*.
2. Configure the primary email address for each agent who:
   - Will need to receive emails in your custom application or from agents who work in your custom application
   - Must be visible in the Address Book

   For more information, see *IC Administration Volume 2: Agents, Customers, & Queues*.

Configuring a Workflow server for transfers and conferences

For agents to be able to transfer or conference voice contacts and chat contacts to virtual queues, you must configure every Workflow server in a user domain for transfers and conferences. Without this configuration, agents will not be able to transfer contacts to queues and may encounter problems with transfers to and conferences with agents.

All Avaya IC systems require Workflow servers in User domains to handle agent transfers and conferences. You must perform these steps if the Avaya IC system includes Avaya Agent or Avaya Agent Web Client.

This section includes the following topics:

Required configuration parameters

The following table describes the required configuration parameters for Workflow servers that handle agent transfers and conferences.

Configuration parameter	Value
Semaphore	agentsearch.update_searchresult
Synchronous Startup Flow	sys_transfer.update_vq_cache
Startup Flow	sys_agentsearch.update_agentstate_cache

Working with transfer workflows

The Avaya IC seed data includes these workflows. When you created the CCQ database, you imported the compiled workflows with the seed data and stored them in the database. However, you must still associate these workflows with the Workflow server.

Configuring a Workflow server

If your Avaya IC system includes multiple Workflow servers, perform these steps on every Workflow server in a user domain and every Workflow server that handles agent searches and transfers between agents.

Important:
If you create a new virtual queue or queue for agent transfers, you must do one of the following for every Workflow server in a user domains that runs workflows for the Unified Agent Directory:

- Manually run the sys_transfer.update_vq_cache workflow
- Restart each Workflow server

To configure the Workflow server for agent transfers and conferences:

1. In the **Server** tab of IC Manager, double-click a Workflow server in a user domain.
2. Select the **Workflow** tab.
3. Confirm that the Workflow server includes the following required semaphore: `agentsearch.update_searchresult`
   a. Select the **Ellipsis (…)** button next to **Semaphores**.

   b. If the rows do not include the required semaphore:
      - Select **New**.
      - In the new row, type **`agentsearch.update_searchresult`**
      - Select **OK**.
4. Confirm that the Workflow server includes the required synchronous startup flows:
   a. Select the **Ellipsis (…)** button next to **Synchronous Startup Flows**.
   b. Verify that the rows include the following required synchronous startup flows:
      - `sys_transfer.update_vq_cache`
      - `sys_transfer.transfertovq`

      If the rows do not include either or both of those required flows, select **New** and add the missing flow.
5. Confirm that the Workflow server includes the following required startup flow:
   a. Select the **Ellipsis (…)** button next to **Startup Flows**.
   b. If the rows do not include the following required startup flow: `sys_agentsearch.update_agentstate_cache`
      - Select **New**.
      - In the new row, type **`sys_agentsearch.update_agentstate_cache`**.
      - Select **OK**.
6. Select **OK**.
7. Stop and restart the Workflow server.

   Repeat these steps for every Workflow server in a user domain.

Chapter 10: Deploying Avaya Agent

Perform the steps in the following topics to deploy Avaya Agent:

1. Required privileges for the agent installer on page 307.
2. Creating installation files for agent applications on page 307.
3. Preparing for installation by agents on page 313.
4. Configuring automatic updates for agent applications on page 315.
5. Configuring the Citrix integration on page 318.

Important:
Read the Avaya IC Readme file and *IC Installation Planning and Prerequisites* before you install Avaya Agent.

Required privileges for the agent installer

All Avaya IC users who create agent installers and who install or configure Avaya IC components require an Administrator login or a login with administrator privileges.

Creating installation files for agent applications

To create installation files for agent applications, perform the steps in the following topics:

1. Cautions and tips for installation files on page 308
2. Required information for the Agent Site Preparation wizard on page 310.
3. Running the Avaya Agent site preparation wizard on page 311.
4. Copying the server implementation file on page 312.

Cautions and tips for installation files

Before you run the Agent Site Preparation wizard, note the cautions and tips in the following topics:

- Disabling firewalls on page 308.
- Stopping agent desktop applications on page 308.
- Installation path for agent desktop applications on page 309.
- Size of agent installer directory on page 309.
- Installer directory availability on page 309.
- Location for Avaya Agent installation on page 309.
- Size of Avaya Agent installation directory on page 309.
- Solaris or AIX machine on page 309.

Disabling firewalls

If the machine where you want to install Avaya Agent has a personal or desktop firewall, you need to disable the firewall before you start the installation. You can re-enable the firewall after the installation is complete.

Stopping agent desktop applications

Before you or an agent runs the Agent Installer on an agent desktop machine, confirm that there are no Avaya IC agent desktop applications or qui.exe processes running on the agent machine. The Agent Installer may stop responding or pause indefinitely if an agent desktop or qui.exe process is still running.

Configuring Internet Explorer on agent workstations

Set the following internet options in Internet Explorer for all agents who will handle chat contacts:

- Security level: Medium if agents use Windows 2003.
- ActiveX controls: allow to run.
- Trusted sites: add the URL of the Website server to the Trusted Sites list.

Installation path for agent desktop applications

The agent installer automatically adds the following to the installation path for agent desktop applications: `\apps\<application_name>`

When you specify the initial section for the installation path, do not include any duplication of the directories. If you include a duplicate directory, the `-d` parameter in the shortcut cannot find the working directory for the applications.

For example, if you specify `C:\apps` as the installation path for agent desktop applications, the `-d` parameter cannot locate the apps directory, as it is duplicated in the installation path of `C:\apps\Avaya\IC71\apps\interaction_center`

Size of agent installer directory

Select a network share with at least 110MB of available disk space for each agent installer directory.

Installer directory availability

Make sure that the network machine is online when you run the Agent Site Preparation wizard.

Location for Avaya Agent installation

Select the directory path for the Avaya Agent installation on the desk top machines.

Size of Avaya Agent installation directory

Make sure that the agent desktop machines have at least 350 MB of available disk space. Approximately 220 MB of the required available space must be in a `temp` directory. The agent installer deletes the files in the `temp` directory when you reboot the agent machine.

Solaris or AIX machine

If you plan to host the agent installer on a Solaris or AIX machine, you must:

1. Run the Agent Site Preparation wizard on a Windows machine.
2. Transfer the files to a Samba share on the Solaris or AIX machine.

Required information for the Agent Site Preparation wizard

Before you complete the required information, you must know how many different agent configurations your contact center requires. If you must create multiple agent configurations, you must run the Agent Site Preparation wizard for each configuration.

You must plan your agent desktop configuration before you run the Agent Site Preparation wizard. The tables in each section provide examples of the kind of planning and information that you must complete before you run the Agent Site Preparation wizard. You can fill out your configuration information in these tables, or create similar tables of your own.

Path for agent installers: The path for agent installers specifies the directory path for the folder where you place the agent installer and configuration data for each agent configuration.

The default directory is: `C:\Program Files\Avaya\IC71\AgentInstaller`. You can copy the installation files to another location, such as a Web server, after you create the agent installer.

By default, the Agent Site Preparation Wizard places the agent installer in a directory path that includes *IC71* to ensure that you do not overwrite an earlier version of the agent installer. The default directory path is **C:\Program Files\Avaya\IC71\AgentInstaller**.

Directory on agent desktop: The directory on the agent desktop specifies where the agent installer will install Avaya Agent. Use a drive and directory that is valid on all agent desktop machines. The agent installer will present this directory to all agents during the installation. If desired, you can let agents override the default installation directory and select their own installation directory.

By default, the agent installer places the agent desktop applications in a directory path that includes *IC71* to ensure that the agent applications are correctly updated.

For example, the default directory and path for installing agent desktop applications is: `C:\Program Files\Avaya\IC71\`

Applications to be installed: Most Avaya Agent installations use Interaction Center as the agent application to include in each agent configuration.

Telephony switch type: If your Avaya IC system includes Telephony, you must know the type of telephony switch used by the agents who will use the version of Avaya Agent installed by this agent installer.

Automatic updates: Automatic updates configure Avaya Agent to update agent configurations to the latest version whenever agents log in. For more information, see Configuring automatic updates for agent applications on page 315.

Running the Avaya Agent site preparation wizard

Repeat this entire procedure for each Avaya Agent configuration in the Avaya IC system.

To run the Avaya Agent site preparation wizard:

1. Insert Avaya IC Release 7.1 CD-ROM 4.

   The Avaya IC installer starts automatically. If you disabled Autorun on the machine, navigate to the Servers directory on the CD-ROM and run `setup.exe`.

2. When the Avaya IC installer opens, read the entire Avaya IC license agreement carefully, then accept the terms of the agreement. Select **Next**, then follow the prompts in the installer.

   The Avaya IC installer exits if you do not agree to the terms of the agreement.

3. In the product installation screen, select **Avaya Rich Client Preparation Wizard 7.1**. Select **Next**, then follow the prompts in the installer.

4. In the Avaya Agent installation folder screen:

   a. Accept the default or type the path to the directory where the agent installer will install the application files on each agent desktop.

   b. Select one of the options in the following table:

Option	Description
Yes, allow agents to choose an alternate folder	Allows agents to decide where to install Avaya Agent.
No, always use the pre-defined folder	Does not allow agents to decide where to install Avaya Agent. If you select this option, Avaya Agent will always be installed in the same folder on the agent desktop.

   Note:
   Do not use `apps` in the installation path for agent desktop applications. If you do, the `-d` parameter cannot locate the apps directory and start the application.

   c. Select **Next**.

5. In the applications screen:

   a. Select one of the following applications for agents who use this configuration:

   - interaction_center
   - listq
   - report_wizard

   If you plan to use Avaya Agent only, select interaction_center.

b. Select one of the options in the following table:

Option	Purpose
Yes, allow Avaya Agent to perform updates automatically	To have Avaya Agent automatically check for and apply updates each time an agent logs in.
No, updates will be done manually	To require agents to apply updates manually when you notify them that an update is available.

c. Select **Next**.

6. In the telephony switch window, select the type of phone switch to use with Avaya Agent.

   If this configuration does not include Telephony, select **None**.

7. Select **Finish** to complete the agent installer.

Copying the server implementation file

The agent installer requires access to the `vesp.imp` server implementation file from the machine that hosts the primary ORB server. You must copy this file to a location where the agent installer has access.

To copy the server implementation file.

1. Navigate to the following directory where the vesp.imp file is located:

   IC_INSTALL_DIR\IC71\etc

2. Copy the `vesp.imp` file to the following directory on the machine that hosts the agent installer:

   IC_INSTALL_DIR\IC71\AgentInstaller\config

Note:
Do not copy the `vesp.imp` file to the *IC_INSTALL_DIR*\IC71\bin directory. The `vesp.imp` file cannot function properly from this directory.

Preparing for installation by agents

As you complete these procedures, refer to the following table for the directories and files in the Avaya Agent installer directory.

Directory	Contents
<*agent_installdir*>\`config`	This directory contains the files that agents install to update Avaya Agent.
<*agent_installdir*>\`update`	This directory contains updates that you make available to the agent applications.
<*agent_installdir*>\`AgentInstaller.exe`	The executable that runs the installation of an agent configuration on the agent desktop.

To prepare an agent installer for installation by agents, perform the steps in the following topics:

1. Testing the agent installer on page 313.
2. Creating installation instructions for agents on page 314.
3. Configuring automatic updates for agent applications on page 315.

Testing the agent installer

You must test the agent installer to make sure that:

- The agent installer works properly.
- The correct installation options are available for agents when they install the agent configuration.
- The agents can access the agent installer through a shared network drive.

Note:
Before you install Avaya IC agent applications, configure all agent workstations with restore points. The agent installer replaces some system files during the installation. If software conflicts arise, restore points allow easy rollback after you uninstall Avaya IC. See the Windows documentation or third-party guides for procedures on enabling such functionality.

If you placed the agent installer on a shared network drive, agents can copy the folders to their machines, or run the agent installer across the network.

If the agents will run the agent installer across the network, they must be able to access the shared network drive from their machines. Agents cannot use the **Run** dialog box on the **Start** menu to run the agent installer.

To test the agent installer:

1. Close down all Windows applications.
2. Use Windows Explorer to navigate to the folder, then double-click **AgentInstaller.exe**.
3. When the Avaya Agent installer opens, read the entire Avaya IC license agreement carefully, then accept the terms of the agreement: Select **Next**, then follow the prompts in the installer.

   The Avaya Agent installer exits if you do not agree to the terms of the agreement.
4. After the Avaya Agent installer completes:
   a. Select **Yes, restart my computer**.
   b. Select **Finish**.

   After the machine reboots, the installer registers all necessary DLLs and OCXs.

Creating installation instructions for agents

Follow these steps to send the URL or directory path and other instructions to all agents who must install a specific agent configuration.

Create instructions for agents that include the following:

- Directory path to the network drive.
- Instructions to close all applications before starting the installation.
- Any other special instructions, such as whether they can select their own installation directory.
- The name of a person to contact if they have problems.

Configuring automatic updates for agent applications

Avaya IC allows you to make different types of updates to agent desktop applications. If you enable more than one type of update, Avaya IC applies the updates in the following order:

1. Language pack updates that install updated language packs for all supported languages.
2. Service pack updates that install updated application files on the agent desktop.
3. Point patch updates that install patch updates to the application files.

Note:
For any type of automatic update to work correctly, the agents must have Read access to the `version.html` file and to the updates. For example, if you install the language pack update on a network server, each agent that logs in must have Read permissions for the directory.

If you enabled Automatic Updates in the Agent Site Preparation wizard:

1. When an agent logs in, Avaya IC reads the `version.html` file from `<agent installdir>\config`.
2. Avaya IC compares the values for the following fields against the values in the agent machine's registry at `HKLM\Software\Avaya\IC\7.1\Agent`:
   - majorversion
   - minorversion
   - patchversion
   - servicepackversion
   - languagepackversion
3. If the following is true, then Avaya IC invokes the automatic updates:
   - Value of `icagent` in the `version.html` file is "1"
   - Values for `majorversion` and `minorversion` in the downloaded `version.html` file on the agent machine match the values in the agent registry
   - Values for `patchversion`, `servicepackversion`, or `languagepackversion` are greater than the values in the agent registry
4. When the automatic update is invoked:
   a. A message is displayed to the agent.
   b. The agent application exits.
   c. Avaya IC updates the agent applications on the agent desktop.

Updating the version.html file

You must update the `version.html` file in the agent installer directory with new values to invoke automatic updates of the agent applications. The `version.html` file contains the following fields. You can update the highlighted section.

```
<versioninfo>
  <remote>
    <client>
      <icagent enabled="1" majorversion="6" minorversion="0" patchversion="0"
      patchpath="%VALUE%" servicepackversion="0" servicepackpath="%VALUE%"
      languagepackversion="0" languagepackpath="%VALUE%"/>
    </client>
    <server>
    </server>
  </remote>
  <local>
    <client>
      <icagent regkeyname="Agent"/>
    </client>
    <server>
    </server>
  </local>
</versioninfo>
```

To update the version.html file:

1. Open the `version.html` file in a text editor.
2. In the `version.html` file, increase the value of one or more of the fields as shown in the following table by one. For example, if the value of a field is currently 1, increase the value to 2.

Field	Purpose
languagepackversion	Increase the value of this field for a language pack update.
servicepackversion	Increase the value of this field for a service pack update.
patchversion	Increase the value of this field for a patch update.

Do not change the `majorversion` and `minorversion` values unless specifically instructed.

3. In the `version.html` file, type the location of the agent installer files in one or more of the following fields. The shared network directory or Web site must be available from the agent desktop.

Field	Purpose
languagepackpath	Type the location in this field for a language pack update.
servicepackversion	Type the location in this field for a service pack update.
patchversion	Type the location in this field for a patch update.

   Avaya IC checks this field before it downloads the files from that location. If the URL or network directory is not valid, an error message is displayed to the agent. After the agent selects **OK**, the agent applications are launched without being updated.

4. Save the `version.html` file.
5. Repeat these steps for every Avaya Agent configuration.

Temporarily disabling automatic updates

In some cases, you may want to disable your Automatic Update option temporarily and allow agents to log in without waiting for the Automatic Update to complete.

To disable Automatic Updates:

1. Open the `version.html` file in the `<agent_installdir>\config` directory.
2. Change the value of the `icagent enabled` field to 0.
3. Save the file.

Configuring the Citrix integration

The Citrix client interface with the seamless window causes issues with the login behavior and the appearance of the Avaya IC agent desktop applications. Avaya provides two tools that prevent these potential issues. For more information, see *IC Installation Planning and Prerequisites*.

You do not need to perform additional steps if the Avaya IC uses the Citrix Web interface.

For this configuration, the Citrix integration requires some additional steps to ensure that the agents can connect to the agent desktop applications and that the agent desktop applications function correctly in the Citrix interface.

This section includes the following topics:

For more detailed information about the Avaya IC tools and the Citrix integration with Avaya IC, see *IC Installation Planning and Prerequisites*.

About the Citrix integration

Avaya IC supports the following methods of publishing applications in Citrix:

- Agent applications accessed as embedded applications in the Citrix Web interface.
- Agent applications accessed in a seamless window in the Citrix client interface.

This section includes the following topics:

Limitations of Citrix integration with Avaya IC

Before you deploy your Avaya IC agent desktop applications on a Citrix server, consider the following limitations:

- Do not host embedded applications and seamless window applications on the same Citrix server. To use both publishing methods in an Avaya IC system, host the embedded applications on a different Citrix server from seamless window applications.
- Do not use the Web browser tool, the Executable tool, or the Avaya Agent INI file (qui.ini) on a Citrix server that hosts embedded applications.

Configuring Citrix integration for seamless window applications

If the Avaya IC system includes access to Avaya IC agent desktop applications through the Citrix client interface in a seamless window, you can configure the Citrix integration in the following ways:

- Configure and run the Web browser tool to access the agent desktop applications.
- Configure and run the Executable tool to access the agent desktop applications.

Installing the agent applications on the Citrix server

To install the agent desktop applications on a Citrix server, follow the procedures in Testing the agent installer on page 313. You do not have to perform any additional steps during the installation.

Depending upon the environment, you may need to adjust the size of the Avaya Agent framework then re-create the agent installer. For more information on how to customize the framework size, see *Avaya Agent Integration*.

Note:
You cannot install the agent desktop applications in a Citrix environment if you do not select the Citrix installation option in the Agent Site Preparation Wizard. For more information, see Running the Avaya Agent site preparation wizard on page 311.

Locating the files for the tools

The files for the tools are in the following directory on the Avaya IC Windows CD-ROM 1:

```
<CD-ROM_drive>\Utils\Citrix
```

Configuring the Avaya Agent INI file

If the Avaya IC system includes agents accessing the Citrix client interface with the seamless window, you must configure the Avaya Agent INI file on each of the Citrix server machines that hosts Avaya IC agent desktop applications.

CAUTION:
Do not create or configure the Avaya Agent INI file on any machine except a Citrix server that an agent will access through the Citrix client interface with the seamless window. The parameter needed for the seamless window can cause undesirable formatting and sizing of the Avaya Agent in other deployments.

To configure the Avaya Agent INI file:

1. In Notepad or another text editor, open a new document.
2. Type the following information into the document:

```
[QConsole]
ResizeDesktop=FALSE
```

3. Save the file with the following name: `qui.ini`
4. Install the file in the Windows installation directory on each Citrix server that hosts Avaya IC agent desktop applications.

   For example, the Windows installation directory is typically either `C:\Winnt` or `C:\Windows`.

Configuring the Avaya IC Web browser tool

To use the Avaya IC Web browser tool to access the agent desktop applications on the Citrix server:

1. Configure the Avaya IC Web browser tool.
2. Copy the files to the machine that hosts the Web server used by Avaya IC.

This section includes the following topics:

Components of the Web browser tool

The Avaya IC Web browser tool includes the files listed in the following table.

File	Description
ActiveX control	`SetupLocalDesktopForAgentViaCitrixCtr.CAB` Digitally signed ActiveX control with unique class ID
HTML access page	`BasicStartAgent.htm` • Specifies the URL for the applications on the Citrix server. • Determines the text that the agent sees on the links. You can customize this text.

Updating the HTML page for the Web browser tool

The following table describes the parameters you can configure and add to the HTML page. The only required parameter is CitrixClientURL.

CAUTION:
Do not delete or change the javascript or other code in the HTML page.

Property	Description
CitrixClientURL	Specifies the location of the startup link for the Avaya IC agent desktop applications on the Citrix server. The value for the property must be a valid URL. For example: `CitrixClientURL="http://`*server_name.com*`/ICAgent/ICAgentAppMode.ica"`
<A href="javascript: Main.SetDesktopForICAgent()"> Start Avaya Agent</A>	Specifies the text on the link that the agent clicks to access the agent desktop applications on the Citrix server.
<A href="javascript: Main.ResetDesktop();window.close ()">EXIT</A>	Specifies the text on the link that the agent clicks to close the interface with the agent desktop applications on the Citrix server.
<A href="javascript: Main.ForcedResetDesktop()">Forc e Reset</A>	Specifies the text on the link that the agent clicks to force a reset of the interface with the agent desktop applications on the Citrix server in the event of a failure.
DontStartMultipleInstancesOfAgent	Determines how the tool acts when an agents logs in to and exits from the tool. This property is optional. You can add it to the HTML page, if desired. For more information, see DontStartMultipleInstancesOfAgent on page 324.

