



Implementing Intelligent Customer Routing (ICR)

Release 6.0
August 2011

Notice

While reasonable efforts have been made to ensure that the information in this document is complete and accurate at the time of printing, Avaya assumes no liability for any errors. Avaya reserves the right to make changes and corrections to the information in this document without the obligation to notify any person or organization of such changes.

Documentation disclaimer

"Documentation" means information published by Avaya in varying mediums which may include product information, operating instructions and performance specifications that Avaya generally makes available to users of its products. Documentation does not include marketing materials. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of documentation unless such modifications, additions, or deletions were performed by Avaya. End User agrees 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 End User.

Link disclaimer

Avaya is not responsible for the contents or reliability of any linked Web sites referenced within this site or documentation provided by Avaya. Avaya is not responsible for the accuracy of any information, statement or content provided on these sites and does not necessarily endorse the products, services, or information described or offered within them. Avaya does not guarantee that these links will work all the time and has no control over the availability of the linked pages.

Warranty

Avaya provides a limited warranty on its Hardware and Software ("Product(s)"). 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 to Avaya customers and other parties through the Avaya Support Web site: <http://support.avaya.com>. Please note that if you acquired the Product(s) from an authorized Avaya reseller outside of the United States and Canada, the warranty is provided to you by said Avaya reseller and not by Avaya.

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, [HTTP://SUPPORT.AVAYA.COM/LICENSEINFO/](http://support.avaya.com/licenseinfo/) ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AUTHORIZED AVAYA RESELLER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AUTHORIZED AVAYA RESELLER. UNLESS OTHERWISE AGREED TO BY AVAYA IN WRITING, AVAYA DOES NOT EXTEND THIS LICENSE IF THE SOFTWARE WAS OBTAINED FROM ANYONE OTHER THAN AVAYA, AN AVAYA AFFILIATE OR AN AVAYA AUTHORIZED RESELLER; AVAYA RESERVES THE RIGHT TO TAKE LEGAL ACTION AGAINST YOU AND ANYONE ELSE USING OR SELLING THE SOFTWARE WITHOUT A LICENSE. BY INSTALLING, DOWNLOADING OR USING THE SOFTWARE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE INSTALLING, DOWNLOADING OR USING THE SOFTWARE (HEREINAFTER REFERRED TO INTERCHANGEABLY AS "YOU" AND "END USER"), AGREE TO THESE TERMS AND CONDITIONS AND CREATE A BINDING CONTRACT BETWEEN YOU AND AVAYA INC. OR THE APPLICABLE AVAYA AFFILIATE ("AVAYA").

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 originally sold by Avaya and ultimately utilized by End User.

License types

Designated System(s) License (DS). End User may install and use each copy of the Software on only one Designated Processor, unless a different number of Designated Processors is indicated in the Documentation or other materials available to End User. Avaya may require the Designated Processor(s) to be identified by type, serial number, feature key, location or other specific designation, or to be provided by End User to Avaya through electronic means established by Avaya specifically for this purpose.

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 Software that permits one user to interface with the Software. Units may be linked to a specific, identified Server.

Database License (DL). End User 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.

CPU License (CP). End User may install and use each copy of the Software on a number of Servers up to the number indicated by Avaya provided that the performance capacity of the Server(s) does not exceed the performance capacity specified for the Software. End User may not re-install or operate the Software on Server(s) with a larger performance capacity without Avaya's prior consent and payment of an upgrade fee.

Named User License (NU). End User may: (i) install and use the Software on a single Designated Processor or Server per authorized Named User (defined below); or (ii) install and use the Software on a Server so long as only authorized Named Users access and use the Software. "Named User", means a user or device that has been expressly authorized by Avaya to access and use the Software. At Avaya's sole discretion, a "Named User" may be, without limitation, designated by name, corporate function (e.g., webmaster or helpdesk), an e-mail or voice mail account in the name of a person or corporate function, or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software.

Shrinkwrap License (SR). Customer may install and use the Software in accordance with the terms and conditions of the applicable license agreements, such as "shrinkwrap" or "clickthrough" license accompanying or applicable to the Software ("Shrinkwrap License"). (see "Third-party Components" for more information).