In addition to the parameters in the above table, you can also customize the HTML page as follows:

- Add a corporate logo, a graphic for the background, or otherwise customize the appearance of the HTML page.
- Add one or more of the properties in the Application or Desktop sections of the INI file for the executable tool, as described in Updating the INI file for the Avaya IC executable tool on page 324.

Note:
You cannot add properties from the GUI section of the INI file for the executable tool.

Installing the Web browser tool

To install the Web browser tool:

1. For Avaya IC systems that use Microsoft IIS as the Web server, when you set up and test the Web browser tool, configure a virtual directory in IIS for the Web browser tool.
2. Copy the following files to the machine that hosts the Web server used by the Avaya IC system:
   - `SetupLocalDesktopForAgentViaCitrixCtr.CAB`
   - `BasicStartAgent.htm`

   For example, if the Avaya IC system uses the Microsoft IIS as the Web server, copy the files to the machine that hosts that Web server.

Accessing more than one Citrix server

If the agents need to access the agent desktop applications on more than one Citrix server:

1. For each Citrix server that hosts agent desktop applications, configure the files for a Web browser tool.
2. Install the following files in the same folder on the machine that hosts the Web server:
   - One copy of the ActiveX control: `SetupLocalDesktopForAgentViaCitrixCtr.CAB`
   - For each Citrix server that the agents need to access, one copy of `BasicStartAgent.htm`
3. Create a desktop icon or an Internet Explorer **Favorites** menu for each Web browser tool.

Configuring the executable tool

To use the Avaya IC executable tool to access the agent desktop applications on the Citrix server:

1. Configure the Avaya IC executable tool.
2. Copy the files to either the agent workstations or to a network share that can be accessed by all agents.

This section includes the following topics:

Components of the executable tool

The Avaya IC executable tool includes the files listed in the following table.

File	Description
Executable file	`SetupLocalDesktopForAgentViaCitrix.exe` Launches the dialog box used by agents to access the Citrix server that hosts the agent desktop applications.
INI file	`AgentDesktopCtr.ini` After you update this file: • Specifies the directory path to the agent desktop applications on the Citrix server. • Determines the text on the buttons in the dialog box. You can customize this text to suit the needs of the contact center and to match the corporate style.

Updating the INI file for the Avaya IC executable tool

The following table describes the parameters that you can configure and update in the **AgentDesktopCtr.ini file**. The only required parameter is the directory path for the agent desktop applications on the Citrix server.

Section	Property	Description
APPLICATION	CitrixClientURL	Specifies the location of the startup link for the Avaya IC agent desktop applications on the Citrix server. The value for the property must be a valid URL. For example: `CitrixClientURL="http://`*server_name.com*`/ICAgent/ICAgentAppMode.ica"`
APPLICATION	DontStartMultipleInstances OfAgent	Determines how the tool acts when an agents logs in to and exits from the tool. Default setting is TRUE. When this property is set to TRUE, if an agent logs out of Avaya Agent without exiting from the tool, the agent cannot use the tool to log back in to Avaya Agent. Instead, the agent sees an error which states that Avaya Agent is already running. The agent must follow the correct sequence of steps if you use this setting. For more information, see Sequence for using the Avaya tools for Citrix on page 326. When this property is set to FALSE, if an agent logs out of Avaya Agent without exiting from the tool, the agent can use the tool to log back in to Avaya Agent. The tools will allow the agent to start a "new" instance of Avaya Agent.
APPLICATION	AgentAlreadyRunningMsg	Specifies the message displayed to the agent if an interface is already open and you set DontStartMultipleInstancesOfAgent is set to TRUE. For example, `AgentAlreadyRunningMsg=The Avaya agent was already started`
DESKTOP	ClientBarHight	Controls the desktop area reserved for the bottom of the Avaya Agent framework. The default value is 125 pixels. For example, `ClientBarHight= 151`
DESKTOP	ClientBarWidth	Controls the desktop area reserved for the left side bar of the Avaya Agent framework. The default value is 200 pixels. For example, `ClientBarWidth=201`

Section	Property	Description
GUI	Caption properties	The following caption properties allow you to specify the text for the dialog box: ● `WindowCaption="Avaya Agent Desktop Control (customize me)"` ● `StopButtonCaption="Exit Avaya Agent (customize me)"` ● `StartButtonCaption="Start Avaya Agent (customize me)"` ● `ResetButtonCaption="Reset Desktop (customize me)"` ● `ApplicationFrameCaption="Application Controls (customize me)"` ● `ResetFrameCaption="Emergency Control (customize me)"`
GUI	MinimizeWindowOnLanchedAppStart	Automatically minimizes the interface after the agent accesses the agent desktop applications on the Citrix server. For example, `MinimizeWindowOnLanchedAppStart=TRUE`
GUI	MaximizeWindowOnLanchedAppExit	Automatically maximizes the interface after the agents starts the agent desktop applications on the Citrix server. Only set this property to TRUE if you also set AutoResetOnExit to TRUE. For example, `MaximizeWindowOnLanchedAppExit=TRUE`
GUI	DisableStartButtonAfterFirstClick	Automatically disables the **Start** button on the dialog box after the agent starts the agent desktop applications on the Citrix server. For example, `DisableStartButtonAfterFirstClick=FALSE`
GUI	AskForExitConformation	Ensures that the interface asks the agent to confirm before exiting the interface to the Citrix server. Avaya recommends that you set this property to FALSE if you experience problems with minimizing or maximizing Avaya Agent. For example, `AskForExitConformation=FALSE`

Installing the executable tool

You can install the executable in either of the following locations:

- On a network share that is accessible to all agents who need to use the executable tool.
- Every agent workstation used by an agent who needs to use the executable tool.

To install the executable tool, copy the following files to the desired location:

- `SetupLocalDesktopForAgentViaCitrix.exe`
- `AgentDesktopCtr.ini`

Accessing more than one Citrix server

If an agent needs to access the agent desktop applications on more than one Citrix server:

1. For each Citrix server that hosts agent desktop applications, configure the files for a executable tool.
2. Install a executable tool for each Citrix server in separate folders on the agent workstation.
3. Create a desktop icon or **Start** menu item for each executable tool.

Sequence for using the Avaya tools for Citrix

Agents must use the following sequence when they use either the Web browser tool or the Executable tool. If an agent does not follow this sequence, Avaya Agent and other agent desktop applications may no longer size properly in the Citrix interface.

The proper sequence for using the Avaya tools for Citrix is:

1. Agent starts the Avaya tool:
   - For Web browser tool, agent clicks the **Start** link.
   - For the Executable tool, agent selects **Start**.

   Avaya Agent on the Citrix server starts.
2. Agent logs in to Avaya Agent through Citrix.
3. Agent handles contacts and performs required tasks in Avaya Agent.
4. Agent logs out from Avaya Agent through Citrix.
5. Agent exits the Avaya tool:
   - For Web browser tool, agent clicks the **Exit** link.
   - For Executable tool, agent selects **Exit**.

Chapter 11: Deploying Avaya Agent Web Client

Avaya Agent Web Client is an Avaya Interaction Center (Avaya IC) agent application. When you deploy Avaya Agent Web Client in a contact center:

- Deploy Avaya Agent Web Client software on an application server.
- Do not install Avaya Agent Web Client on an agent workstation.
- Access Avaya Agent Web Client in a Web browser from an agent workstation.

Important:
Read the Avaya IC Readme file and *IC Installation Planning and Prerequisites* before you deploy Avaya Agent Web Client.

For information about how to customize Avaya Agent Web Client, see *Avaya Agent Web Client Customization*.

To deploy Avaya Agent Web Client, perform the following steps:

Before you deploy Avaya Agent Web Client

This section includes information that you need to know and steps you must perform before you deploy Avaya Agent Web Client.

This section includes the following topics:

Prerequisites for Avaya Agent Web Client

Before you deploy the Avaya Agent Web Client, make sure that you have completed the prerequisites for the following:

Avaya IC components

For Avaya IC components, make sure that you have completed the following tasks:

- Install and configure all Avaya IC prerequisites, as described in *IC Installation Planning and Prerequisites*.
- Install and configure Avaya IC, including all media channels and Avaya FTSE.
- Install and configure Avaya Agent on at least one machine for a contact center supervisor, so the supervisor can create global resources or monitor chat sessions.
- Configure agents for Avaya Agent Web Client, as described in Configuring the working directory property on page 299.

Avaya Agent Web Client components

For Avaya Agent Web Client, make sure that you have completed the following tasks with the instructions and configuration recommendations provided by IBM:

- Install IBM WebSphere Application Server (WAS) 6.0 on all machines that will host the Avaya Agent Web Client application.
- Install IBM WAS Application Toolkit (ASTK) with the default configurations on the machines described in *IC Installation Planning and Prerequisites*.
- Install the IBM HTTP server provided with IBM WAS.

Agent workstations

Install and configure the following prerequisites on all agent workstations that will be used to access Avaya Agent Web Client:

- Install Internet Explorer version 6 with the *Sun Java Plug-in* version 1.4.2_08 enabled. Microsoft Internet Explorer will use the Microsoft Java Plug-in by default.
- Install Microsoft DirectX version 9.

  To check the DirectX version, type **`dxdiag`** at a command prompt.
- Configure the Internet Options of Internet Explorer as follows:
  - Security level: Medium if agents use Windows 2003.
  - ActiveX controls: allow to run.

    Avaya recommends that you add the URL of the Avaya Agent Web Client system to the Trusted Sites list.
  - Proxy server settings: Add the fully qualified domain name of the contact center to the proxy **Exceptions** field. For example, you can enter ***`*.company_name.com`*** or ***`*.*.company_name.com`***. You can add multiple names. Check the documentation for your operating system for details.
  - Pop-up blockers: disable or configure to allow pop-ups on the Avaya Agent Web Client URL.

Avaya Agent Web Client deployment requirements for IBM WAS

IBM WAS 6.0 enables you to define profiles that you can use to run multiple servers. Depending upon the needs of the contact center, you can deploy Avaya Agent Web Client in the default profile or in custom profiles.

Do not install any other applications in the same profile as Avaya Agent Web Client.

If you intend to install applications other than Avaya Agent Web Client in the default profile, deploy Avaya Agent Web Client in its own profile.

For more information about profiles and deployment recommendations, see the IBM documentation.

Cautions and tips for Avaya Agent Web Client

This section includes some important cautions and tips that you need to consider when you deploy Avaya Agent Web Client.

This section includes the following topics:

JRE version

Avaya Agent Web Client requires the following versions of JRE:

Avaya Agent Web Client on IBM WAS machines: No special version requirement. Avaya Agent Web Client uses the version of JRE installed with IBM WAS.

Avaya Agent Web Client on agent desktop machines: Requires at least JRE version 1.4.2_08. Avaya Agent Web Client automatically installs that version if JRE is not installed. If an older version of JRE is already installed, the agent must upgrade JRE to the latest version.

Required administrator privileges

The installer for Avaya Agent Web Client requires the same administrator privileges as the installers for the Avaya IC servers and the Avaya IC Design & Administration Tools. For more information, see Required administrator privileges on page 25.

Important:
You can install Avaya Agent Web Client as root or as a user with the same privileges as root. If you install as root, Avaya recommends that you do not run Avaya Agent Web Client as the root user. See section Changing ownership for Avaya Agent Web Client - Solaris and AIX only on page 349 for instructions.

Location of IBM WAS Application Server Kit

Install IBM WAS Application Toolkit (ASTK) on a Windows machine, as described in the following table.

Location of IBM WAS	Location of IBM ASTK
Windows machine	You can install IBM ASTK: • On the same machine as IBM WAS • On a different Windows machine than IBM WAS
Solaris or AIX machine	Install IBM ASTK on a separate Windows machine.

Location of Avaya Agent Web Client

Install Avaya Agent Web Client on all machines that host:

- IBM WAS
- IBM ASTK

Working directory property

The working directory holds Avaya Agent Web Client agent settings for agents, agent resources, and global resources. Avaya Agent Web Client uses agent file persistence to save settings for each agent.

CAUTION:
If you do not use a valid directory path when you configure the working directory, Avaya Agent Web Client will not function properly. Avaya Agent Web Client displays an error message on the Status Bar, and the chat and email channels will be disabled.

For more information about the working directory and recommended settings for that directory, see Configuring the working directory property on page 299.

Re-installing Avaya Agent Web Client

If you need to re-install the Avaya Agent Web Client software, you must remove the existing Avaya Agent Web Client software first. For more information, see Uninstalling Avaya Agent Web Client on page 444.

Changing the web.xml file

Do not change the filter mapping for the Login Filter section in the web.xml file. If you change the filter mapping for the Login Filter, agents will not be able to log in to Avaya Agent Web Client.

Installing the Avaya Agent Web Client Connector

Install the Avaya Agent Web Client Connector on the machine that hosts IBM Websphere, as described in Installing Avaya IC server and administration components on page 29.

Running the Avaya Agent Web Client site preparation wizard

The Avaya Agent preparation wizard installs all Avaya Agent Web Client files required to build the EAR in IBM WebSphere ASTK. You must run the Avaya Agent Web Client preparation wizard on the machine that hosts IBM WebSphere ASTK.

To run the Avaya Agent Web Client site preparation wizard:

1. Insert Avaya IC Release 7.1 CD-ROM 4.

   The Avaya IC installer starts automatically. If you disabled Autorun on the machine, navigate to the Servers directory on the CD-ROM and run `setup.exe`.

2. When the Avaya IC installer opens, read the entire Avaya IC license agreement carefully, then accept the terms of the agreement. Select **Next**, then follow the prompts in the installer.

   The Avaya IC installer exits if you do not agree to the terms of the agreement.

3. In the product installation screen, select **Avaya Agent Web Client Preparation Wizard 7.1**. Select **Next**, then follow the prompts in the installer.

   The Avaya IC installer copies the requested files to the machine. This process can take several minutes.

4. Select **Finish**.

   Important:
   Avaya recommends that users avoid running Avaya IC software as the root user wherever possible for security reasons. For more information, see Changing ownership for Avaya Agent Web Client - Solaris and AIX only on page 349.

Setting up the Java Application Bridge

The Application server for Avaya Agent Web Client uses the Java Application Bridge to communicate with the Avaya IC servers and databases.

This section includes the following topics:

Configuring an agent account for the Java Application Bridge

The Java Application Bridge requires a non-human agent account for Avaya IC. You use this agent account when you create the IBM WAS Application server. This account is the DCO Bridge account.

The Avaya IC seed data includes one non-human agent account for the DCO Bridge. You can use this account for the first Java Application Bridge in the Avaya IC system.

You must create a unique non-human agent account for each additional Java Application Bridge in the Avaya IC system. Avaya recommends that you name each account dcobridge*N*. The agent name can also include the name of the machine that hosts the Java Application Bridge.

Tip:
The following instructions describe how to create additional non-human agent accounts for the Java Application Bridge. If you use the account in the Avaya IC seed data, you should double-click that agent account and complete Step 5 below.

To configure an agent account for the Java Application Bridge:

1. In IC Manager, select the **Agent** tab.
2. Expand the **DefaultTenant** node in the left pane.

   If you want to create this agent account in a different tenant, expand that node in the left pane instead of **DefaultTenant**.
3. Select **Agent** > **New**.

4. Select the **General** tab and complete the following fields:

Field	Recommended entry
First Name	dcobridge*N* (for example, dcobridge2)
Last Name	dcobridge*N* (for example, dcobridge2)
Preferred Name	dcobridge*N* (for example, dcobridge2)
Employee ID	dcobridge*N* (for example, dcobridge2)
Login ID	dcobridge*N* (for example, dcobridge2)
Domain	The same user domain as the Java Application Bridge that will use this agent account. For example, User1.
Task Load	0
Task Ceiling	0
Site	DefaultSite

5. Select the **Security** tab and complete the fields as shown in the following table:

Field	Recommended entry
Password	Enter a password for this account. **Tip:** Avaya recommends that you change the password for the pre-defined Java Application Bridge account.
Confirm	Re-enter the password for this account.
Force password change on login	Clear this field. Do not check this field for non-human Avaya IC users
Disable login	Do not check this field.
Role	Check the **Agent** role. **Note:** Do not check any of the other roles.

6. Select **OK**.

Creating a Java Application Bridge

The Java Application Bridge is not a true Avaya IC server. The Java Application Bridge impersonates each agent who logs in to the Avaya Agent Web Client. When the Java Application Bridge makes a request for an agent, the Java Application Bridge mirrors the domain structure of the agent.

You must create a Java application bridge for each IBM WAS that hosts an Avaya Agent Web Client application.

For example, if your system includes:

- One IBM WAS server, create one Java application bridge.
- Two IBM WAS servers on different server machines, create two Java application bridges.
- Two IBM WAS servers on different nodes of the same server machine, create two Java application bridges.

To configure a Java application bridge in Avaya IC:

1. In IC Manager, select the **Server** tab.
2. Select **Server** > **New**.
3. Select **JavaAppBridge** from the list of servers. Select **OK**.

4. Select the **General** tab and complete the fields shown in the following table.

Field	Recommended entry	Notes
Name	Enter a name for the Java Application Bridge.	Include the name of the machine that hosts the IBM WAS application server to identify the location of the JavaAppBridge.
Domain	Select an Avaya IC User domain for the Java Application Bridge from the drop-down list.	For example, select `User1` from the drop-down list. Assign the Java Application Bridge to the same User domain as the majority of the agents who use Avaya Agent Web Client. If the Avaya IC system includes Avaya Agent Web Client at different sites, use the User domain that contains the majority of agents at that site. If the Avaya IC system includes agents in multiple domains, you do not need a Java Application Bridge in each User domain. Ensure that the domain with the Java Application Bridge fails over to the following domains: • Itself • The Default domain • All domains with an ADU server
Host	Enter the IP address of the machine that hosts IBM WAS.	
Port	Enter a port assignment for the Java Application Bridge.	You can use any available port in the 9000 range for the Java Application Bridge. If you do not host other Avaya IC servers on the same machine as IBM WAS, Avaya recommends that you use port 9002.

Field	Recommended entry	Notes
Directory	Enter the path to the `etc` directory for Avaya Agent Web Client.	For example enter: *`IC_INSTALL_DIR`*`\IC71\etc` where *`IC_INSTALL_DIR`* is the path to this directory on the IBM WAS machine. For example, if you used the default, the path would be: `C:\Program Files\Avaya\IC71\etc`
Executable	Enter `jabsrv`	Leave the default entry. **Tip:** This entry exists because this is a required field in IC Manager. No separate executable exists.

5. Record the **Name** value for the Java Application Bridge for use in Setting up the JACL scripts on page 342.
6. Select the **JavaAppBridge** tab and complete the fields shown in the following table.

Field	Recommended entry	Notes
IC User	Enter the name of the agent account for this Java Application Bridge server.	Use the agent account that you created in Configuring an agent account for the Java Application Bridge on page 333. For example, enter dcobridge1.
IC Password	Enter the password associated with the agent account.	

7. Select **OK**.

Important:
Do not start the Java Application Bridge. When you start IBM WAS Application server, that server starts the Java Application Bridge.

Setting up UNC to UNIX mapping - Solaris and AIX only

The **UNC to UNIX Path Mapping** field of the Java Application Bridge maps the UNC address of a network folder which holds files that agents can attach to resources with the UNIX path that IBM WAS uses to access the folder.

Tip:
You do not need to map the working directory for the IBM WAS application server. However, you can map this directory if desired.

This section includes the following topics:

Prerequisites for UNC to UNIX path mapping

You must perform the following steps before you configure UNC to UNIX path mapping:

1. Install Samba (or an equivalent product) on the UNIX machine that hosts the attachments directory to make the folders and files accessible from a Windows machine.
2. Configure the UNIX shares for Samba (or an equivalent product) as follows:
   a. Ensure that the name of each share is the same as the UNIX folder that it shares.
   b. Ensure that all agents have Read permissions for the share. You can give the agents additional permissions for the share, if desired.
   c. Ensure that the UNIX user under which Avaya Agent Web Client runs has the same permissions for the UNIX directory as agents have for that directory's share.

Requirements for entries in the UNC to UNIX Path Mapping field

Follow these requirements when you enter information in the **UNC to UNIX Path Mapping** field:

- You can only create one entry for each machine. The Java Application Bridge only considers the first entry for a given machine in the table. All subsequent entries are ignored.
- You can only use the format `\\machine_name` in the **UNC Machine Name** column.
- You can only use valid UNIX paths in the **UNIX Path** column.

Accessing multiple folders on one machine

You cannot add multiple entries for a machine in the UNC to UNIX Path Mapping field. If you want to store files for attachments in multiple folders on the same machine:

1. Organize the folders so that they are all subfolders of a single folder. For example, create an attachments folder with subfolders titled printers, ink, and cables.
2. Use Samba (or an equivalent product to configure the UNIX shares named printers, ink, and cables for the subfolders of the attachments folder.
3. Give agents Read permissions, at a minimum, for the shares.
4. In the **UNC Machine Name** column, enter the name of the machine where the attachments folder is located. For example, `\\sunbox1`.
5. In the **UNIX Path** column, enter the UNIX path for the `attachments` directory. For example, `/opt/attachments`.

Examples of entries in the UNC to UNIX Path Mapping field

The following table shows a series of entries in the UNC to UNIX Path Mapping field, including both valid and invalid entries.