Copyright

Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation, Software, or Hardware provided by Avaya. All content on this site, the documentation and the Product provided by Avaya including the selection, arrangement and design of the content is owned either by Avaya or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. You may not modify, copy, reproduce, republish, upload, post, transmit or distribute in any way any content, in whole or in part, including any code and software unless expressly authorized by Avaya. Unauthorized reproduction, transmission, dissemination, storage, and or use without

the express written consent of Avaya 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 regarding distributed Linux OS source code (for those Products that have distributed the Linux OS source code), and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply to them is available on the Avaya Support Web site: <http://support.avaya.com/Copyright>.

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 Toll 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://support.avaya.com>. Suspected security vulnerabilities with Avaya products should be reported to Avaya by sending mail to: securityalerts@avaya.com.

Trademarks

The trademarks, logos and service marks ("Marks") displayed in this site, the Documentation and Product(s) provided by Avaya are the registered or unregistered Marks of Avaya, its affiliates, or other third parties. Users are not permitted to use such Marks without prior written consent from Avaya or such third party which may own the Mark. Nothing contained in this site, the Documentation and Product(s) should be construed as granting, by implication, estoppel, or otherwise, any license or right in and to the Marks without the express written permission of Avaya or the applicable third party.

Avaya is a registered trademark of Avaya Inc.

All non-Avaya trademarks are the property of their respective owners, and "Linux" is a registered trademark of Linus Torvalds.

Downloading Documentation

For the most current versions of Documentation, see the Avaya Support Web site: <http://support.avaya.com>.

Contact 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 Web site: <http://support.avaya.com>.

Contents

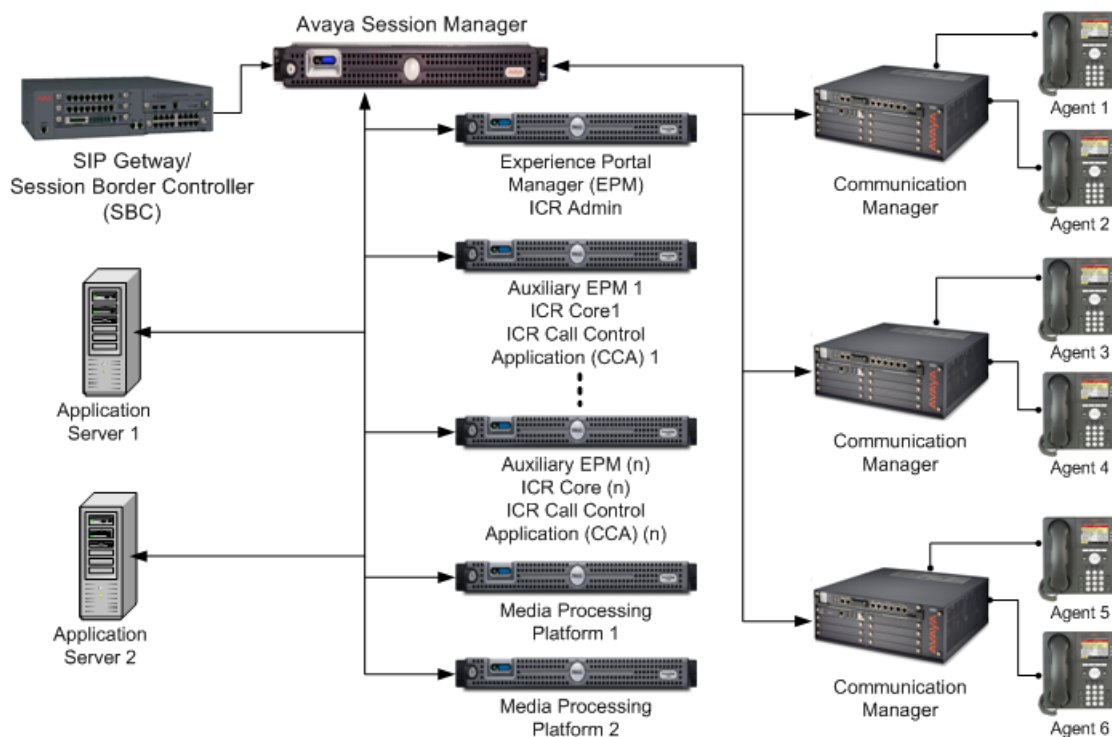
Chapter 1: Introduction.....	7
Benefits.....	8
Features.....	9
Components.....	11
ICR Admin.....	11
ICR Core.....	12
ICR Call Control Application (CCA).....	12
Chapter 2: Deployment Scenarios for ICR.....	13
Deploying ICR.....	13
ICR deployment models.....	13
Deploying ICR in the single site contact center environment.....	14
Deploying ICR in the single data center and multiple contact centers environment.....	14
Deploying ICR in the multiple data centers and multiple contact centers environment.....	15
Chapter 3: Installing Intelligent Customer Routing (ICR).....	17
Intelligent Customer Routing requirements.....	17
About ICR installation.....	17
Installing ICR Admin.....	19
Installing ICR CCA.....	21
Installing ICR Core.....	23
Installing ICR on a single system.....	26
Installing ICR Core on multiple systems.....	31
Configuring Terracotta server in the high availability mode.....	31
Installing ICR using silent installer.....	35
Chapter 4: Configuring Avaya Aura® Communication Manager.....	39
Log in to the CM server.....	39
Adding Session Manager IP Address.....	39
Creating a signaling-group.....	40
Creating a Trunk group.....	42
Creating Hunt group.....	43
Creating a Vector for polling VDN.....	44
Creating a Vector for Queuing VDN.....	45
Creating a Polling VDN.....	46
Creating a Queue VDN.....	48
Adding the Queuing VDN to public unknown numbering plan.....	49
Adding the IP Network Region.....	50
Adding the IP codec set.....	51
Chapter 5: Configuring Avaya Aura® Session Manager.....	53
Logging on to System Manager Web interface.....	53
Adding a SIP domain.....	54
Adding SIP Entities/Elements.....	54
Adding SIP Entity for SIP Gateway or Session Border Controller (SBC).....	54
Adding SIP Entities for Communication Manager.....	55
Adding SIP Entity for Avaya Aura® Experience Portal.....	56
Adding SIP Entities for ICR Core.....	57