UNC to UNIX Path Mapping entry		**Description**
UNC Machine Name	**UNIX Path**	
\\sunbox1	/opt/data/attachments	A valid entry in both columns.
\\sunbox2\	/opt/data/attachments	An invalid entry in the **UNC Machine Name** column. The Java Application Bridge cannot accept an entry that ends with a backslash.
\\sunbox1	/opt/data	Entry will be ignored as there is already an entry for this UNC machine name.
\\sunbox3	/	A valid entry in both columns. The **UNIX Path** entry points to the root directory on the machine.
\\sunbox4		An invalid entry in the UNIX Path column. For root directory, enter /, as shown in the above entry.

Configuring UNC to UNIX Path Mapping

The UNC to UNIX Path Mapping field of the Java Application Bridge maps the UNC address of a network folder which holds files that agents can attach to resources with the UNIX path that IBM WAS uses to access the folder.

When you restart the IBM WAS application server, the entries in the **UNC to UNIX Path Mapping** field are validated. Alarms are generated and added to the logs if an error is detected. For more information, see Troubleshooting the Java Application Bridge on page 430.

Note:
Do not complete this field if IBM WAS is hosted on a Windows machine.

To configure UNC to UNIX Path Mapping for IBM WAS on Solaris or AIX:

1. If necessary, double-click the Java Application Bridge in the **Server** tab of IC Manager.
2. Select the **JavaAppBridge** tab.
3. select the Ellipsis (**...**) button next to the **UNC to UNIX Path Mapping** field.
4. In the **UNC to UNIX Path Mapping** dialog box:
   a. Select **New**.
   b. In the **UNC Machine Name** column, enter the name of the machine that hosts the attachments folder in UNC format. For example, enter `\\testbox`
   c. In the **UNIX Path** column, enter the path that the IBM WAS machine uses to access the attachments folder. For example, enter `/opt/data/attachments`
   d. After you create entries for each attachments folder, select **OK**.
   e. Select **OK** to close the Server Editor.
5. Restart the Avaya Agent Web Client application server in IBM WAS.

Packaging the Web application

To package the Avaya Agent Web Client Web application:

1. In IBM ASTK, right-click an empty area in the **Navigator** pane and select **Import...**.
2. In the **Import** dialog box:
   a. Select **Existing Project into Workspace**.
   b. Select **Next**.

3. In the **Import Project from File System** dialog box:
   a. Browse to the *IC_INSTALL_DIR*\IC71\WebClient\web directory.

      where *IC_INSTALL_DIR*\IC71\ is the location where you installed the Avaya Agent Web Client software on the Windows machine that hosts IBM ASTK.

   b. Verify that the project name has been automatically entered by the system.
4. Select **OK**.
5. Select **Finish**.
6. Repeat Steps 1 through 5, using the following location in step 3a:

   IC_INSTALL_DIR\IC71\WebClient\application
7. In the **Navigator** pane of IBM ASTK, select the **application** project.
8. Right-click on **application** and select **Export**.
9. In the **Export** window, select **EAR File** and follow the prompts.

Configuring IBM WAS server

You must perform all of the procedures in this section to ensure that the IBM WAS application server can deploy and run Avaya Agent Web Client.

Important:
Before you configure the IBM WAS server for Avaya Agent Web Client, see the information in Avaya Agent Web Client deployment requirements for IBM WAS on page 329.

Perform all of the procedures in this section in the same order as the following topics:

Setting up the JACL scripts

You need to customize and use the following JACL scripts to configure IBM WAS for Avaya Agent Web Client:

- AAWCConfigure.jacl
- AAWCParameters.jacl

To set up the JACL scripts:

1. Copy the JACL scripts listed above from *IC_INSTALL_DIR*/IC71/config to the following directory: *WAS_INSTALL_ROOT*/AppServer/profiles/*default*/bin

   where *WAS_INSTALL_ROOT* is the directory path where you installed IBM WAS and *default* is the profile name.

2. In a text editor, open AAWCParameters.jacl.

   The contents of the file should include the following text:

```
set ServerName {server1}

set JavaAppBridgeName {JavaAppBridgeName_mymachine}
set AvayaICHome {C:/Avaya/IC71}
set WebClientURL {http://mymachine.mycompany.com:9080}
```

3. Customize the values in AAWCParameters.jacl as described in the following table.

   Tip:
   When you customize the values in the file, do not delete the brackets that surround the default values.

Parameter name	Parameter value
ServerName	Default value: server1 Enter the name of the IBM WAS application server that will host the Avaya Agent Web Client application.
JavaAppBridgeName	Default value: JavaAppBridgeName_mymachine Enter the name of the Java Application Bridge that you created in Creating a Java Application Bridge on page 335.

Parameter name	Parameter value
AvayaICHome	Default value: C:/Avaya/IC71 Enter the path to the directory where you installed the Avaya Agent Web Client software. **Note:** This value is case-sensitive. You must use the exact case of the directories.
WebClientURL	Default value: http://mymachine.mycompany.com:9080 Enter the URL for Avaya Agent Web Client in one of the following formats: *HTTP_protocol*://*WAS_SERVER_NAME*:*port* where *port* is an available port that can be used to access the Avaya Agent Web Client application. For example, enter `http://testbox.domain.com:9080` Or for an SSL implementation, enter `https://testbox.domain.com:9080` **Note:** This value is case-sensitive.

4. Save AAWCParameters.jacl.

Verifying the environment variable

To verify the environment variable, perform the task described in the following table:

Operating system	Procedure
Windows	Review the Windows environment variables and verify that the Avaya IC installer added the following to the Path variable: *IC_INSTALL_DIR*\IC71\bin where *IC_INSTALL_DIR*\IC71\ is the location where you installed the Avaya Agent Web Client software. If necessary, add the directory path for Avaya Agent Web Client to the Path variable.
Solaris and AIX	Verify that the Avaya IC installer modified *IC_INSTALL_DIR*/IC71/bin/aawc.sh to set the var AVAYA_IC_HOME. If necessary, set the value of the var AVAYA_IC_HOME to *IC_INSTALL_DIR*/IC71/ where *IC_INSTALL_DIR*/IC71/ is the location where you installed the Avaya Agent Web Client software.

Applying the JACL scripts

You need to apply the JACL scripts on each IBM WAS instance that will host an Avaya Agent Web Client application.

Tip:
If you do not save the changes made by the JACL scripts, those changes can cause conflicts with Administrative user changes in the IBM WAS Administrative Console.

This section includes the following topics:

Applying the JACL scripts on Windows

To apply the JACL scripts on Windows:

1. In a Command Prompt window, navigate to the following directory:

   WAS_INSTALL_ROOT\AppServer\profiles*default*\bin

   where *WAS_INSTALL_ROOT* is the directory path where you installed IBM WAS and *default* is the profile name.

2. Execute the following command:

   startServer server1

   where server1 is the name of the IBM WAS server that hosts the IBM WAS Administrative Console.

3. When that command is successful, execute the following command:

   wsadmin -f AAWCConfigure.jacl

Applying the JACL scripts on Solaris or AIX

To apply the JACL scripts on Solaris and AIX:

1. Copy aawc.sh from *IC_INSTALL_DIR*/IC71/bin to

   /*WAS_INSTALL_ROOT*/AppServer/profiles/*default*/bin

   where *WAS_INSTALL_ROOT* is the directory path where you installed IBM WAS and *default* is the profile name.

2. Navigate to the following directory:

   /*WAS_INSTALL_ROOT*/AppServer/profiles/*default*/bin

3. Execute the following command:

   `sh aawc.sh start server1`

   where `server1` is the name of the IBM WAS server that hosts the IBM WAS Administrative Console.

4. When that command is successful, execute the following command:

   `wsadmin.sh -f AAWCConfigure.jacl`

Verifying the settings created by the JACL scripts

Tip:
If the IBM WAS Administrative Console advises that changes made by the JACL scripts can cause conflicts with Administrative user changes, select the option that saves the changes.

To verify the settings created by the JACL scripts:

1. In the left pane of the IBM WAS Administrative Console, select **Servers** > **Application Servers** > ***WAS_APP_SERVER***.

   where WAS_APP_SERVER is the name of the IBM WAS application server that hosts Avaya Agent Web Client. For example, Server1.

2. Select the link for the ***`WAS_APP_Server`***.
3. Select **Java and Process Management** under the **Server Infrastructure** heading.
4. Select **Process Definition**.
5. Select **Java Virtual Machine** under the **Additional Properties** heading.
6. Select **Custom Properties** under the **Additional Properties** heading.
7. Verify the values of the following properties:
   - avaya.ic.home
   - avaya.ic.vesp.javaappbridge.name
   - avaya.ic.webclient.url
8. In the message frame at the top of the page, select **Save or Discard**.
9. On the next page, select **Save**.
10. On the next page, retain the default values displayed on page and click on "Save" button again.

Deploying the application EAR file

When you deploy the Avaya Agent Web Client application, Avaya highly recommends that you pre-compile the JSP files used by Avaya Agent Web Client. If you pre-compile the JSP files, the IBM WAS server does not need to access and compile the JSPs when the Avaya Agent Web Client application is run for the first time after deployment.

If you do not pre-compile the JSP files, some Avaya Agent Web Client components can take significantly longer to open for the first agent to log in than for all subsequent agents.

For more information on JSP pre-compilation, see the IBM WAS documentation.

To deploy the application EAR file:

1. In the left pane of the IBM WAS Administrative Console, select **Applications** > **Install New Application**.
2. In the first **Preparing for the application installation** page:
   a. Select **Browse** and navigate to the location of the **AvayaAgentWebClient.ear** file.

      You created the EAR file in Packaging the Web application on page 340.

   b. Select **Next**.
3. In the second **Preparing for the application installation** page:
   a. Accept the default settings.
   b. Select **Next**.
4. In the third **Preparing for the application installation** page, select **Next**.
5. In the **Install new application** page:
   a. Select and check the **Pre-compile JSP** field.
   b. In the **Application name** field, enter a name for the application.

      For example, enter **AvayaAgentWebClient**.

   c. Accept defaults for all other fields.
   d. Select **Next**.
6. In the **Map modules to application servers** page:
   a. In the **Clusters and Servers** box, select the following:
      - The name of the IBM WAS server that hosts Avaya Agent Web Client.
      - All Web servers that will route incoming http requests to this Application server.

        If you did not configure a Web server in IBM WAS, you may not see any other Web servers in the **Clusters and Servers** box.

   b. In the **Module** table, check the boxes for all of the modules.

c. Select **Apply** above the **Module** table.

d. Verify that the IBM WAS server name in the **Server** column of the **Module** table matches the IBM WAS server that hosts Avaya Agent Web Client.

   If the IBM WAS server names do not match, repeat Step 6.

e. Select **Next**.

7. In the **Map virtual hosts for web modules** page:

   a. Select and place a checkmark on **Avaya IC Web Application, Web module**.

   b. Accept the default values for all other fields.

   c. Select **Next**.

8. Select **Finish** on the **Summary** page.

   The IBM WAS Administrative Console installs the application.

9. Save the changes to the IBM WAS Master Configuration:

   a. Select **Save to the Master Configuration**.

   b. On the next page, select **Save**.

10. Restart the IBM WAS application server for Avaya Agent Web Client, as described in Starting and stopping Avaya Agent Web Client on page 350.

Note:
The IBM WAS Administrative Console may show the IBM WAS application status as Unavailable. This status is acceptable at this stage in the deployment.

Starting the HTTP server

Note:
You must start Avaya Agent Web Client before you perform the steps in this section. For more information, see Starting and stopping Avaya Agent Web Client on page 350.

This section includes the following topics:

Starting the HTTP server on Windows

For the HTTP server to run correctly on a Windows machine, you must stop the service for Internet Information Services.

To start the HTTP server on a Windows machine:

1. On the machine that hosts the IBM HTTP server used by IBM WAS, open the Windows Services panel.
2. For the **World Wide Web Publishing Service**:
   a. Set the startup type to **Manual**.
   b. Stop the service.
3. For the **IIS Administrative Service**:
   a. Set the startup type to **Manual**.
   b. Stop the service.
4. Start the service for IBM HTTP Server.

Starting the HTTP server on Solaris

For the HTTP server to run correctly on a Solaris machine, you must stop the processes for the Sun One HTTP server.

To start the HTTP server on a Solaris machine:

1. On the machine that hosts the IBM HTTP server used by IBM WAS, stop the following processes for the Sun One HTTP server:
   - httpd
   - webservd
2. Navigate to the `IC_INSTALL_DIR/IC71/bin` directory.
3. Enter the following command to start IBM HTTP Server:

   ```
   ./httpserver.sh start
   ```

Starting the HTTP server on AIX

To start the HTTP server on an AIX machine:

1. On the machine that hosts the IBM HTTP server used by IBM WAS, navigate to the *IC_INSTALL_DIR*/IC71/bin directory.
2. Enter the following command to start IBM HTTP Server:

   ./httpserver.sh start

Changing ownership for Avaya Agent Web Client - Solaris and AIX only

If you installed Avaya Agent Web Client as the root user, change ownership for Avaya Agent Web Client and the IBM WAS application server to run under a non-root user.

Important:
Avaya recommends that users avoid running Avaya IC software as the root user wherever possible for security reasons. Create a user for the Avaya IC system before you perform these steps. For more information, see *IC Installation Planning and Prerequisites*.

This section includes the following topics:

Changing IBM WAS to run under non-root user

To run IBM WAS under a non-root user:

1. For IBM WAS, see the IBM WAS documentation for information about how to run an application server with a non-root user ID.
2. For a Deployment Manager configuration, start the Node Agent with the non-root user. If you start as root, the application cannot write to the log files and will not start.

Tip:
If you have already run the application as a root user, you must change the ownership of all files to the non-root user ID.

Changing Avaya Agent Web Client to run under non-root user

For specific steps to change ownership of a directory or directory hierarchy, see Changing ownership of the Avaya IC directories and files on page 38.

To change Avaya Agent Web Client to run under non-root user:

1. Set the owner of the Avaya IC directory where you installed the Avaya Agent Web Client software to the non-root user and group.
2. Ensure that the Avaya Agent Web Client application has the following permissions for the Avaya Agent Web Client installation directory hierarchies:
   - Read
   - Write
   - Execute
3. Set the owner of the working directory for Avaya Agent Web Client to the same non-root user and group. For more information about the working directory and recommended settings for that directory, see Configuring the working directory property on page 299.

Starting and stopping Avaya Agent Web Client

This section includes the following topics:

Starting and stopping Avaya Agent Web Client on Windows

By default, IBM WAS only provides menu shortcuts to start and stop the default application server (server1). You can create shortcuts on the Windows desktop to start and stop IBM WAS application server that you created for Avaya Agent Web Client.

To start and stop IBM WAS application server for Avaya Agent Web Client on Windows:

1. From the Windows Program menu, right-click on the following IBM Websphere menu items and copy the shortcuts to the desktop:
   - Start the server
   - Stop the server
2. For each shortcut on the Windows desktop:
   a. Right-click the shortcut and select **Properties**.
   b. If necessary, replace the information in the **Target** field with the correct profile and server information for Avaya Agent Web Client.
   c. Select **OK**.
3. Double-click the appropriate shortcut to stop and start the IBM WAS server.
4. Verify that the IBM WAS server for Avaya Agent Web Client has started or stopped correctly by reviewing the log files in the following directory: `*WAS_INSTALL_ROOT*\AppServer\profiles\*default*\logs` directory

   where `*WAS_INSTALL_ROOT*` is the directory path where you installed IBM WAS and `*default*` is the profile name.

   For example, to verify that a server has started correctly, review the following files:
   - startServer.log
   - SystemOut.log
5. After you start Avaya Agent Web Client, verify in IC Manager that the Java Application Bridge is running.

Starting and stopping Avaya Agent Web Client on Solaris and AIX

CAUTION:
Always use the `aawc.sh` script to start the IBM WAS application server that hosts the Avaya Agent Web Client application, even in a clustered IBM WAS environment. Do not use the IBM WAS Administrative Console, or the `startServer.sh` script provided with IBM WAS.

Avaya Agent Web Client includes an `aawc.sh` script that sets the library path variable for loading native libraries and that you use to start or stop:

- IBM WAS application server that hosts the Avaya Agent Web Client application on Solaris or AIX
- Avaya Agent Web Client application

To start and stop Avaya Agent Web Client on Solaris or AIX:

1. Navigate to `/WAS_INSTALL_ROOT/AppServer/profiles/default/bin`

   where *WAS_INSTALL_ROOT* is the directory path where you installed IBM WAS and *default* is the profile name.

2. Execute the following command:

   sh aawc.sh [start | stop] *WAS_SERVER*

   where ***WAS_SERVER*** is the name of the IBM WAS application server that you hosts Avaya Agent Web Client.

3. Verify that the IBM WAS server for Avaya Agent Web Client has started or stopped correctly by reviewing the log files in the following directory: `/WAS_INSTALL_ROOT/AppServer/profiles/default/logs` directory

   where *WAS_INSTALL_ROOT* is the directory path where you installed IBM WAS and *default* is the profile name.

   For example, to verify that a server has started correctly, review the following files:

   - startServer.log
   - SystemOut.log

4. After you start Avaya Agent Web Client, verify in IC Manager that the Java Application Bridge is running.

Disabling autostart in a clustered IBM WAS environment - Solaris and AIX only

By default, when an IBM WAS process fails, IBM WAS starts another process automatically. This auto-start cannot start Avaya Agent Web Client cleanly. You must start Avaya Agent Web Client with the `aawc.sh` script, as described in Starting and stopping Avaya Agent Web Client on Solaris and AIX on page 352.

To disable autostart in a clustered environment:

1. In the IBM WAS Deployment Manager Administration Console, select **Application servers** > ***WAS_APP_SERVER*** > **Java And Process Management** > **Process Definition** > **Monitoring Policy**.

   where WAS_APP_SERVER is the name of the IBM WAS application server that hosts Avaya Agent Web Client. For example, Server1.

2. Uncheck the **Automatic restart** box.
3. Repeat steps 1 and 2 for each member server of the IBM WAS cluster.
4. Restart each member server cluster that you modified.
5. Restart the node-agent on each machine that hosts an Avaya Agent Web Client application server, as follows:

   ***WAS_INSTALL_ROOT*\AppServer\profiles*PROFILE_NAME*\bin\stopNode**

   ***WAS_INSTALL_ROOT*\AppServer\profiles*PROFILE_NAME*\bin\startNode**

   where WAS_INSTALL_ROOT is the directory path where you installed IBM WAS and PROFILE_NAME is the name of profile.

Testing Avaya Agent Web Client

Note:
For information about Avaya Agent Web Client log files and troubleshooting issues, see *IC Administration Volume 1: Servers & Domains*.

To test Avaya Agent Web Client:

1. In a Web browser, navigate to the following URL:

   `http://`*`WAS_SERVER_NAME`*`/avaya/agent/login.jsp`

   where ***`WAS_SERVER_NAME`*** is the fully qualified domain name of the machine that hosts IBM WAS server.

2. Log in to Avaya Agent Web Client with the login ID and password of an agent in the Avaya IC system.

Deploying Avaya Agent Web Client in an IBM WAS clustered environment (optional)

This section includes two methods that you can use to configure Avaya Agent Web Client on an IBM WAS cluster. The first method provides a completely manual setup. The second method uses the JACL scripts installed with Avaya Agent Web Client.

Depending upon your IBM WAS cluster setup, you can configure Avaya Agent Web Client manually or use the JACL scripts provided with Avaya IC.

This section includes the following topics:

Prerequisites for an IBM WAS clustered environment deployment

Perform the following steps before you configure Avaya Agent Web Client in an IBM WAS clustered environment:

1. Review the deployment scenarios for a clustered environment in *IC Installation Planning and Prerequisites*.
2. Set up the IBM WAS clustered environment, including the IBM WAS Network Deployment Manager software. For more information, see the documentation provided by IBM.
3. Install Avaya Agent Web Client site preparation wizard on the IBM ASTK workstation machine.
4. Install the Avaya Agent Web Client Connector on each machine that hosts IBM Websphere, as described in Installing Avaya IC server and administration components on page 29.
5. Run the Avaya Agent Web Client preparation wizard on the machine that hosts IBM WebSphere ASTK, as described in Running the Avaya Agent Web Client site preparation wizard on page 332.
6. Set up the required Java Application Bridges for your deployment, as described in Setting up the Java Application Bridge on page 333.
7. Prepare the Avaya Agent Web Client Web application, as described in Packaging the Web application on page 340.

Configuring Avaya Agent Web Client on the IBM WAS cluster

To configure Avaya Agent Web Client on the IBM WAS cluster, perform one of the following:

- Setting up the JAAS related parameters on page 355
- Configuring the cluster members to run Avaya Agent Web Client on page 356

Setting up the JAAS related parameters

To set up the JAAS-related parameters:

1. Open the IBM WAS Administrative Console connected to the Deployment Manager.
2. On the **LHS** tab, select **Security** > **Global Security**.
3. On the **RHS** page under the **Authentication** header, select **JAAS Configuration** > **Application Logins**.
4. Select **New**.
5. For **CUP**, enter the Alias name, then select **Apply**.

6. Under the **Additional Properties** header, select **JAAS Login Modules**.
7. Select **New** to create a new JAAS Login Module.
8. In the **Module Class Name** field, enter **com.avaya.security.auth.CUPLoginModule**.
9. Select the **Use Login Module Proxy** check box.
10. Select **OK**.
11. Save the changes.

Configuring the cluster members to run Avaya Agent Web Client

The following procedure assumes that you have already created an IBM WAS cluster to host Avaya Agent Web Client.

To configure the cluster members to run Avaya Agent Web Client:

1. Open the IBM WAS Administrative Console connected to the Deployment Manager.
2. On the **LHS** tab, select **Servers** > **Application Server**.
3. On the **RHS** page, select an application server that belongs to the Avaya Agent Web Client application cluster.
4. Under the **Server Infrastructure** header, expand the **Java and Process Management** link and select **Process definition**.
5. Under the **Additional Properties** header, select **Java Virtual Machine**.
6. Under the **Additional Properties** header, select **Custom Properties**.
7. Select **New** button and enter the properties in the following table.

Property name	Value
JavaAppBridgeName	Enter the name of the Java Application Bridge that you created in Creating a Java Application Bridge on page 335.

Property name	Value
AvayaICHome	Enter the path to the directory where you installed the Avaya Agent Web Client software. **Note:** This value is case-sensitive. You must use the exact case of the directories.

WebClientURL	Enter the URL for Avaya Agent Web Client in one of the following formats:
	HTTP_protocol://*WAS_SERVER_NAME*:*port*
	where *port* is an available port that can be used to access the Avaya Agent Web Client application.
	For example, enter
	`http://testbox.domain.com:9080`
	Or for an SSL implementation, enter
	`https://testbox.domain.com:9080`
	Note: This value is case-sensitive.

8. Repeat Steps 3 through 7 for each member of the cluster.
9. Restart each member server of the cluster so that these applied settings become effective.

Configuring Avaya Agent Web Client on the IBM WAS cluster with the JACL scripts

Use the instructions in this section only if you have not already created an IBM WAS cluster for Avaya Agent Web Client, and if you do not have an IBM WAS cluster for non-Avaya applications. If either of these conditions are true, follow the manual steps in Configuring Avaya Agent Web Client on the IBM WAS cluster on page 355.

Important:
You can configure Avaya Agent Web Client with the JACL scripts only if you have single federated node to a given Cell. If you have more than one node with the same server name federated to the cell, the JACL scripts will fail. If you do not want to unfederate additional nodes so that the JACL scripts can run successfully, see Configuring Avaya Agent Web Client on the IBM WAS cluster on page 355,

To configure Avaya Agent Web Client on the IBM WAS cluster with the JACL scripts:

1. Federating and adding a node to an IBM WAS cell on page 358
2. Setting up the JACL scripts on page 358
3. Running the JACL scripts on page 360
4. Creating the Avaya Agent Web Client application cluster on page 360

Federating and adding a node to an IBM WAS cell

This section describes how to federate a node and add it to an IBM WAS cell in the IBM WAS Administrative Console. You can also use the wsadmin script to perform these steps.

To federate and add a node to an IBM WAS cell:

1. Make sure that the IBM WAS server with the node you want to federate is up and running.
2. Open the IBM WAS Administrative Console connected to the Deployment Manager.
3. On the **LHS** tab, select **System Administration** > **Nodes**.
4. On the **RHS** page, select **Add Node**.
5. On the next page, select **Next**.

   By default, **Managed Node** is selected.
6. In the **Host** field, enter the Host name.
7. Enter the appropriate SOAP port.

   The default SOAP port is 8880.
8. Select **OK** to federate a node to the cell.

Setting up the JACL scripts

To setup the JACL scripts:

1. Copy the AAWCConfigure.jacl and AAWCParameters.jacl scripts from *IC_INSTALL_DIR*/IC71/config to the following directory: *WAS_INSTALL_ROOT*/AppServer/profiles/*deployment_manager_profile_name*/bin

   where *WAS_INSTALL_ROOT* is the directory path where you installed IBM WAS and *deployment_manager_profile_name* is the Deployment Manager profile name.
2. In a text editor, open AAWCParameters.jacl.

   The contents of the file should include the following text:

```
set ServerName {server1}

set JavaAppBridgeName {JavaAppBridgeName_mymachine}
set AvayaICHome {C:/Avaya/IC71}
set WebClientURL {http://mymachine.mycompany.com:9080}
```

3. Customize the values in AAWCParameters.jacl for the node as described in the following table.

Tip:
When you customize the values in the file, do not delete the brackets that surround the default values.

Parameter name	Parameter value
ServerName	Default value: server1 Enter the name of the IBM WAS application server that will host the Avaya Agent Web Client application.
JavaAppBridgeName	Default value: JavaAppBridgeName_mymachine Enter the name of the Java Application Bridge that you created in Creating a Java Application Bridge on page 335.
AvayaICHome	Default value: C:/Avaya/IC71 Enter the path to the directory where you installed the Avaya Agent Web Client software. **Note:** This value is case-sensitive. You must use the exact case of the directories.
WebClientURL	Default value: http://mymachine.mycompany.com:9080 Enter the URL for Avaya Agent Web Client in one of the following formats: *HTTP_protocol*://*WAS_SERVER_NAME*:*port* where `port` is an available port that can be used to access the Avaya Agent Web Client application. For example, enter `http://testbox.domain.com:9080` Or for an SSL implementation, enter `https://testbox.domain.com:9080` **Note:** This value is case-sensitive.

4. Save AAWCParameters.jacl.

Running the JACL scripts

To run the JACL script:

1. Navigate to the following directory: *WAS_INSTALL_ROOT*/`AppServer/profiles/`*`deployment_manager_profile_name`*`/bin`

   where *`WAS_INSTALL_ROOT`* is the directory path where you installed IBM WAS and *`deployment_manager_profile_name`* is the Deployment Manager profile name.

2. Execute the following command:

   `wsadmin -f AAWCConfigure.jacl`

   For more information, see Applying the JACL scripts on page 344.

Creating the Avaya Agent Web Client application cluster

You create the Avaya Agent Web Client application cluster with the federated node that you added to the cell in Federating and adding a node to an IBM WAS cell on page 358.

To create the Avaya Agent Web Client application cluster:

1. Open the IBM WAS Administrative Console connected to the Deployment Manager.
2. On the **LHS** tab, select **Servers** > **Cluster**.
3. On the **RHS** page, select **New**.
4. On the next page, enter the cluster name and select **Next**.
5. Enter the member name and select **Existing Application Server**.
6. Select the application server that you federated to the cell in Federating and adding a node to an IBM WAS cell on page 358.

   This server is used as a template to create subsequent cluster members. All JVM custom properties that you applied to the first cluster member through the JACL scripts are replicated to all new cluster members.

7. Add more cluster members to the cluster as needed.
8. For each additional cluster member, update the JVM custom properties, as described in Configuring the cluster members to run Avaya Agent Web Client on page 356.
9. Restart the cluster so that these applied settings become effective.

Configuring SSL security for Avaya Agent Web Client (optional)

You can configure Avaya Agent Web Client to work with Secure Sockets Layer (SSL) to provide secure Internet sessions. SSL is optional.

To configure SSL security for Avaya Agent Web Client:

1. Configure IBM WAS for SSL as described in the documentation provided by IBM. For example, see *IBM WebSphere v6.0 Security; Websphere handbook series*.
2. Make sure that IBM WAS includes an SSL-enabled port. For example, by default, IBM WAS 6.0 assigns port 9443 to be the SSL-enabled port.
3. *For IBM WAS on Solaris only*:
   a. In the IBM WAS Administrative console, select **Servers** > **Application Servers** > **WAS_APP_SERVER** > **Configuration Tab** > **Server Infrastructure** >**Java And Process Management** > **Process Definition** > **Java Virtual Machine** pane,

      where WAS_APP_SERVER is the name of the IBM WAS application server that hosts Avaya Agent Web Client. For example, Server1.

   b. Create a customer property with the following parameters:
      - **Name**: java.protocol.handler.pkgs
      - **Value**: com.ibm.net.ssl.internal.www.protocol
   c. Save the changes to the IBM WAS Master Configuration:
      1. Select **Save to the Master Configuration**.
      2. On the next page, select **Save**.
4. Update the AAWCParameters.jacl:
   a. In a text editor, open AAWCParameters.jacl.
   b. For the value of the WebClientURL property in AAWCParameters.jacl, enter the URL for Avaya Agent Web Client in the following format:

      `https://`*`WAS_SERVER_NAME`*`:`*`SSL_ENABLED_PORT`*

      where ***`WAS_SERVER_NAME`*** is the fully-qualified domain name of the machine that hosts the Avaya Agent Web Client and ***`SSL_ENABLED_PORT`*** is the SSL port where the Avaya Agent Web Client application listens. For example, for an SSL implementation, enter `https://testbox.domain.com:9080`

   c. Save AAWCParameters.jacl.
5. Apply the JACL scripts, as described in Applying the JACL scripts on page 344.
6. Continue to deploy Avaya Agent Web Client with Deploying the application EAR file on page 346.

Redeploying the application EAR file (optional)

You can update and redeploy the application EAR file without uninstalling all Avaya Agent Web Client components. For example, use this procedure to redeploy the application EAR file after you:

- Change the configuration of the IBM WAS server.
- Customize Avaya Agent Web Client.
- Install certain types of patches for Avaya Agent Web Client.

Important:
This procedure assumes that you have already completed all steps required to install Avaya Agent Web Client.

This section includes the following topics:

Uninstalling the application EAR file

To uninstall the application EAR file:

1. Start the IBM WAS Administrative Console.
2. Stop the Avaya Agent Web Client application.
3. Uninstall the application EAR file, as described in Uninstalling the Avaya Agent Web Client application on page 445.
4. If the redeployed application EAR file includes changes to items that will be impacted by agent preferences, you might need to clean up the agent preferences. For more information, see *Avaya Agent Web Client Customization*.

Reassembling the application EAR file

To reassemble the application EAR file:

1. Save all changes to the configuration of the IBM WAS server or customized Avaya Agent Web Client files.
2. In IBM ASTK, update the Web applications in the **Navigator** pane:
   a. Select the following Web applications:
      - web
      - application
   b. Right-click the applications and select **Refresh**.

   Note:
   You can safely ignore any errors that begin with "The Manifest Class-Path for archive..." when you update the Web applications.
3. In the **Navigator** pane of IBM ASTK, select the **application** project.
4. Right-click on **application** and select **Export**.
5. In the **Export** window, select **EAR File** and follow the prompts.

Deploying the updated application EAR file

To deploy the updated application EAR file, follow the procedures described in Deploying the application EAR file on page 346.

Chapter 12: Deploying Client SDK components

This section includes the following topics:

Important:
Read the Avaya IC Readme file and *IC Installation Planning and Prerequisites* before you deploy the Client SDK.

Before you deploy Client SDK components

Before you deploy Client SDK server or design components:

- Install the required third-party software, as described in *IC Installation Planning and Prerequisites*.
- Install and configure all Avaya IC prerequisites, as described in *IC Installation Planning and Prerequisites*.
- Install and configure Avaya IC, including all media channels and Avaya FTSE.
- Create and configure agent accounts for agents who will use custom applications developed with the Client SDK, as described in Configuring agent accounts on page 283.

Installing the Client SDK components

Install the Client SDK server and design components, as described in Installing Avaya IC server and administration components on page 29.

Tip:
Avaya recommends that you install the Client SDK server components on a dedicated machine.

The following table lists the Client SDK components installed with each operating system.

Operating system	Deployment
Windows	Installs the following components: • Client SDK server components • Java and .NET design components
Solaris and AIX	Installs the following components: • Client SDK server components • Java design components To get the .NET design components, you must install the Client SDK on a Windows machine.

Configuring a secondary ORB server environment

The Client SDK server requires a secondary ORB server. Configure a secondary server environment, as described in Configuring a secondary ORB server environment on page 35.

Client SDK files

The following table describes the contents of the SDK directories created when you install the Client SDK components.

Directory	Contents
sdk/server	Client SDK server files, including the WAR file for Tomcat
sdk/design	All design files for the Client SDK in the following directories: • dotnet • java The following diagrams in PDF format: • Object model • State models for all stateful Client SDK objects
sdk/design/dotnet/lib	C# client libraries for the Client SDK client
sdk/design/dotnet/sample	Source code and binaries for the .NET sample client
sdk/design/dotnet/doc	Client API reference documentation for the .NET API
sdk/design/java/lib	Java client libraries for the Client SDK client
sdk/design/java/sample	Source code and binaries for the Java sample client
sdk/design/java/doc	Client API reference documentation for the Java API.

Setting up the Java Application Bridge

The Client SDK server uses the Java Application Bridge to communicate with the Avaya IC servers and databases.

This section includes the following topics:

Creating an agent account for the Java Application Bridge

The Java Application Bridge requires a non-human agent account for Avaya IC. You use this agent account when you configure Tomcat for the Client SDK server. This account is the DCO Bridge account.

The Avaya IC seed data includes one non-human agent account for the DCO Bridge. You can use this account for the first Java Application Bridge in the Avaya IC system.

You must create a unique non-human agent account for each additional Java Application Bridge in the Avaya IC system. Avaya recommends that you name each account dcobridge*N*. The agent name can also include the name of the machine that hosts the Java Application Bridge.

Tip:
The following instructions describe how to create additional non-human agent accounts for the Java Application Bridge. If you use the account in the Avaya IC seed data, double-click that agent account and complete Step 5 below.

To create an agent account for the Java Application Bridge:

1. In IC Manager, select the **Agent** tab.
2. Expand the **DefaultTenant** node in the left pane.

   If you want to create this agent account in a different tenant, expand that node in the left pane instead of **DefaultTenant**.
3. Select **Agent** > **New**.
4. Select the **General** tab and complete the following fields:

Field	Recommended entry
First Name	dcobridge*N* (for example, dcobridge2)
Last Name	dcobridge*N* (for example, dcobridge2)
Preferred Name	dcobridge*N* (for example, dcobridge2)
Employee ID	dcobridge*N* (for example, dcobridge2)
Login ID	dcobridge*N* (for example, dcobridge2)
Domain	The same user domain as the Java Application Bridge that will use this agent account. For example, User1.
Task Load	0
Task Ceiling	0
Site	DefaultSite

5. Select the **Security** tab and complete the fields as shown in the following table:

Field	Recommended entry
Password	Enter a password for this account. **Tip:** Avaya recommends that you change the password for the pre-defined Java Application Bridge account.
Confirm	Re-enter the password for this account.
Force password change on login	Clear this field. Do not check this field for non-human Avaya IC users
Disable login	Do not check this field.
Role	Check the **Agent** role. **Note:** Do not check any of the other roles.

6. Select **OK**.

Creating a Java Application Bridge

You must create a Java Application Bridge on the Client SDK server machine. The Java Application Bridge is not a true Avaya IC server. The Java Application Bridge impersonates each agent who logs in to the Client SDK. When the Java Application Bridge makes a request for an agent, the Java Application Bridge mirrors the domain structure of the agent.

To create a Java application bridge:

1. On the **Server** tab of IC Manager, select **Server** > **New**.
2. Select **JavaAppBridge** from the list of servers. Select **OK**.
3. Select the **General** tab and complete the fields shown in the following table.

Field	Recommended entry	Notes
Name	Enter a name for the Java Application Bridge.	Include the name of the machine that hosts the Tomcat application server to identify the location of the JavaAppBridge.

Field	Recommended entry	Notes
Domain	Select an Avaya IC User domain for the Java Application Bridge from the drop-down list.	For example, select `User1` from the drop-down list. Assign the Java Application Bridge to the same User domain as most Client SDK application users. You do not need a Java Application Bridge in each User domain. Ensure that the domain with the Java Application Bridge fails over to the following domains: ● Itself ● Default domain ● All domains with an ADU server
Host	Enter the IP address of the machine that hosts the Client SDK server.	
Port	Enter a port assignment for the Java Application Bridge.	You can use any available port in the 9000 range for the Java Application Bridge. Avaya recommends that you use port 9002.
Directory	Enter the path to the `etc` directory for the Client SDK server.	For example, enter: *IC_INSTALL_DIR*\IC71\etc where *IC_INSTALL_DIR* is the path to this directory on the Client SDK server machine. For example, if you used the default, the path is: `C:\Program Files\Avaya\IC71\etc`
Executable	Enter `jabsrv`.	Leave the default entry. **Tip:** This entry exists because Executable is a required field in IC Manager. No separate executable exists for the Java Application Bridge.

4. Record the **Name** value for the Java Application Bridge. You will need this name in Configuring Client SDK services on page 371.
5. Select the **JavaAppBridge** tab and complete the fields shown in the following table.

Field	Recommended entry	Notes
IC User	Enter the name of the agent account for this Java Application Bridge server.	Use the account that you created in Creating an agent account for the Java Application Bridge on page 368. For example, enter dcobridge1.
IC Password	Enter the password associated with the agent account.	

6. Select **OK**.

Important:
Do not start the Java Application Bridge in IC Manager. When you start the Client SDK server in Tomcat, that server starts the Java Application Bridge.

Configuring Client SDK services

Configure Client SDK services on all machines that host Client SDK server or design components.

To configure Client SDK services:

1. Start the Configuration Tool:

Operating system	Procedure
Windows	Select **Start** > **Programs** > **Avaya Interaction Center 7.1** > **Configuration Tool**.
Solaris and AIX	1. Navigate to `IC_INSTALL_DIR/IC71/bin` 2. Run **`./configure`**

2. Log in with your IC Manager login ID and password.
3. Select the **SDK Server** tab.
4. In the **SDK Server Machine** field, type the fully-qualified domain name of the machine that hosts the Client SDK server.

5. In the **JavaAppBridge Name** field, type the name of the Java Application Bridge that this Client SDK server will use.
6. Select **Apply Settings**.
7. Select **Exit**.

Starting and stopping the Client SDK server

This section includes the following topics:

- Starting and stopping the Client SDK server on Windows on page 372
- Starting and stopping the Client SDK server on Solaris and AIX on page 373

Starting and stopping the Client SDK server on Windows

To start, stop and configure the Client SDK server on Windows:

1. In the Services control panel, right-click on the Avaya IC 7.1 SDK Service.
2. From the right-click menu, select one of the options in the following table:

Task	Options
Start Client SDK server	Select **Start**.
Stop Client SDK server	Select **Stop**.
Set startup options	1. Select **Properties**. 2. Select **Automatic** from the **Startup Type** drop-down list. 3. Select **OK**.

Starting and stopping the Client SDK server on Solaris and AIX

Execute all Client SDK server commands from the *IC_INSTALL_DIR*/IC71/bin directory. For the Client SDK server to be able to log in, the Avaya IC servers must start first.

Starting the Client SDK server: To start the Client SDK server, execute the following command:

```
nohup ./ictomcat.sh start SDK
```

Stopping the Client SDK server: To stop the Client SDK server, execute the following command where -force is an optional parameter that terminates the server processes:

```
nohup ./ictomcat.sh stop SDK -force
```

Running a sample client

Perform these procedures on the development machine where you installed the Client SDK components. For more information about the Client SDK sample clients, see *IC Client SDK Programmer Guide*.

This section includes the following topics:

Running the .NET sample client on Windows

To run the .NET sample client on a Windows machine:

1. select **Start** > **Programs** > **Avaya Interaction Center 7.1** > **Run .Net Sample Client**.
2. In the dialog box, enter:
   - URL for the Client SDK server

     The URL must use the format: http://<*SDK_Server_Machine_Name*>:<*Port*>/<*Application_context*>. For example, with the default configuration, the URL could be http://testbox.xyzcorp.com:9700/icsdk
   - Avaya IC agent account
   - Password for the Avaya IC agent account
3. Select **OK**.

Running the Java sample client on Windows

To run the Java sample client on a Windows machine:

1. Select **Start** > **Programs** > **Avaya Interaction Center 7.1** > **Run Java Sample Client**.
2. In the dialog box, enter:
   - URL for the Client SDK server

     The URL must use the format: `http://<SDK_Server_Machine_Name>:<Port>/<Application_context>`. For example, with the default configuration, the URL could be `http://testbox.xyzcorp.com:9700/icsdk`
   - Avaya IC agent account
   - Password for the Avaya IC agent account
3. Select **OK**.

Running the Java sample client on Solaris or AIX

To run the Java sample client on a Solaris or AIX machine:

1. Navigate to the following folder:

   IC_INSTALL_DIR`\IC71\sdk\design\java\sample\bin`
2. Execute the following command: **`RunClient.sh`**
3. In the dialog box, enter:
   - URL for the Client SDK server

     The URL must use the format: `http://<SDK_Server_Machine_Name>:<Port>/<Application_context>`. For example, with the default configuration, the URL could be `http://testbox.xyzcorp.com:9700/icsdk`
   - Avaya IC agent account
   - Password for the Avaya IC agent account
4. Select **OK**.

Optional advanced configuration for the Client SDK server

This section includes the following topics:

Configuring the log4j files for the Client SDK server (optional)

To configure the log4j files for the Client SDK server:

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

   IC_INSTALL_DIR\IC71\tomcat\bin\icsdk.bat

2. Navigate to the section between MODIFICATION SECTION BEGIN and MODIFICATION SECTION END.
3. Update the following parameters in this section:

Parameter	Notes
LOG4J_CONFIGURATION	Enter the full path and file name for the Log4j XML file.
LOG4J_DEBUG	Set the Log level as follows: ● **true** to enable logging ● **false** to disable logging
JAVA_SECURITY_AUTH_LOGIN_CONFIG	Enter the full path to the directory that contains the cup.security file. For example: C:\Program Files\Avaya\IC71\SDK\cup.security

4. Save the icsdk.bat file.

Changing default port range (optional)

By default, the Client SDK server accepts connections from a client in a port range between 8000 and 9000. If a client is outside the firewall, you must open up ports in this range.

You can change the port range in the web.xml file. The web.xml file does not include

To change the default port range:

1. Open web.xml in a text editor.
2. Search for the `messaging.listener.port.range` entry.

   This entry does not exist out-of-the-box.
3. If the entry does not exist, add the `messaging.listener.port.range` entry to the web.xml file.
4. Set the value of `messaging.listener.port.range` entry to the desired port range, as follows:

   <a>-<b>

   where the value of a is greater than the value of b, and where a and b are unsigned integers which represent a valid port range. For example, a valid value is 9050-8050.
5. Save the file.
6. Restart the Tomcat server, as described in Starting and stopping the Client SDK server on Windows on page 372.

Chapter 13: Deploying Web Services

This section includes the following topics:

Important:
Read the Avaya IC Readme file and *IC Installation Planning and Prerequisites* before you deploy Web Services.

Before you deploy Web Services components

Before you deploy Web Services components:

- Install the required third-party software, as described in *IC Installation Planning and Prerequisites*.
- Install and configure all Avaya IC prerequisites, as described in *IC Installation Planning and Prerequisites*.
- Install and configure Avaya IC, including all media channels and Avaya FTSE.
- Create and configure agent accounts for agents who will use Web Services, as described in Configuring agent accounts on page 283.

Installing the Web Services components

Install the Web Services components, as described in Installing Avaya IC server and administration components on page 29.

Configuring a secondary ORB server environment

The Web Services server requires a secondary ORB server. Configure a secondary server environment, as described in Configuring a secondary ORB server environment on page 35.

Web Services files

The following table describes the contents of the SDK directories created when you install the Web Services components.

Directory	Contents
sdk/WebServices	Web Services server files, including the WAR file for Tomcat
sdk/webservices/sample	Sample Web Services client files

Setting up the Web Services Bridge

The Web Services server uses the Web Services Bridge to communicate with the Avaya IC servers and databases.

This section includes the following topics:

Creating an agent account for the Web Services Bridge

The Web Services Bridge requires a non-human agent account for Avaya IC. You use this agent account when you configure Tomcat for the Web Services server. This account is a DCO Bridge account.

You must create a unique non-human agent account for each Web Services Bridge in the Avaya IC system. Avaya recommends that you name each account dcobridge*N*. The agent name can also include the name of the machine that hosts the Web Services Bridge.

To create an agent account for the Web Services Bridge:

1. In IC Manager, select the **Agent** tab.
2. Expand the **DefaultTenant** node in the left pane.

   If you want to create this agent account in a different tenant, expand that node in the left pane instead of **DefaultTenant**.
3. Select **Agent** > **New**.
4. Select the **General** tab and complete the following fields:

Field	Recommended entry
First Name	dcobridge*N (*for example, dcobridge2)
Last Name	dcobridge*N (*for example, dcobridge2)
Preferred Name	dcobridge*N (*for example, dcobridge2)
Employee ID	dcobridge*N (*for example, dcobridge2)
Login ID	dcobridge*N (*for example, dcobridge2)
Domain	The same user domain as the Web Services Bridge that will use this agent account. For example, User1.
Task Load	0
Task Ceiling	0
Site	DefaultSite

5. Select the **Security** tab and complete the fields as shown in the following table:

Field	Recommended entry
Password	Enter a password for this account.
Confirm	Re-enter the password for this account.

Field	Recommended entry
Force password change on login	Clear this field. Do not check this field for non-human Avaya IC users
Disable login	Do not check this field.
Role	Check the **Agent** role. **Note:** Do not check any of the other roles.

6. Select **OK**.

Creating a Web Services Bridge

You must create a Web Services Bridge on the Web Services server machine. The Web Services Bridge is not a true Avaya IC server.

To create a Web Services Bridge:

1. On the **Server** tab of IC Manager, select **Server** > **New**.
2. Select **WebServices** from the list of servers. Select **OK**.
3. Select the **General** tab and complete the fields shown in the following table.

Field	Recommended entry	Notes
Name	Enter a name for the Web Services Bridge.	Include the name of the machine that hosts the Tomcat application server to identify the location of the Web Services Bridge.
Domain	Select an Avaya IC User domain for the Web Services Bridge from the drop-down list.	For example, select `User1` from the drop-down list. Ensure that the domain with the Web Services Bridge fails over to the following domains: • Itself • Default domain • All domains with an ADU server
Host	Enter the IP address of the machine that hosts the Web Services server.	

Field	Recommended entry	Notes
Port	Enter a port assignment for the Web Services Bridge.	You can use any available port in the 9000 range for the Web Services Bridge. Avaya recommends that you use port 9003.
Directory	Enter the path to the `etc` directory for the Web Services server.	For example, enter: *IC_INSTALL_DIR*\IC71\etc where *IC_INSTALL_DIR* is the path to this directory on the Web Services server machine. For example, if you used the default, the path is: `C:\Program Files\Avaya\IC71\etc`
Executable	Enter `wssrv`.	Leave the default entry. **Tip:** This entry exists because Executable is a required field in IC Manager. No separate executable exists for the Web Services Bridge.

4. Record the **Name** value for the Web Services Bridge. You will need this name in Configuring Web Services on page 382.
5. Select the **WebServices** tab and complete the fields shown in the following table.

Field	Recommended entry	Notes
IC User	Enter the name of the agent account for this Web Services Bridge.	Use the account that you created in Creating an agent account for the Web Services Bridge on page 379. For example, enter dcobridge1.
IC Password	Enter the password associated with the agent account.	

6. Select **OK**.

Important:
Do not start the Web Services Bridge in IC Manager. When you start the Web Services server in Tomcat, that server starts the Web Services Bridge.

Configuring Web Services

Configure Web Services on all machines that host Web Services components.

To configure Web Services:

1. In a text editor, open the following file:
   - Solaris or AIX: *IC_INSTALL_DIR*/IC71/tomcat/bin/icwebservices.sh
   - Windows: *IC_INSTALL_DIR*\IC71\tomcat/bin/icwebservices.bat
2. Navigate to the section between MODIFICATION SECTION BEGIN and MODIFICATION SECTION END.
3. Update the following parameters in this section to match your development environment:

Parameter	Notes
AVAYA_IC_WEBCLIENT_URL	Enter the correct protocol, host name, and port for the machine that hosts Avaya IC Web Services: http://<ws_machine>:[<ws_port>] For example, if you install Web Services on icwsbox.customuser.com, enter: http://icwsbox.customuser.com:9800/
AVAYA_IC_VESP_ JAVAAPPBRIDGE_NAME	Enter the name of the Web Services Bridge hosted on the machine. **Note:** This value is case sensitive.

4. Save the file.

Starting and stopping the Web Services server

This section includes the following topics:

Starting and stopping the Web Services server on Windows

To start, stop and configure the Web Services server on Windows:

1. In the Services control panel, right-click on the Avaya IC 7.1 Web Services.
2. From the right-click menu, select one of the options in the following table:

Task	Options
Start Web Services	Select **Start**.
Stop Web Services	Select **Stop**.
Set startup options	1. Select **Properties**. 2. Select **Automatic** from the **Startup Type** drop-down list. 3. Select **OK**.

Starting and stopping the Web Services server on Solaris and AIX

Execute all Web Services server commands from the *IC_INSTALL_DIR*/IC71/bin directory. For the Web Services server to be able to log in, the Avaya IC servers must start first.

Starting the Web Services server: To start the Web Services server, execute the following command:

```
nohup ./ictomcat.sh start webservices
```

Stopping the Web Services server: To stop the Web Services server, execute the following command where -force is an optional parameter that terminates the server processes:

```
nohup ./ictomcat.sh stop webservices -force
```

Appendix A: Configuring a localized version

To configure a localized version of Avaya IC, perform the steps in the following topics during the installation:

About localized versions of Avaya IC

The localized version of an Avaya IC release allows Avaya IC agent desktop applications to run in the supported languages for that release.

Typically, the localized version is delivered thirty days after the English release. However, for some releases, the localized version is delivered with the English release.

Where necessary, the topics in this section provide instructions for both types of delivery.

The following are known limitations of localization in Avaya IC:

Menu items may not be localized: Some menu items in Avaya IC applications are not completely localized. These items display in English. For example, you may see English text in some secondary built in forms and menu items, and on **OK** and **Cancel** buttons on some dialog boxes.

Accelerator keys do not work in Russian: Accelerator keys do not work for Web Agent in Russian. Ensure agents who work with Web Agent in Russian are aware that accelerator keys will not work.

For a list of the languages supported for a specific release, see *IC Installation Planning and Prerequisites*.

About the NLS Lang setting for Oracle

If your Avaya IC system includes an Oracle database, you must specify the NLS Lang property on the **Initial Configuration** tab of the Configuration Tool when you configure a primary or secondary server environment. The Configuration Tool automatically adjusts these settings when you provide the NLS_LANG parameter in the **Initial Configuration** tab.

Note:
The NLS Lang setting must match the value used to create the Oracle database. This value must include UTF8, because Avaya IC requires a UTF8 database.

This section includes the following topics:

For more information, see the Oracle documentation.

About the NLS Lang property

Oracle uses National Language Support (NLS LANG) values to set up language-specific databases. The character set part of the NLS_LANG parameter specifies the character set used by the Data server.

Where Oracle specifies the NLS Lang property

On Solaris, NLS_LANG is specified as an environment variable.

On Windows, NLS_LANG is set in the registry under the following:

```
HKEY_LOCAL_MACHINE > SOFTWARE > ORACLE > HOMEn
```

Cautions for the NLS Lang property

Do not use abbreviations in the NLS LANG parameter. For example, do not use "US" to designate American English. You must use AMERICAN_AMERICA.UTF8.

The character set in the NLS LANG parameter must match the character set of your Oracle database. If these character sets are different, strange character conversions and string truncations may result.

NLS Lang settings for supported languages

The following table includes the NLS Lang settings for the languages supported in this Avaya IC release.

Language	NLS Lang Setting
English	AMERICAN_AMERICA.UTF8
Spanish	SPANISH_SPAIN.UTF8
German	GERMAN_GERMANY.UTF8
French	FRENCH_FRANCE.UTF8
Italian	ITALIAN_ITALY.UTF8
Portuguese	BRAZILIAN PORTUGUESE_BRAZIL.UTF8
Simplified Chinese	SIMPLIFIED CHINESE_CHINA.UTF8

Language	NLS Lang Setting
Korean	KOREAN_KOREA.UTF8
Japanese	JAPANESE_JAPAN.UTF8
Thai	THAI_THAILAND.UTF8
Traditional Chinese	TRADITIONAL CHINESE_TAIWAN.UTF8
Russian	RUSSIAN_CIS.UTF8

Enabling Database Designer for localization

To use Database Designer with languages other than English, you must add a Localization section to the Database Designer INI file (`qdesigner.ini`). This section identifies the character encoding that you are using for translations in your locale.

When you open an ADL file for localization, your Database Designer INI file must contain a Localization section with character encoding that matches the language in the localized design.

The Localization section includes the following:

- ISO-639-1 (alpha 2) two letter language abbreviations
- Character encoding used in the output generated by Database Designer

The two letter language abbreviation also identifies the language in all language-specific files.

Important:
You must host Database Designer on a machine with an operating system that supports the target encoding. For example, you can use a localized version of Windows, or set the default system locale to the correct region in the **Regional Options** section of the Windows Control Panel.

To enable localization in Database Designer:

1. With Database Designer closed, open the Database Designer INI file (qdesigner.ini) in Notepad or another text editor.

   The Database Designer INI file is installed in the Windows directory. For example, in machines using Windows, the Windows directory is typically `c:\winnt`.

2. Add a Localization section at the end of the INI file, including values for TargetLanguage and TargetEncoding fields to match the desired locale using the information in the following table:

Language	Language Code	Localization Section Update

English	en	`[Localization]`
		`;English`
		`TargetLanguage=en`
		`TargetEncoding=windows-1252`

Spanish	es	`[Localization]`
		`;Spanish`
		`TargetLanguage=es`
		`TargetEncoding=windows-1252`

German	de	`[Localization]`
		`;German`
		`TargetLanguage=de`
		`TargetEncoding=windows-1252`

French	fr	`[Localization]`
		`;French`
		`TargetLanguage=fr`
		`TargetEncoding=windows-1252`

Italian	it	`[Localization]`
		`;Italian`
		`TargetLanguage=it`
		`TargetEncoding=windows-1252`

Portuguese	pt	`[Localization]`
		`;Portuguese`
		`TargetLanguage=pt`
		`TargetEncoding=windows-1252`

Simplified Chinese	zh	`[Localization]`
		`;Simplified Chinese`
		`TargetLanguage=zh`
		`TargetEncoding=gb2312`

Korean	ko	`[Localization]`
		`;Korean`
		`TargetLanguage=ko`
		`TargetEncoding=korean`

Language	Language Code	Localization Section Update

Japanese	ja	`[Localization]`
		`;Japanese`
		`TargetLanguage=ja`
		`TargetEncoding=shift_jis`

Thai	th	`[Localization]`
		`;Thai`
		`TargetLanguage=th`
		`TargetEncoding=windows-874`

Traditional Chinese	zt	`[Localization]`
		`;Traditional Chinese`
		`TargetLanguage=zt`
		`TargetEncoding=Big5`

Russian	ru	[Localization] ;Russian TargetLanguage=ru TargetEncoding=windows-1251

3. Save the INI file.
4. Close the text editor.

Configuring Avaya Agent for a supported language

You do not need to perform these steps for Avaya Agent Web Client. Only perform these steps for Avaya Agent.

To configure Avaya Agent for a supported non-English language:

1. When you generate your Interaction Center data source (as discussed in Generating the Interaction Center application on page 84):
   a. Check the **Avaya Agent Layout** box and select an Avaya Agent Layout for the appropriate language.
   b. Check the **EDU Layout** box and select an EDU Layout for the appropriate language.

      If you do not know the directory path, select the **Ellipsis** (**…**) button and navigate to the directory.
2. To create and run the Agent Installer, follow the instructions in Creating installation files for agent applications on page 307.

Configuring Avaya IC for multiple languages

If your Avaya IC system requires that Avaya Agent or Avaya Agent Web Client run in multiple languages, you must store the messages for each language in the database. Perform these steps after you generate the Interaction Center data source for the first language.

To configure Avaya Agent for multiple languages:

1. Close Database Designer if you have it open.
2. Update the `[Localization]` section of the Database Designer INI file for the language.

   For more information, see Enabling Database Designer for localization on page 388.
3. In Database Designer, open the CCQ ADL file.
4. Select **File** > **Generate Windows Application**.
5. In the **Generate Windows Application** dialog box:
   a. Check the **Messages** box only.
   b. Check the **Avaya Agent Layout** box and select an Avaya Agent Layout for the appropriate language.
   c. Check the **EDU Layout** box and select an EDU Layout for the appropriate language.

      To find the path, select the **Ellipsis** (**...**) button and navigate to the directory.
   d. Select **interaction_center** from the **Name** list.
   e. Type the path for the directory where you want Database Designer to store the application files.

      For example, type `C:\Program Files\Avaya\IC71\apps`.

      To find the path, select the **Ellipsis** (**...**) button and navigate to the directory.
   f. From the **DB Connection Set** drop-down list, select **defaultDBConnectionSet**.
   g. If the fields in the following table do not have entries, re-enter your IC Manager account and password.

Field	Recommended entry
Login Id	Type your IC Manager login ID. **Note:** Do not use your DBA login ID and password.
Password	Type your password.

   h. Select **OK**.

   Repeat these steps for each additional language.

Importing localized seed data

The localized seed data allows your Avaya IC system to have localized interfaces for the Website. You perform these steps on the machine that hosts Database Designer.

To install the localized seed data:

1. In Notepad or another text editor, open the following file: *IC_INSTALL_DIR*\IC71\design\CallCenterQ\data\seed_L10N.cfg
2. Verify that the **DestinationPasswd** field has the correct password for the Admin account.
3. Save the seed_L10N.cfg file.
4. Open a command window.
5. Navigate to *IC_INSTALL_DIR*\IC71\design\CallCenterQ\data
6. Run the following file to import the localized seed data: import_seed_L10N.bat

Configuring the Website for supported languages

To configure your Website for supported languages:

1. In IC Manager, select **Services** > **MultiTenancy Administration**.
2. Select **Define Languages** from the **Tenants Admin** menu.
3. In the **Properties** box:
   a. Select a language code.

      For both Simplified Chinese and Traditional Chinese, select **zh**.

   b. Assign a country/region code:
      - For Traditional Chinese, select **TW**.
      - For all other supported languages, leave the country/region code blank.

   c. Type a default description.

   d. Type a default display name.

   e. Select **Add Language**.

   If Avaya IC cannot find a property for a supported language, Avaya IC will use the default language. English is always the default language for the default tenant.

Setting language properties for agents

When you configure the language for an agent, you specify the language that the agent desktop applications use. You must set this property for all agents who work with an agent desktop language other than English.

Note:
Web Agent obtains the language setting from Avaya Agent. You do not need to configure the language for Web Agent separately.

To configure the agent language property for agents:

1. In IC Manager, select **Tools** > **Groups**.
2. Select the **Properties** tab.
3. Select the **IC** node in the left pane.
4. In the **Sections** list, select **Agent**.
5. Double-click the **UILanguage** property.
6. In the **Edit Property UILanguage** dialog box:
   a. From the **Property Value** drop-down list, select one of the values in the following table:

Value	Language
de	German
en	English
es	Spanish
fr	French
it	Italian
ja	Japanese
ko	Korean
pt	Portuguese
ru	Russian
th	Thai

Value	Language
zh	Simplified Chinese
zt	Traditional Chinese **Note:** zt is a non-standard two letter language code that certain components of Avaya IC use differentiate between Traditional Chinese and Simplified Chinese.

b. Select **OK**.

7. For languages that have regional variations of a particular language, such as Simplified Chinese and Traditional Chinese:

   a. Double-click the **UICountryOrRegion** property.

   b. From the **Property Value** drop-down list, select one of the values in the following table.

Value	Language
CN	China (Simplified Chinese)
TW	Taiwan (Traditional Chinese)

   Setting the **UICountryOrRegion** property also allows for regional differences in the date and time formats. For more information about how to customize Avaya Agent Web Client for regional differences, see *Avaya Agent Web Client Customization*.

   c. Select **OK**.

8. Select **OK**.

Localizing string table messages

You can use the **Localization** node in Database Designer to localize messages in the string table. For more information, see *IC Database Designer Application Reference*.

This section includes the following topics:

Translating string table messages

To translate string table messages:

1. Under the **Localization** placeholder, select **String Table** in the tree view.

   The String Table **Properties** tab opens and displays all available string table messages.
2. In the String Table **Properties** tab, select the message to be translated.
3. Select the message text in the **String Text** column.
4. Delete the message text and type in the translation.
5. Select **File** > **Save** to save the ADL file with the localized string table entries and generate the ALM file.

Deleting string table messages

If you delete a string table message that is connected to a form, the Avaya Business Application will not be able to display the message to the user.

To delete a string table message.

1. In the String Table **Properties** tab, select the message to be deleted.
2. Select **Delete**.

Configuring a Notification server for alternate email encodings

The Notification server uses a default Microsoft Windows codepage value for the outgoing email charset. You can override this value on the **Configuration** tab of the Notification server in IC Manager.

For example, if you want to use an alternate email encoding for a supported languages, such as iso-2022-jp instead of Windows-932 (Shift-JIS) for Japanese, you need to configure the Notification server to accept the alternate email encoding.

To configure a Notification server for alternate email encodings:

1. In IC Manager, double-click the HTTP Connector server in the lists of servers.
2. Select the **Configuration** tab.
3. Select **New**.
4. In the **CTI Type Editor** dialog box:
   a. Complete the fields as shown in the following table:

Field	Recommended entry
CTI Type	Couple
Name	charset This field is case-sensitive.
Value	*EmailCharset* where EmailCharset is the character set for the alternate email encoding. For example, type `iso-2022-jp` for Japanese.

   b. Select **OK**.
5. Select **OK**.
6. Stop and restart the Notification server.

Configuring an HTTP Connector server for Traditional Chinese

To configure an HTTP Connector server for Traditional Chinese:

1. In IC Manager, double-click the HTTP Connector server in the lists of servers.
2. Select the **Configuration** tab.
3. Select **New**.
4. In the **CTI Type Editor** dialog box:
   a. Complete the fields as shown in the following table:

Field	Recommended entry
CTI Type	Couple
Name	charsetmap This field is case-sensitive.
Value	Big5:Big5

   b. Select **OK**.
5. Select **OK**.
6. Stop and restart the HTTP Connector server.

Configuring an HTTP Connector server for Russian

To configure an HTTP Connector Server for Russian:

1. In IC Manager, double-click the HTTP Connector server in the lists of servers.
2. Select the **Configuration** tab.
3. Select **New**.

4. In the **CTI Type Editor** dialog box:
   a. Complete the fields as shown in the following table:

Field	Recommended entry
CTI Type	Couple
Name	charsetmap This field is case-sensitive.
Value	windows-1251:cp1251

   b. Select **OK**.
5. Select **OK**.
6. Stop and restart the HTTP Connector server.

Configuring the Customer HTML Chat Client for Japanese IMEs (optional)

Some Japanese Input Method Editors (IMEs) use the **Enter** key to select characters. If a Website customer uses one of these IMEs, the Customer HTML Chat Client may respond to the **Enter** key and send the message prematurely. You can configure the Customer HTML Chat Client not to automatically send a message when a customer presses the **Enter** key.

If you disable Send on Enter, the Website customer must select **Send** in the Customer HTML Chat Client to send a chat message to an agent.

To configure the Customer HTML Chat Client for Japanese IMEs:

1. In IC Manager, select **Services** > **MultiTenancy Administration**.
2. Select **Tenant Properties** in the **Tenant Admin** menu.
3. Select the tenant you want to customize from the **Select a Tenant** drop-down list.
4. Select **Customize Tenant**.
5. In the **Customize Tenant** page:
   a. Select **Japanese** from the **Select Language** drop-down list at the top of the page.
   b. Select **chat**.
   c. Scroll down to the **chat.htmlclient.entry.sendonenter** property.
   d. Change the value of this property to 0.
   e. Select **Update Data** at the bottom of the page.

Appendix B: Troubleshooting

This section includes the following troubleshooting topics:

Additional troubleshooting information is available in the following documentation:

- Avaya IC Readme and Readme Addendum
- Alarm Monitor online help in IC Manager
- Documentation for each Avaya IC component

If you encounter an issue not in the documentation, contact Avaya Technical Support.

Important:
Always consult the log files for information that can assist you in troubleshooting the problem. Always backup and retain the relevant log files until you have resolved the problem.

Troubleshooting installation and configuration

This section includes the following problems that can occur during Avaya IC installation and configuration:

Avaya IC installer does not display or stops abruptly on UNIX

Problem: The Avaya IC installation on Solaris and AIX does not display anything on the monitor or stops abruptly.

Solution: Verify that the `DISPLAY` property is set and the following temp file has sufficient space:

- Solaris: `/var/tmp`
- AIX: `/tmp`

Avaya IC requests time-out without completing

Problem: Avaya IC requests time-out without completing. For example, the ORB server or Avaya IC ORB Service 7.1 do not start automatically on a Windows machine. If you change the system clock in large increments (over 2-3 seconds per minute) when Avaya IC is running, IC requests may fail with "Time-out" errors.

Solution: Do not change the system in large increments when Avaya IC is running. Potential solutions are as follows:

- Use a time synchronization utility. Some commercial time synchronization products may provide gradual clock corrections over time. For more information, see *IC Installation Planning and Prerequisites*.
- For the Tardis time synchronization utility, verify the configuration. Tardis may make large time changes at unpredictable times that causes service requests to time out. To avoid this time-out problem, set the time adjustment increments in milliseconds, as follows:
  - For **Maximum correction allowed**, set in a range from a minimum of 50 milliseconds to a maximum of 500 milliseconds
  - For **How often the time is set**, set to **Every Minute**

  For information, see *IC Installation Planning and Prerequisites* and the Tardis online help.

libftet.so file is missing on Solaris

Problem: On Solaris, Avaya IC displays an error message about missing the **libftet.so** file when starting a Tomcat application.

Solution: Re-install Avaya IC server components on the Tomcat machine, including Avaya FTSE as described in Installing Avaya IC server and administration components on page 29.

Cannot start a service for a Web application with httpserver.sh

Problem: Cannot start a service for a Web application with the `httpserver.sh start` script. This problem typically occurs because the `.../HTTPServer/conf.httpd.conf` file includes multiple instances of `ictomcat.cfg`.

Solution: Do the following:

1. In a text editor, open the `.../HTTPServer/conf.httpd.conf` file and remove the multiple entries for `ictomcat.cfg`.
2. Restart the IBM http server, as described in Starting and stopping IBM http Web server on page 130.

Agent installer does not open on Windows 2000 Professional

Problem: Agent installer does not open on Windows 2000 Professional and Java process hangs. This problem is seen typically when you access the machine through pcAnywhere. Avaya Agent includes a Java 1.4.2 supported user interface. pcAnywhere has a known issue with Java 1.4.2 user interfaces on Windows 2000 operating systems.

Solution: To run the agent installer:

1. Uninstall pcAnywhere.
2. Install and use a different remote control software for the agent machine.

Troubleshooting the Configuration Tool

This section includes the following problems that can occur when you use the Configuration Tool:

Cannot access the Initial Configuration tab again to update values

Problem: Cannot access the Initial Configuration tab again to update or change the values chosen to configure the server or client environment.

Solution: To access the Initial Configuration tab after you have configured the server or client environment on a machine:

1. Rename the vesp.imp file in *IC_INSTALL_DIR*\IC71\etc to vesp_old.imp.
2. Start the Configuration Tool.

Apply Settings is not enabled in the Configuration Tool

Problem: After you make a change to a field in the Configuration Tool, **Apply Settings** is not enabled.

Solution: If **Apply Settings** is still not enabled, close and re-open the Configuration Tool.

Configuration Tool fails to load vesp.imp

Problem: When configuring a secondary ORB server environment, the Configuration Tool displays the following message: Failed to load vesp.imp.

Solution: Do the following, then rerun the Configuration Tool:

1. Backup the following logs:
   - General.log
   - General_Admin.log
   - Admin.log
2. Verify the following values in the Initial Configuration tab.
   - **IC Login** and **Password** must be valid.
   - **ORB port** must match the port of the ORB server on the primary machine.
3. Make sure you can "ping" the primary hostname.
4. Make sure that you started the Configuration Tool from the Start menu or from within the working directory of *IC_INSTALL_DIR*\IC71\bin.
5. If none of the above solutions work:
   a. Navigate to *IC_INSTALL_DIR*\IC71\bin and execute **configure -d**
   b. Backup the following logs again: General.log, General_Admin.log, and Admin.log.
   c. Contact Avaya Technical Support and provide both versions of the logs that you backed up.

Configuration Tool does not install ISAPI extensions in IIS properly

Problem: After configuring the Avaya IC Website, the Configuration Tool did not install the ISAPI extensions in Microsoft IIS properly.

Solution: Review the events in the Windows Event Viewer:

1. Look for recent Application events with WSH as the resource.
2. Look for the following events, which show where the ISAPI installation script began and ended:
   - ConfigTool install IIS components - started...
   - ConfigTool install IIS components - finished.
3. Review all events that occurred between these two events to identify the problems that caused the ISAPI extension installation to fail.

Troubleshooting the Avaya IC servers

This section includes the following topics:

Troubleshooting server communication issues

This section includes the following problem that can occur with server communications:

Avaya IC servers on the same machine cannot communicate when disconnected from network

Problem: If a machine that hosts Avaya IC servers is disconnected from the network, the servers on that machine may not be able to communicate with each other. This problem may cause agents who are currently logged into the system to not recover properly from the network failure when the network connection on the Avaya IC server machine is reestablished.

This problem occurs if a network cable is unplugged from a machine that hosts Avaya IC servers. All servers that use the IP Address to locate another server will not be able to communicate with those servers, even if those servers are on the same box.

This problem may exist on all supported operating systems. For a discussion of the issue on Windows, see the following Microsoft article:

http://support.microsoft.com/default.aspx?scid=KB;en-us;q239924

Solution: The following possible solutions exist for this problem:

- For Windows, see the workaround in the Microsoft article.
- For all supported operating systems, consider the following solution:
  a. Avaya recommends that you connect the Avaya IC server machines to a network hub, as follows:

     Avaya IC servers -------> Hub ----------> Rest of the network

  b. If the Avaya IC Server machine needs to be disconnected from the rest of the network, do the following:

     Avaya IC servers --------> Hub -----X------> Rest of the network

     Do not do the following:

     Avaya IC servers ---X---> Hub ----------> Rest of the network

Troubleshooting the Data server

This section includes the following problems that can occur when you configure a Data server:

Error message: Cannot find implementation

Problem: IC Manager displays the following error message: Cannot find implementation. This problem typically occurs if IC Manager has not updated one of the following servers with the Data server configuration:

- ORB server
- Directory server

Solution: Do the following:

1. Update the ORB server:
   a. Right-click on the ORB server.
   b. Select **Update**.
   c. Start the Data server.
2. If you continue to get the same message:
   a. Stop and start the Directory server.
   b. Start the Data server.

Error message: ld.so.1: <*IC_INSTALL_DIR*> qorasrv: fatal: libclntsh.so.8.0: open failed: No such file or directory

Problem: ORACLE_HOME is set to the wrong value.

Solution: Use the Configuration Tool to set ORACLE_HOME to the correct value.

Data server fails for an Avaya IC system that includes an Oracle database

Problem: The Data server fails for an Avaya IC system that includes an Oracle database, and the log file for the Data server includes the following error: `OCI Error: ORA-04031`

Solution: Increase the value for the shared pool size. The shared pool size is a configuration parameter for the Oracle database.

Troubleshooting the Workflow server

This section includes the following problems that can occur when you configure a Workflow server:

Workflow server cannot assign to an Avaya IC server

Problem: The Workflow server is unable to assign to another Avaya IC server. For example, the Workflow server cannot assign to an ADU server. This problem typically occurs because:

- The channel configuration of the Workflow server is set to "Server type".
- The name of the other Avaya IC server is identical to the server type.

Solution: To enable the Workflow server to assign to the other Avaya IC server:

1. Rename the other server, following the Server naming guidelines on page 100.
2. Restart the Workflow server.
3. Verify that the Workflow server can assign to the other server.

Troubleshooting the refresh in IC Manager

Tip:
Attempt to refresh IC Manager after each step.

If you do not receive a Success message after you refresh IC Manager:

1. Stop and then restart the Directory server.
2. If you still do not receive a Success message, stop and then restart the Data server.
3. If you still do not receive a Success message, check the connections to the database.
4. If you still do not receive a Success message, exit IC Manager, then log back in.

Troubleshooting Web Management

This section includes the following topics:

Troubleshooting the ICM server

This section includes the following problems that can occur with the ICM server:

Chat failure - login connections

Problem: Login connection errors prevent a chat from occurring. This problem can display several symptoms, including:

- ICM server is running but cannot log into Avaya IC core servers.
- The icmlog.txt file may include the following repeated message:
  `initToolkit@IcmParmMgr - Error: Toolkit Login Failed`
- ICM server may have an invalid login in the systemParms.txt file.
- The Avaya IC environment may not be properly configured.

Solution: Do the following:

1. Verify that AVAYA_IC_HOME system variable is set to `IC_INSTALL_DIR\IC71\`.
2. Verify that the Avaya IC core servers are up and running.
3. Verify that the vesp.imp configuration file is up-to-date in the `IC_INSTALL_DIR\IC71\etc` directory.
4. If necessary, re-run the Configuration Tool on the machine that hosts the ICM server, making sure that the **IC Login** and **IC Password** fields contain valid information.
5. Restart the ICM server, as described in Starting and stopping Avaya IC services on page 127.

Chat failure - connection issues

Problem: Connection errors prevent a chat from occurring. This problem can display several symptoms, including:

- ICM server is running but is unable to bind to its service ports (9501-9520). Another server is using these ports.
- ICM server or another java process may have been started while another ICM server was running (either as a Windows service or Java application).

Solution: To resolve this problem:

1. Stop all instances of the ICM service or icm java application (javaw.exe).

   Be careful terminating the ICM java applications. You must determine which javaw.exe process represents the ICM.
2. Reconfigure the ICM ports as described in Changing the default ICM service ports on page 436.
3. Restart the ICM server, as described in Starting and stopping Avaya IC services on page 127.

Chat failure - no resources

Problem: The ICM server is running but cannot read the configuration data from database due to PDM initialization failure or PDM query error. The PDM file may not be properly configured, the database login credentials may be incorrect, The database client software may be improperly configured, or the Data server or Database server may be down.

This problem can display several symptoms, including:

- The Chat application displays an establishing connection message then hangs.
- The Chat application displays an establishing connection message, then displays "Missing Phrase" repeatedly.
- Error messages in the <*icm_name*>_website.log file indicate a problem with the PDM.

Solution: To resolve this problem:

1. Verify that the Data server is running.
2. Verify that the Database server is running, as shown in the following table:

Database	Verification steps
SQL Server	Verify that: ● SQL Server DSNs are configured correctly. ● Database application is running.
Oracle	Verify that: ● Oracle client software is installed. ● Oracle Service Name is correctly configured on the client. ● Oracle DSN for ccq is created.
DB2	Verify that the DB2 client software is installed.

3. Restart the Tomcat server that hosts your Website application, as described in Starting and stopping Avaya IC services on page 127:
4. If these do not resolve the problem, re-run the Configuration Tool on the machine that hosts the ICM server with the following information In the **Web** tab:
   - Make sure the **IC Login** and **IC Password** fields contain a valid Avaya IC login and password.
   - Make sure the **Database Login** and **Database Password** fields contain a valid DBA login ID and password for the database server.
   - Check **Configure Website**.

Chat failure - system out of service

Problem: When you initiate a chat session from the Website, the chat client displays a message stating that the server connection is established, then displays a "System is Out of Service" message.

- The icmlog.txt file contains an "Agent Router Not Ready" error.
- The Alarm Monitor in IC Manager displays an "Error calling WACD Assign" alarm.

Solution: The solution depends upon the cause of the problem. Try each of the following solutions:

If the ICM server is running, but either the ICM Bridge in the Attribute server or the WebACD server is not available:

1. In IC Manager, start the Attribute server.

2. Verify that the Attribute server can start the WebACD server.

If the ICM server is running but the ICM Bridge has not been configured correctly:

1. Verify the configuration of the Attribute server as described in Creating the Attribute server on page 181.
2. Restart the Attribute server.

If the ICM, Attribute, and WebACD servers are running and the ICM Bridge has been configured, but the ICM Bridge cannot login, or can login but cannot connect to the WebACD server:

1. Verify the configuration of the Attribute server as described in Creating the Attribute server on page 181.
2. Verify that the IC Login name and password in the ICM Bridge are valid. Re-type password if necessary.
3. Verify that the IC Login for the ICM Bridge is in the same Avaya IC domain as the WebACD server. If the domain is different and cannot be changed, make sure the domain of the WebACD server is in the failover path for that domain.
4. Restart the Attribute server.

Transcript failure - transcript not sent

Problem: Transcripts from completed chats are not sent to customers. Typically, this problem occurs because the default SMTP server for the transcripts has not been set.

Solution: To set the default SMTP server for transcripts:

1. Set the **SMTP Host** parameter of the ICM server, as described in Configuring the ICM server on page 211.
2. Restart the ICM server, as described in Starting and stopping Avaya IC services on page 127:

ICM server cannot bind to ports

Problem: The ICM server cannot bind to ports when stopped and restarted immediately. Avaya IC performs a orderly shutdown of all the listening ports after the server is stopped. The ICM server cannot bind to these ports again until after the shutdown is complete.

Solution: After you shutdown the ICM server:

1. Wait for approximately one minute to ensure the ICM server and service are completely shutdown.
2. Restart the ICM server, as described in Starting and stopping Avaya IC services on page 127.

Customer chat reports busy lines when ICM server running

Problem: The ICM server is running, but a customer chat cancels out saying that the lines are busy.

Solution: Do the following:

- The Attribute server may not have established communication properly. Stop and restart the ICM server.
- Make sure that the ICM server configuration on the **Attribute** tab of the Attribute server. includes the ICM server on the Website machine where the customer is attempting to chat with an agent.

Troubleshooting Website pages

This section includes the following problems that can occur with Website pages:

Website does not start

Problem: Website does not start.

Solution: Take the following troubleshooting steps:

1. Validate the Website user:
   a. Verify that the Website user is logged in.
   b. Check whether the Website user is locked.
2. Verify passwords:
   a. Verify that the password for the Website user is the same password that was entered in the Configuration Tool when you configured Web Management services.
   b. Verify that the database password is the same password that was entered in the Configuration Tool when you configured Web Management services.
   c. If the password was changed in IC Manager, re-run the Configuration Tool, as described in Configuring Web Management services on page 186.
3. Review the website.log and website_general.log for the exact error.

4. Verify the PDM logs:
   a. Verify that the following logs are present in the *IC_INSTALL_DIR*\IC71\logs directory:
      - pdm_dco.log
      - pdm_ccq.log
      - pdm_qrepository.logs

      If pdm_ccq and pdm_qrepository.logs are not present, a PDM initialization error has occurred. You can find the exact error in pdm_dco.log.
   b. Verify that pdm_ccq.log or pdm_qrepository.log are 0kb in size.

      If these logs are larger than 0kb in size, PDM initialization error may have occurred. Possibly, native database drivers for SQL, Oracle, and DB2 have leading errors. You can find these errors with error codes in these logs.
   c. Verify that the pdm.xml file is present in the *IC_INSTALL_DIR*\IC71\etc directory.
   d. If none of the above logs show errors, verify that you can access an IC Test page.

      You can deploy an IC Test page from the Configuration Tool.

      If you cannot access an IC Test page, a Tomcat issue has occurred. Check the *IC_INSTALL_DIR*\IC71\logs\tomcat.log for the exact error.

Cannot access Website pages

Problem: Either or both of the Administrative or Customer Website pages are unavailable from the browser. This problem can occur for several reasons, including the following:

- Website cannot resolve the host name or locate the Web server.
- Website encounters DNS problems resolving location of the Web server
- Website did not initialize properly and has redirected browser to invalid URL.
- URL in Web browser contains the word "null"
- website.log file contains PDM error messages

Solution: Do the following:

If the browser displays an error, such as Host Name Not Resolved or Cannot Find Server:

- Restart the Web server, for example IIS, Sun ONE server or IBM http server.
- Restart the Tomcat applications, as described in Starting and stopping Avaya IC services on page 127.
- Verify that the password you used for the **IC Password** field of the Configuration Tool when you configured the Website has not expired.

If the Website is having DNS problems resolving location of the Web server:

1. Test for DNS issues by trying to access the home page of the Web server at the following URL: `http://<server>.<domain>.com`
2. Test for DNS issues by trying to access home page of Web server with its IP address, for example: `http://123.123.123.123`
3. Follow the instructions in *IC Installation Planning and Prerequisites* for configuring DNS resolution.
4. Check to see if your Web browser proxy settings are interfering with host name resolution.
5. Consult your Network Administrator about the DNS resolution of the Web server.

If another issue seems to be causing the problem, the PDM file may not be properly configured, the database login credentials may be incorrect, database client software may be improperly configured, or the Data server or Database server may be down. For solutions, see Chat failure - no resources on page 408.

Public Website - Blank start page

Problem: When trying to access the customer Website, the browser displays:

- A blank start page containing just the Avaya logo
- A "website.pages.startpage" metadata error
- A "website.pages.public" metadata error
- A null pointer exception error message

Solution: The PDM file is not properly configured or database services are unavailable. For solutions, see Chat failure - no resources on page 408.

Customer Website cannot login to Avaya IC servers

Problem: The Website application is running but cannot login to Avaya IC core servers. This problem can result in the following entries in the website.log file:

- Repeated login failed exception
- Repeated "Retry Toolkit Login after 60 seconds ..." message

See Login connection errors prevent a chat from occurring. This problem can display several symptoms, including: on page 407 for solution.

Customer management failure

Problem: The Administrative Website causes repeated generic error messages when you:

- Add a customer from the Public Website
- Manage Customer accounts from the Multi Tenancy Administration Web pages

Solution: For each Workflow servers that runs customer management workflows:

1. Verify that the Workflow server is in the same Avaya IC domain as the IC Login used by the Web Management application in the following file:

   `IC_INSTALL_DIR\IC71\comp\website\WEB-INF\web.xml`

   This login is the one that was entered in the **IC Login** field of the Configuration Tool. See the dsLogin parameter of the following file:
2. If a Workflow server is in a different domain from the IC Login, make sure the Workflow server domain is in the failover path of the IC Login domain.
3. Build and load the customer management workflows in the Webcenter project. For more information, see Using workflows for Web Management on page 206.
4. Restart the Workflow server.

Troubleshooting Web Management integration

The section includes the following problems that can occur with Web Management integration:

Authentication key could not be retrieved

Problem: You see an error message indicating that an authentication key could not be retrieved when you select one of the following options from the **Services** menu in IC Manager:

- WebACD
- Web Response Unit (Self-Service)
- Multi-tenant Administration

Solution: Do the following:

1. Verify that IC Manager is configured to access Web Management, as described in Integrating Web Management Administration on page 201.
2. Restart the Tomcat server that hosts your Website application, as described in Starting and stopping Avaya IC services on page 127.
3. Restart IC Manager to verify whether your administrative login for IC Manager has just reset its password:

Web browser does not open

Problem: The Web browser is not opened when you select one of the following options from the **Services** menu in IC Manager:

- WebACD
- Web Response Unit (Self-Service)
- Multi-tenant Administration

Solution: Configure IC Manager for your Web browser:

1. In IC Manager, select **Manager** > **Options**.
2. Select the **Environment** tab.
3. Select the **Ellipsis** (**…**) button next to the **Browser** field.
4. Select **Select from List**.
5. Select **Search Filesystem**.
6. Select the drive where the browser is installed. Select **OK**.
7. After the search is complete, select the Web browser from the list. Select **OK**.
8. Select **OK**.

Browser encounters an internal error

Problem: The Web browser displays a message stating that there was an internal error, when you select **Services** > **WebACD** in IC Manager. This problem typically indicates that the domain of the URL used to access the WebACD server is different from the domain expected by the WebAdmin plugin.

Solution: Do the following:

1. In IC Manager, verify that the following properties are the same:
   - System/Configuration - ChatLoginServer
   - WebACD server - WACD Web Server
   - Configuration Tool - Web Server Host and Web Server Domain
2. If the ChatLoginServer value is different:
   a. Enter the correct value.
   b. Select **Manager** > **Refresh**.
3. If the WACD Web Server value is different:
   a. Enter the correct value.
   b. Restart the Tomcat server that hosts your Website application, as described in Starting and stopping Avaya IC services on page 127.

   c. Restart the WebACD server.
4. If the Configuration Tool values are different:
   a. Rerun the Configuration Tool with the correct values
   b. Restart the Tomcat server that hosts your Website application.
   c. Restart the Web server.

Troubleshooting Web Scheduled Callback

This section contains the following problems you may encounter with Web Scheduled Callback:

Callback cannot be scheduled on this date/time. Please try again...

Problem: Scheduled calls are not registered from the Website. The Website user receives the following error message:

> Callback cannot be scheduled on this date/time. Please try again...

This problem usually occurs because the Website user attempted to schedule a call with a date or time in the past.

Solution: The Website user must schedule a call with a time that is at least one minute ahead of the current time.

CreateRecord exception

Problem: Scheduled calls are not registered from the Website. An alarm occurs with an exception for CreateRecord.

This problem usually occurs because the Web Scheduled Callback workflow was not properly uploaded to the database.

Solution: To solve this problem:

1. In Workflow Designer, open the webcenter project.
2. Build this project to reload the flows in the Workflow server.
3. Restart the Workflow server.

Scheduled calls are not delivered to agents

Problem: Scheduled calls are not delivered to agents.

Solution: This problem can occur for multiple reasons. For information about the specific error, review the contents of the WSC logfile.

Scheduled calls are not delivered to the agent at the scheduled time

Problem: Scheduled calls are scheduled but the call is not delivered to the agent at the scheduled time. The delivery of the scheduled call to the agent is delayed.

Solution: Web Scheduled Callback is a time-bound feature. For Web Scheduled Callback to work correctly, all Avaya IC servers and the database must be in the same time zone.

If the time on the machines that host Avaya IC servers and the database is not synchronized, a time lag may occur between the scheduled time for the callback and the exact time that a Web Scheduled Callback request is delivered to an agent.

Sorry callback is closed right now! Please try again later

Problem: Scheduled calls are not registered from the Website. The Website user receives the following error message:

> Sorry callback is closed right now! Please try again later.

This problem usually occurs because the call is scheduled for a time that is outside of the configured working hour range of the contact center.

Solution: Configure the working hours for the contact center, as described in Configuring the Website for Web Scheduled Callback on page 225.

Troubleshooting DataWake

This section contains the following problem you may encounter with the DataWake feature of Web Self-Service:

Windows only - no DataWake records visible for customer

Problem: An administrator or agent does not see any DataWake records for a customer in Web Self-Service. This problem typically occurs because the Configuration Tool did not insert the DataWake Sensor filter into IIS when you created the Website. As a result, the connector filter for the Website Tomcat server is either not present or is a global filter. DataWake requires that the connector filter be a local filter.

Solution: To add the local filter to IIS:

1. In Internet Services Manager, right-click on the Web Service where you installed the filter for the Website and select **Properties**.
2. Select the **ISAPI Filters** tab.
3. If there is no dwsensor filter listed or the filter has a red arrow to the left:
   a. Select **Add**.
   b. Type dwsensor in **Filter Name** field.
   c. Type the following directory and file name in the **Executable** field.

      `IC_INSTALL_DIR\IC71\bin\dwsensor.dll`

   d. Select **OK**.
4. Select **OK** in the **ISAPI Filters** tab.
5. In the Windows Services control panel, stop and restart the World Wide Web Publishing Service.

Web Management configuration files

Web Management uses the configuration files in the following table.

File Name	File Location	Description
web.xml	`IC_INSTALL_DIR\IC71\comp\website\WEB-INF\web.xml`	Web Management uses this Servlet API application startup file as a bootstrap file to log into the Avaya IC core servers. Use the Configuration Tool to update this file.
pdm.xml	`IC_INSTALL_DIR\IC71\etc\pdm.xml`	This property configuration database access file contains database and Data server configuration information. Use the Configuration Tool to update this file.

File Name	File Location	Description
vesp.imp vespidl.pk	*IC_INSTALL_DIR*\IC71\etc\vesp.imp *IC_INSTALL_DIR*\IC71\etc\vespidl.pk	Avaya IC server configuration files. The machine that hosts Web Management must have copies of these files.
local.properties	*IC_INSTALL_DIR*\IC71\servers\ *IC_INSTALL_DIR*/IC71/local.properties	This configuration file contains the definition of the Website application, including the Classpath and JNI path settings.

ICM server configuration files

The ICM server uses the configuration files in the following table.

File Name	File Location	Description
systemParms.txt	*IC_INSTALL_DIR*\IC71\etc\systemParms.txt	The ICM server uses this bootstrap file to log into Avaya IC Core servers. Use the Configuration Tool to update this file.
pdm.xml	*IC_INSTALL_DIR*\IC71\etc\pdm.xml	This property configuration database access file contains database and Data server configuration information. Use the Configuration Tool to update this file.
cirssystemParms.txt	*IC_INSTALL_DIR*\IC71\etc\cirssystemParms.txt	The CIRS server uses this bootstrap file to log into Avaya IC Core servers. Use the Configuration Tool to update this file.
vesp.imp vespidl.pk	*IC_INSTALL_DIR*\IC71\etc\vesp.imp *IC_INSTALL_DIR*\IC71\etc\vespidl.pk	Avaya IC server configuration files. The machine that hosts the ICM server must have copies of these files.

Web Management log files

Web Management uses the log files in the following table.

File Name	File Location	Description
<*website*>.log	*IC_INSTALL_DIR*\IC71\logs\website.log	This file is the main property configuration log file for Web Management. <*website*> is the value of the **dsObjectName** property in the web.xml file.
<*website*>_*.log	*IC_INSTALL_DIR*\IC71\logs\website_*.log	All other log files generated by the integration of the ICM server and the Avaya IC servers. <*website*> is the value of the **dsObjectName** property in the web.xml file.

ICM server log files

The ICM server uses the log files in the following table.

File Name	File Location	Description
icmlog.txt	*IC_INSTALL_DIR*\IC71\logs\icmlog.txt	This file is the main log file for the ICM server. This file contains server and connectivity status and call events.
icmlog.txt - icmlocalparms.txt	*IC_INSTALL_DIR*\IC71\logs\icmlog.txt - icmlocalparms.txt	This file is a temporary log file used by the ICM server. Do not edit this file.
<*icm*>_website.log	*IC_INSTALL_DIR*\IC71\logs\icm_website.log	This file is the main log file for the Website. <*icm*> is the value of the **dsObjectName** property in the systemParms.txt file.
<*icm*>_*.log	*IC_INSTALL_DIR*\IC71\logs\icm_*.log	All other log files generated by the integration of the ICM server and the Avaya IC servers. <*icm*> is the value of the **dsObjectName** property in the systemParms.txt file.

Web Scheduled Callback log files

Web Scheduled Callback uses the log files in the following table.

File Name	Description
wscallback.log	This file is the main log file for Web Scheduled Callback. This log includes all call statistics for Web Scheduled Callback. If the jloader.log does not report exceptions or problems, review this log file. **Note:** wscallback.log may use the name specified in the Web Scheduled Callback server configuration.
<*server_name*>_website.log	This file is the main log file for the Web Scheduled Callback server. <*server_name*> is the name of the Web Scheduled Callback server.
jloader.log	This file includes all Web Scheduled Callback start up information.

Troubleshooting Avaya FTSE

This section includes information about the following troubleshooting problems that you may encounter when you configure Avaya FTSE:

- Full text search configuration error messages on page 422.
- Verifying Web Self-Service configuration on page 423.
- Troubleshooting Web Self-Service pages on page 424.

Full text search configuration error messages

The following table includes some of the messages and errors that you might see when you configure full-text searches. These messages can occur on any operating system.

Message	Description
The object, "w_qw_wru_view", already exists in database.	You can ignore this message. This message does *not* indicate that you have encountered a problem with the configuration.
ERROR at line 1: ORA-00955: name is already used by an existing object	You can ignore this error. This message indicates that the view already exists.
execsql: execute failed SQLSTATE: SGS00, Native error: 0, error text [Hummingbird][SearchServer] Invalid table name	You may see this error message twice in fulcrum.err. This error occurs because the script is attempting to drop a table that does not yet exist. You can ignore this error when you run the `fulcrum_setup` command for the first time on a machine. However, if you receive this error when you repeat the command on a machine, investigate why the script cannot access the database to perform the following tasks: ● unprotect table qw_wru_en ● drop table qw_wru_en
ld.so.1: /opt/Avaya/IC71/fulcrum/bin/ execsql: fatal: libftet.so: open failed: No such file or directory	For Solaris or AIX only. You defined one of the following environment variables in your shell: ● ORACLE_HOME on Solaris ● DB2DIR on AIX To workaround this issue: 1. Unset ORACLE_HOME (on Solaris) or DB2DIR (on AIX) 2. Re-run fulcrum_setup.sh. 3. Reset the environment variable.

Verifying Web Self-Service configuration

This section includes the following topics, which assist you to troubleshoot and verify the Web Self-Service configuration:

- Verifying the Web Self-Service configuration on Microsoft Windows on page 423.
- Verifying the Web Self-Service configuration on Sun Solaris on page 423.
- Verifying the Web Self-Service configuration on IBM AIX on page 424.

Note:
If any of the configuration settings are not present or are invalid, re-configure Avaya FTSE as described in Configuring Avaya Full Text Search Engine on page 217.

Verifying the Web Self-Service configuration on Microsoft Windows

To verify the Web Self-Service configuration:

1. In Windows ODBC Administration, verify that the following system DSN was successfully created: **ICWRU**
2. In a text editor, such as Notepad, verify the Web Self-Service settings in the `pdm.xml` file:
   a. Open the following file: *`IC_INSTALL_DIR`*`\IC71\etc\pdm.xml`
   b. Find the section between the following headings:
   `<QE name="fulcrum"> ... </QE>`
   c. Make sure that this section is not commented out.
3. In a text editor, such as Notepad, verify the database settings in the `ec56.did` file:
   a. Open the following file: *`IC_INSTALL_DIR`*`\IC71\etc\wru_sql\ec56.did`
   b. Find the entries for the database user name and password.
   c. Confirm that these entries are valid.

Verifying the Web Self-Service configuration on Sun Solaris

To verify the Web Self-Service configuration:

1. Verify the database settings in the `ec56.did` file:
   a. Open the following file: *`IC_INSTALL_DIR`*`\IC71\etc\wru_sql\ec56.did`
   b. Find the entries for the database user name and password.
   c. Confirm that these entries are valid.
2. Verify that the following script was created in *`IC_INSTALL_DIR`*`/IC71/bin`:
   `fulcrumenv.sh`

Verifying the Web Self-Service configuration on IBM AIX

To verify the Web Self-Service configuration:

1. Verify that the following files were successfully created in *IC_INSTALL_DIR*\IC71\etc\wru_sql
   - ODBC.ini
   - wru_createview.sql
2. Verify that the fulcrumenv.sh script was created in *IC_INSTALL_DIR*/IC71/bin.

Troubleshooting Web Self-Service pages

Problem: Web Self-Service fails and displays one or more of the following symptoms:

- Web Self-Service Management fails when trying to submit, update, or delete documents.
- You see generic error messages when trying to search FAQs.
- You see PDM errors in website.log when you search, submit, update, or delete documents.

Solution: Do the following:

1. Repeat the steps to configure Avaya FTSE, as described in Configuring Avaya Full Text Search Engine on page 217.
2. Verify the Web Self-Service configuration, as described in Verifying Web Self-Service configuration on page 423.
3. Restart the ICM server, as described in Starting and stopping Avaya IC services on page 127.
4. If the problem still exists, determine whether the Web Management database access manager (PDM) has lost database connectivity:
   a. Verify that the Data server is running.
   b. Verify that the Database server for the RDBMS is running.
   c. Restart the Tomcat server that hosts your Website application, as described in Starting and stopping Avaya IC services on page 127.

Troubleshooting Avaya Agent and Web Agent issues

Tip:
Further troubleshooting information for agent configurations is available in *Avaya Agent Integration* and *Avaya Agent User Guide*.

This section includes the following problems that can occur when you configure and test Avaya Agent and Web Agent:

Avaya Agent - error upon log in

Problem: Avaya Agent shows an error when an agent logs in.

Solution: Verify the configuration of the IC data source for the Workflow server that processes events for the agent. For more information, see Creating a Workflow server on page 109.

Avaya Agent - layout not found

Problem: Avaya Agent displays the following message after login attempt: Avaya Agent Agent layout not found.

Solution: Verify the layout configuration:

1. In IC Manager, navigate to the following configuration property for the individual agent or for the workgroup: Agent/Desktop/Layout
2. Verify that the value of this property is set to the name of the Avaya Agent layout file, without the CDL extension. For example, if your Avaya IC system includes the default English Avaya Agent layout, type **`avaya_agent_en`**.

Avaya Agent - login error after power failure

Problem: A machine that hosts Avaya Agent has a power failure while the application was running. When power is restored, the agent receives an error attempting to log back in. For example, Avaya Agent displays an error message, such as: The Object has disconnected from its clients. This error can occur if the script cache (.sch) file on the agent machine has been corrupted.

Solution: Delete the script cache files on the agent machine from all Avaya IC directories. When the agent logs back in, Avaya IC automatically recreates the script cache files.

Avaya Agent - license error for voice channel after failure

Problem: After Avaya Agent fails, the agent can log back in to email channel and chat channel, but cannot log back in to voice channel. Avaya Agent displays a license error when attempting to log back in to voice channel.

Solution: To log in to the voice channel, agent can do one of the following:

- Login through Softphone
- Log out of Avaya Agent, then log back in again.

Avaya Agent - cannot login after Task Manager shutdown

Problem: Avaya Agent fails and you use Windows Task Manager to shutdown the application. On subsequent login attempts, Avaya Agent displays a Login Failed message. This problem usually occurs because the VTel application for Telephony continues to run in the background.

Solution: To shutdown the VTel application:

1. In Windows Task Manager, select the **Processes** tab.
2. Find the **`vtel.exe`** process.
3. Select **Shutdown**.

Avaya Agent - email channel cannot be enabled

Problem: You cannot enable the Email channel in Avaya Agent. This problem typically occurs because the WebACD server is not properly configured for Email Management.

Solution: Add the configuration parameter emailservername to the WebACD server. For more information, see Configuring the WebACD server for Email Management on page 271.

Avaya Agent - error when transferring contact to virtual queue

Problem: An agent receives an error when transferring a contact to a virtual queue. The agent may see an error such as: Error occurred while searching the selected Object. Please select new object and consult the administrator.

Virtual queue is visible and appears available for transfers in Unified Agent Directory. However, this error typically occurs because the queue cache on the Workflow server that runs workflows for the Unified Agent Directory was not updated when a new queue was created.

Solution: For every Workflow server in a User domain:

- Manually run the sys_transfer.update_vq_cache workflow.
- Restart the Workflow server.

Avaya Agent - menu leaves blank space

Problem: An Avaya Agent menu leaves a blank space on Avaya Agent when an agent clicks off the menu. This problem is caused because Windows XP Professional does not repaint display correctly.

Solution: To repaint and display the missing area:

1. Minimize Avaya Agent.
2. Restore Avaya Agent to full size.

Avaya Agent - Windows Start menu hidden

Problem: The **Start** menu for Windows XP Professional displays behind Avaya Agent if Avaya Agent is set to Always On Top. Windows XP Professional does not handle Always on Top setting correctly.

Solution: To view and access the **Start** menu for Windows XP Professional, do one of the following:

- Minimize Avaya Agent.
- Select the Avaya Agent Start menu and disable Always On Top. If you choose this option, you must enable Always on Top again, if you do not want other applications to open on top of Avaya Agent.

Web Agent - does not display

Problem: The Web Agent does not display on the agent desktop, even though Avaya Agent is running. This problem typically occurs because the agent desktop does not know the location of the Paging server.

Solution: In IC Manager, set the Agent/Desktop/WAC/Server property to the fully-qualified domain name of the machine that hosts the Paging server.

Web Agent - displays but IC Email server light is red

Problem: Web Agent displays, but the WACD light is green and the IC Email server light is Red.

Solution: This problem can occur if you started the WebACD server before the License server. When that occurs, the WebACD server cannot access an Avaya IC license. Stop and restart the WebACD server.

Web Agent - accelerator keys do not work in Russian environment

Problem: For Web Agent in Russian environment, an agent uses an accelerator key to access menu items, but nothing happens. Accelerator keys do not work for Web Agent in Russian.

Solution: Ensure agents who work with Web Agent in Russian are aware that accelerator keys will not work.

Troubleshooting Avaya Agent Web Client

This section contains the following problems you may encounter with Avaya Agent Web Client:

Tip:
For information about how to customize Avaya Agent Web Client, see *Avaya Agent Web Client Customization.*

Troubleshooting general Avaya Agent Web Client issues

This section contains the following problems you may encounter with Avaya Agent Web Client:

Avaya Agent Web Client starts but does not become available

Problem: Avaya Agent Web Client appears to start, but never becomes available. All channels display an hourglass and after a few seconds the "network loss connection" message box appears.

Solution: Set the working directory property to a valid directory, as described in Configuring the working directory property on page 299.

Automation server cannot create object

Problem: When agent receives a work item, Avaya Agent Web Client displays the following message: "Maybe security settings are too high. Automation Server cannot create object"

Solution: On the agent machine, configure the security settings in the Internet Options of Internet Explorer as described in Prerequisites for Avaya Agent Web Client on page 328.

Avaya Agent Web Client - Solaris and AIX issues after default shell changed

Problem: For Solaris or AIX, Avaya Agent Web Client does not function correctly if default shell is changed after installing Avaya Agent Web Client software.

Solution: If you change the default shell, you must stop and restart the IBM WAS server for Avaya Agent Web Client, as described in Starting and stopping Avaya Agent Web Client on Solaris and AIX on page 352.

Troubleshooting the Java Application Bridge

This section contains the following problems you may encounter with the Java Application Bridge:

Java Application Bridge does not start

Problem: Java Application Bridge does not start. Typically, the Java Application Bridge fails to start because it is in the wrong domain, or the IBM WAS is not up and running.

Solution: Verify that the Java Application Bridge is in an Avaya IC User domain and that domain has the correct failover path. For more information, see Creating a Java Application Bridge on page 335.

If the Java Application Bridge is in the correct domain, verify that the IBM WAS server that hosts Avaya Agent Web Client is up and running.

Java Application Bridge does not start on Solaris or AIX

Problem: Java Application Bridge does not start automatically on Solaris or AIX.

Solution: Stop and restart the IBM WAS application server and application for Avaya Agent Web Client, as described in Starting and stopping Avaya Agent Web Client on Solaris and AIX on page 352.

Alarms displays after refreshing Java Application Bridge

Problem: The Alarm Monitor in IC Manager displays the following messages after you refresh the Java Application Bridge:

- Refresh on Address Book cache failed
- Refresh on Address Book filter failed

Typically, a refresh of the Address Book fails for the following reasons:

- Database failure
- Slow response from database
- Network problems

Solution: Do the following:

1. Wait a short period of time, then attempt to refresh the Address Book again.
2. If the second refresh fails again, check the logs and verify that:
   - The database is up and running.
   - There are no network issues.
3. Check the following logs for messages:
   - AvayaDebug.log
   - AvayaErrors.log
   - DCOBridge_<*username*>.log

Inaccessible UNIX path causes problems accessing attachments

Problem: One or more of the UNIX paths are not accessible, so some attachments might not be accessible. An alarm is generated if the IBM WAS application server identifies a problem with the an entry in the **UNC to UNIX Path Mapping** table.

Solution: Do the following:

1. Verify that all UNIX paths are accessible from the machine that hosts the IBM WAS.
2. Correct the entry in the **UNIX Path** column of the **UNC to UNIX Path Mapping** field.
3. Restart the IBM WAS application server for Avaya Agent Web Client.

Invalid UNC to UNIX path mappings causes problems accessing attachments

Problem: One or more of UNC to Unix path mappings are invalid and have been ignored, so some attachments might not be accessible. An alarm is generated if the IBM WAS application server finds invalid entries in the **UNC to UNIX Path Mapping** field.

Solution: Do the following:

1. Verify all of the entries in the **UNC to UNIX Path Mapping** field.
2. Correct the invalid entries in the **UNIX Path** column of the **UNC to UNIX Path Mapping** field.
3. Restart the IBM WAS application server for Avaya Agent Web Client.

Troubleshooting log in issues

This section contains the following problems you may encounter when you log in to Avaya Agent Web Client:

Browser acts strangely when you open Avaya Agent Web Client

Problem: The Web browser acts strangely when you attempt to open Avaya Agent Web Client.

Solution: Verify that you have completed all prerequisites for the agent machine, as described in Prerequisites for Avaya Agent Web Client on page 328.

Cannot access Avaya Agent Web Client start page without using port

Problem: The IBM WAS is hosted on a Windows or Solaris machine, you cannot access the start page for Avaya Agent Web Client without including the port in the URL. This problem can occur if the Web server included with Windows or Solaris is not properly stopped and restarted.

Solution: Restart IBM WAS:

- For IBM WAS on Windows, see Starting the HTTP server on Windows on page 348.
- For IBM WAS on Solaris, see Starting the HTTP server on Solaris on page 348.

DCO bridge errors prevent login

Problem: An agent cannot log in to Avaya Agent Web Client and the systemout log contains DCO bridge errors. This problem can occur if Avaya Agent Web Client cannot locate the required DLL file.

Solution: Verify that the environment or system variable is set correctly:

- For Windows, verify that the AVAYA_IC71_HOME environment variable is correctly set to `IC_INSTALL_DIR\IC71\`. For example, if you installed in the default directory, the environment variable should be set to `C:\Program Files\Avaya\IC71`
- For Solaris and AIX, verify that you started the IBM WAS application server and application for Avaya Agent Web Client with the aawc.sh script. For more information, see Starting and stopping Avaya Agent Web Client on Solaris and AIX on page 352.

VESP bridge errors prevent login

Problem: An agent cannot log in to Avaya Agent Web Client and the systemout log contains VESP bridge related errors.

Solution: Verify the following values:

- The Admin account specified in the web.xml
- The `JavaAppBridgeName` setting in the JACL script

Avaya Agent Web Client start page returns an error after log in

Problem: The Avaya Agent Web Client start page returns an error when an agent attempts to log in.

Solution: Do the following:

1. Verify that the names and values of the Avaya Agent Web Client settings in the JACL scripts are correct. A typographical error in the name or the value of any of these settings can stop you from logging in to Avaya Agent Web Client. For more information, see Setting up the JACL scripts on page 342.
2. In IC Manager, verify that the value of the following agent property is set to avaya_agent: Agent/Desktop/WebClient/Template.

Avaya Agent Web Client freezes after log in

Problem: Avaya Agent Web Client opens after an agent logs in, but remains frozen.

Solution: If your network includes a proxy server, verify that the proxy settings in the Avaya Agent Web Client settings in the JACL scripts are correct. For more information, see Setting up the JACL scripts on page 342.

Troubleshooting IBM WAS application server issues

This section contains the following problems you may encounter with the application server on IBM WAS:

For more troubleshooting information for IBM WAS, see *IC Administration Volume 1: Servers & Domains* and the documentation provided by IBM.

This section includes the following topics:

Avaya Agent Web Client unavailable after network loss of connectivity

Problem: After intermittent network loss of connectivity to the IBM WAS application server, agents do not recover access to Avaya Agent Web Client. When the network becomes unavailable, the Node Agent forces its managed application servers to stop if the loopback is configured for 127.0.0.1. The loopback is configured 127.0.0.1 by default, because NodeAgent uses regular IP protocol to ping the IBM WAS application server.

Solution: To resolve this problem, configure a loopback alias to a real IP address in the system, not the default loopback of 127.0.0.1.

To configure a loopback alias on Windows, install the Microsoft Loopback Adapter in the Windows operating system. For more information, use the documentation provided by Microsoft, or a Web tutorial such as the one at:

http://www.wown.com/articles_tutorials/Install-Microsoft-Loopback-adapter-Windows-XP.html

To configure a loopback alias on Solaris or AIX, execute the following command:

```
ifconfig lo0 addif <WAS_IP_ADDRESS> up netmask 255.255.255.0
```

Avaya Agent Web Client cannot start under non-root user on UNIX

Problem: For IBM WAS on Solaris or AIX, Avaya Agent Web Client application server or application does not start when run under non-root user.

Solution: Verify the following:

- That the required files and folders are owned by the non-root user.
- For a Deployment Manager configuration, that the Node Agent was started with the non-root user.

For more information, see Changing ownership for Avaya Agent Web Client - Solaris and AIX only on page 349.

Changing logging levels for Avaya Agent Web Client

This section contains the following information about how to change logging levels for Avaya Agent Web Client:

Changing the log level on a browser

In IC Manager, set the value of the following agent property to the desired level (trace or debug):

Agent/Desktop/WebClient.LogLevelClient

Changing the log level for Avaya Agent Web Client and IBM WAS

The LogLevelServer agent property and the log4j loglevel work together. You must update both of these items to get desired level of logging.

For the LogLevelServer property, in IC Manager, set the value of the following agent property to the desired level (trace or debug):

Agent/Desktop/WebClient.LogLevelServer

For the log4j loglevel:

1. In the log4j.xml file, navigate to the loglevel entry below the root element.
2. Set the value of loglevel to trace or debug.
3. Save the log4j.xml file.
4. Redeploy the application EAR file, as described in Redeploying the application EAR file (optional) on page 362.

Troubleshooting Business Advocate

This section contains the following problem you may encounter when installing Business Advocate components:

Tip:
Further troubleshooting information for Business Advocate is available in *IC Business Advocate Configuration and Administration.*

- Resource Manager cannot access MSMQ during startup on page 436

Resource Manager cannot access MSMQ during startup

Problem: Resource Manager cannot access MSMQ during start up, and generates a High alarm in the Alarm Monitor of IC Manager. The following error is received from MSMQ:

Important:
Resource Manager won't be notified about administrative changes until the problem is corrected.

This error message occurs when MSMQ is in an indeterminate state. This error message signifies a known problem with MSMQ, and does not signify a problem with Business Advocate or Avaya IC.

Solution: According to Microsoft, this problem was resolved in Service Pack 1 of Windows Server 2003. To resolve this issue, install Service Pack 1 when it becomes available.

Changing default service ports

This section includes the following topics:

- Changing the default ICM service ports on page 436
- Changing default service ports for servers on page 437

Changing the default ICM service ports

You can change some ICM service ports as described in the following topics:

- Changing the ICM tunnel port on page 437
- Changing the CIRS servlet port on page 437

Changing the ICM tunnel port

To change the ICM tunnel port:

1. On the machine that hosts the ICM server, open the following file in a text editor: *IC_INSTALL_DIR*\IC71\comp\website\WEB-INF\web.xml
2. In the section for the Tunnel servlet, add a new parameter with the value in the following table:

Parameter	Value
port	new port number

3. Save the web.xml file.
4. Restart the Website.

Changing the CIRS servlet port

To change the CIRS servlet port:

1. On the primary machine that hosts the ICM server and the Website, open the following file in a text editor: *IC_INSTALL_DIR*\IC71\comp\website\WEB-INF\web.xml
2. In the section for the CIRS servlet, add a new parameter with the value in the following table:

Parameter	Value
port	new port number

3. Save the web.xml file.
4. Restart the Website.

Changing default service ports for servers

You can change the default service ports, if required, as shown in the following topics:

Changing the service port for the WebACD server

For more information about the WebACD server, see Creating the WebACD server on page 177.

To change the service port for the WebACD server:

1. In IC Manager, update the WebACD server configuration:
   a. Double-click the WebACD server in the list of servers.
   b. Select the **WACD** tab.
   c. Change the port number in the **Service Port** field.
2. In Notepad or another text editor, open the Webadmin.cfg file, and change the service port property to the new port number.

Changing the service port for the ComHub server

For more information about the ComHub server, see Creating the ComHub server on page 182.

To change the service port for the ComHub server:

1. In IC Manager, update the ComHub server configuration:
   a. Double-click the ComHub server in the list of servers.
   b. Select the **ComHub** tab.
   c. Change the port number in the **Service Port** field.
2. In IC Manager, update the `masterserverport` property of the WebACD server:
   a. Double-click the WebACD server in the list of servers.
   b. Select the **WACD** tab.
   c. Change the value of the **Comhub Port** field to the new port.
3. In IC Manager, update the Paging server configuration:
   a. Double-click the Paging server in the list of servers.
   b. Select the **Paging** tab.
   c. Right-click on an empty area in the tab and select the **Show Advanced Properties** box.
   d. Change the value of the **Comhub Port** field to the new port.

Changing the service port for the Paging server

For more information about the Paging server, see Creating the Paging server on page 184.

To change the service port for the Paging server:

1. In IC Manager, update the Paging server configuration:
   a. Double-click the Paging server in the list of servers.
   b. Select the **Paging** tab.
   c. Change the port number in the **Service Port** field.
2. In IC Manager, update the port value for the Agent/Desktop/WAC property for each agent. You can change the global value for all agents through the Group Manager, or change the value for each agent. For more information, see:
   - Setting global properties for all agents on page 293.
   - Setting properties for individual agents and workgroups on page 294.

Changing the service port for the Attribute server

For more information about the Attribute server, see Creating the Attribute server on page 181.

To change the service port for the Attribute server:

1. In IC Manager, update the Attribute server configuration:
   a. Double-click the Attribute server in the list of servers.
   b. Select the **Attribute** tab.
   c. Change the port number in the **Port** field.
2. In Notepad or another text editor, open the datawake.cfg file, and change the service port property to the new port number.

Troubleshooting Windows configuration

You can receive an Out of Disk Space error even if the target drive is not full. If you install Avaya IC on a drive other than C:\, Avaya IC uses the `C:\Temp` directory for staging the installation files.

To resolve this issue:

- Free up space on the C:\ drive
- Changing the machine's TEMP environment variable to point to a folder on another drive

For more information, see the Windows documentation provided by Microsoft.

Troubleshooting virtual directories

On a Windows server none of the virtual directories used by Avaya IC get created within IIS for the Web Channel and Email Channel. The virtual directories include **website**, **webadmin**, **aicjakarta**, **icm**, and **rltemplateHelp**.

To troubleshoot virtual directories:

1. Run the Configuration Tool in diagnostic mode. Enter the following command from the ***ICroot*\bin** directory:

   `.\configure -d`

   where ***ICroot*** is the location of your IC software.

2. Look in the ***ICroot*\logs\General_Admin.log** file for the error message, `Input Error: There is no script engine for file extension ".vbs".`

   where ***ICroot*** is the location of your IC software.

   Note:
   The error means that Windows Script Host is either outdated, misconfigured, not installed, or disabled. If this message is not present, then contact IC support and send them the General_Admin.log file.

3. Reinstall the Windows Script Host version 5.6 from Microsoft's support website.
4. If the same error message reappears in the General_Admin.log file, contact your local IT department for further assistance.

Uninstalling Avaya IC

If you must uninstall Avaya IC from a machine, perform the following steps to ensure that all services, files, and related components are removed.

1. Uninstalling Avaya IC components on Windows on page 441.
2. Uninstalling Avaya IC servers on Solaris and AIX on page 442.
3. Uninstalling Web server components on page 442.
4. Uninstalling related third-party components on page 443.
5. Uninstalling Avaya Agent on page 443.
6. Uninstalling Avaya Agent Web Client on page 444.

Uninstalling Avaya IC components on Windows

Note:
The Avaya IC uninstaller occasionally does not remove all entries to the Windows registry. After you uninstall an Avaya IC component from a Windows machine, you may need to manually remove remaining entries from the Windows Registry.

To uninstall Avaya IC components on Windows:

1. In IC Manager, select **Server** > **Shutdown** to stop all Avaya IC servers on the machine.
2. Close all Avaya IC applications on the target machine.
3. Stop all Avaya IC 7.1 services and the World Wide Web Publishing for IIS service.

   For more information about these services, see Starting and stopping services on Windows on page 128.
4. In the Windows Control Panel:
   a. Open **Add/ Remove Programs**.
   b. Select **Avaya IC 7.1 (*component_name*)**.

      where ***component_name*** is the name of the Avaya IC component installed on the machine, such as Core Servers, Connector, or Administration.
   c. Select **Change/Remove** to start the Avaya IC Uninstaller.

   Follow the prompts in the Avaya IC Uninstaller to uninstall Avaya IC services, delete registry settings, and remove files that are not in use.
5. In the Windows Control Panel, delete the Avaya IC environment variable:
   a. Double-click **System**.
   b. On the **Advanced** tab, select **Environment Variables**.
   c. Select the Avaya IC environment variable in the System Variables box.
   d. Select **Delete**.
   e. Select **OK**.
6. Delete the remaining folders and files in the `IC_INSTALL_DIR\IC71\` directory.
7. Delete all shortcuts that you added to the desktop.
8. Open the Windows Registry and confirm that all Avaya IC entries have been removed.
9. Continue with Uninstalling Web server components on page 442 without restarting the target machine.

Uninstalling Avaya IC servers on Solaris and AIX

CAUTION:
Do not use the **`rm -rf`** command to uninstall Avaya IC components from Solaris or AIX.

To uninstall Avaya IC servers on Solaris and AIX:

1. Close all Avaya IC applications on the target machine.
2. In a command window on the target machine, stop the Avaya IC servers as described in Stopping all servers with the Avaya IC Admin utility on page 126.
3. In a command window on the target machine, stop the Avaya IC services as described in Starting and stopping services on Sun Solaris and IBM AIX on page 129.
4. Navigate to `IC_INSTALL_DIR/IC71/`
5. Execute the following script:

   `./uninstall.sh`

   The uninstaller removes all Avaya IC related files from the target machine, including files that were configured after installation, such as the vesp.imp file.
6. Remove all Avaya IC commands that you added to the UNIX startup script.
7. Delete the Avaya IC root directory.
8. Continue with Uninstalling Web server components on page 442 without restarting the target machine.

Uninstalling Web server components

Perform these steps if the target machine includes a Web server. If the target machine does not include Web server components, continue with Uninstalling related third-party components on page 443.

To uninstall Web server components:

1. For Tomcat, perform the following steps:
   a. Delete all Tomcat servers that you created to host Web applications, such as the Website and WebLM.
   b. Uninstall Tomcat, if desired.
2. For the Web server, perform the following steps:
   a. Remove the virtual directories from your Web site.
   b. For IIS, remove the dwsensor and Jakarta Connector filters from the **ISAPI Filters** tab.

Uninstalling related third-party components

Perform these steps to complete your uninstallation.

To uninstall related third-party components:

1. Uninstall all related third-party components that you installed on the target machine.

   For information on uninstallation procedures, see the manufacturer's documentation.
2. If the target machine has a Windows operating system, navigate to **`c:\WINNT\Temp`** and delete all numbered **`_istmp`** directories.
3. If the target machine has a Windows operating system:
   a. Navigate to C:\Documents and Settings\<*install_user_name*>\Local Settings\Temp
   b. Delete all ismpXXX and LREXXX.tmp directories.
4. Restart the target machine.

Uninstalling Avaya Agent

Note:
The Avaya IC agent application uninstaller does not always remove all entries to the Windows registry. The remaining entries in the Windows Registry will not block functionality for other applications on the machine.

To uninstall Avaya Agent.

1. Close all Avaya IC applications on the target machine.
2. In the Windows Control Panel:
   a. Open **Add/ Remove Programs**.
   b. Select **Avaya IC 7.1 (Rich Client)**.
   c. Select **Change/Remove** to start the Avaya IC Uninstaller.

   Follow the prompts in the Avaya IC Uninstaller to uninstall Avaya IC services, delete registry settings, and remove files that are not in use.
3. In the Windows Control Panel, delete the Avaya IC environment variable:
   a. Double-click **System**.
   b. On the **Advanced** tab, select **Environment Variables**.
   c. Select the Avaya IC environment variable in the **System Variables** box.
   d. Select **Delete**.
   e. Select **OK**.

4. For the `...\Backup` directory that was created by the agent installer:
   a. Review the files in the directory.
   b. Confirm that the System32 files are not required by another application.
   c. Restore any files required by another application.
   d. Delete the directory.
5. Delete any remaining folders and files in the *`IC_INSTALL_DIR`*`\IC71\` directory.
6. Delete all shortcuts that you added to the desktop.

Uninstalling Avaya Agent Web Client

You must completely remove the Avaya Agent Web Client software and settings if you need to re-install the software.

This section includes the following topics:

Before you begin

Before you uninstall Avaya Agent Web Client, perform the following steps:

1. If necessary, start the IBM WAS administrative application.
2. Start the IBM WAS Administrative Console.

   For more information, see Applying the JACL scripts on page 344.
3. Stop the IBM WAS application server that hosts Avaya Agent Web Client.

   For more information, see Starting and stopping Avaya Agent Web Client on page 350.

Note:
Wait for application server to stop before you continue with Uninstalling the Avaya Agent Web Client application on page 445.

Uninstalling the Avaya Agent Web Client application

You uninstall the Avaya Agent Web Client application from the IBM WAS Administrative Console:

To uninstall the Avaya Agent Web Client application:

1. In the IBM WAS Administrative Console, select **Applications** > **Enterprise Applications**.
2. In the table, select the checkbox next to the Avaya Agent Web Client application.
3. Select **Uninstall**.
4. When the Uninstall application section appears, select **OK**.
5. When the uninstallation is completed, select **Save** in the upper message box.
6. In the **Save to the Master Configuration** pane, select **Save**.

Deleting the EAR application files

To delete the Enterprise application files:

- Delete the following folder:

  ***WAS_INSTALL_DIR*\AppServer\temp*WAS_MACHINE**WAS_APP_SERVER*\AAWC_Application folder.**

  where:

  - ***WAS_INSTALL_DIR*** is the location where you installed IBM WAS
  - ***WAS_MACHINE*** is the name of the machine that hosts IBM WAS
  - ***WAS_APP_SERVER*** is the IBM WAS application server where you deployed the Avaya Agent Web Client application.

  For example, if you installed IBM WAS in the default directory on a machine named testbox and hosted the Avaya Agent Web Client application on an application server named AAWC_APP_SERVER, you would delete the following folder:

  C:\Program Files\WebSphere\AppServer\temp\testbox\AAWC_APP_SERVER\AvayaAgentWebClient

Deleting the Web applications from IBM ASTK

To delete the Web applications from IBM ASTK:

1. In the **Resource** window of IBM ASTK, select the following projects:
   - web application
   - web
2. Right-click on the projects and select **Delete**.

3. In the Confirm Multiple Project Delete dialog box:
   a. Verify that **Do not delete contents** is selected.
   b. Select **Yes**.

Uninstalling Avaya Agent Web Client software

Follow the instructions in Uninstalling Avaya IC on page 440 to uninstall the Avaya Agent Web Client software.

Appendix C: Configuration Tool advanced properties

The **Web** tab includes advanced properties that specify the following properties for the Java Virtual Machine:

- Initial heap size and maximum heap size
- Stack size

Tip:
Configure the advanced properties only if you expect a high volume of contacts or access to the Web application. For example, configure the advanced properties for the Website and the ICM server if you expect a high volume of chat contacts from the customer Website. For information about performance and contact volume, see the benchmarking information available through an Avaya representative.

This section describes the advanced properties on the **Web** tab and how to access those properties. Topics include:

- Format of the advanced properties on page 448.
- Accessing the advanced properties on page 447.
- Advanced properties on page 448.
- Using the recommended settings for the advanced properties on page 449.

Accessing the advanced properties

To access the advanced properties on the **Web** tab of the Configuration Tool:

1. Right-click in an empty space on the **Web** tab.
2. Check the box next to **Show Advanced Properties**.

Format of the advanced properties

The advanced properties use the following format:

-<initial_Java_heap> -<maximum_Java_heap>

where:

Format	Property	Description
initial_Java_heap	-Xms	Sets the initial Java heap size for the Tomcat application.
maximum_Java_heap	-Xmx	Sets the maximum Java heap size for the Tomcat application.

Advanced properties

The following table describes the fields on the **Web** tab for advanced properties.

Field	Description	Default value
Tomcat Setup	The Multiple option creates a separate Tomcat server for each Web application. Choose Multiple if the machine hosts more than one Web application, and you want to start and stop all Web applications separately.	Multiple
Web License Manager JVM Options	Available only when you select **Configure Web License Manager**. Entries must use the following format: *-<min_heap> -<max_heap>*	Default: `-Xms32m -Xmx64m`
Email Template Administration JVM Options	Available only when you select **Configure Email Template Administration**. Entries must use the following format: *-<min_heap> -<max_heap>*	Default: `-Xms32m -Xmx64m`
Website JVM Options	Available only when you select **Configure Website**. Entries must use the following format: *-<min_heap> -<max_heap>*	Default: `-Xms32m -Xmx64m`

Field	Description	Default value
ICM JVM Options	Available only on Windows, when you select **ICM Service**. Entries must use the following format: -<*min_heap*> -<*max_heap*>	Default: `-Xms32m -Xmx64m`
CIRS JVM Options	Available only when you select **CIRS Service**. Entries must use the following format: -<*min_heap*> -<*max_heap*>	Default: `-Xms32m -Xmx64m`

Using the recommended settings for the advanced properties

The recommended tuning parameters in *IC Administration Volume 1: Servers & Domains* also includes some recommended settings for the advanced properties.

After you install the development Avaya IC system as described in this document:

1. Review the tuning parameters in *IC Administration Volume 1: Servers & Domains*.
2. Verify the expected contact volume in the production system.
3. Test the recommended settings for the tuning parameters to find the optimal settings for the production system.

Index

Symbols

A

B

C

D

E

F

G

H

I

J

K

L

M

N

O

P

Q

R

S

T

U

X