Adding SIP Entity links.....	58
Adding SIP Entity Link for SIP Gateway or SBC.....	58
Adding SIP Entity Link for Communication Manager.....	59
Adding SIP Entity Link for Avaya Aura® Experience Portal.....	60
Adding SIP Entity Link for ICR Core Server.....	61
Defining Policies and Time of Day.....	62
Adding Routing Policy for Communication Manager.....	62
Adding Routing Policy for Avaya Aura® Experience Portal.....	63
Dial Patterns.....	64
Adding dial plan for Avaya Aura® Experience Portal and Communication Manager.....	64
Adding ICR user on System Manager.....	65
Chapter 6: Configuring Avaya Aura® Experience Portal.....	67
About configuring Avaya Aura® Experience Portal.....	67
Adding a SIP connection for Session Manager.....	67
Chapter 7: Installing Pluggable Data Connector.....	69
Pluggable Data Connector (PDC).....	69
Copying PDC to the plugins folder in Orchestration Designer.....	69
Importing sample applications in Eclipse.....	70
Enabling Pluggable Data Connector plug-in for the SSA application.....	71
Chapter 8: Application Server.....	73
About application server.....	73
Importing ICR Core certificate on the application server.....	73
Chapter 9: Configuring ICR properties.....	75
ICR Core property file description.....	75
ICR CCA property file description.....	78
ICR Admin property file description.....	81
Chapter 10: Uninstalling Intelligent Customer Routing.....	85
Uninstalling ICR components installed on a standalone system.....	85
Uninstalling ICR installed in a silent mode.....	86
Appendix A: ICR CCA properties configuration for EWT or queue position update and spike.....	89
Appendix B: Ports used by ICR.....	93
Appendix C: Mounting the ICR media.....	95
Mounting the ISO image of the ICR installer.....	95
Mounting the ICR installer CD or DVD.....	96
Index.....	99

Chapter 1: Introduction

Intelligent Customer Routing (ICR) helps businesses to capitalize on the next competitive differentiator in the Customer Experience. ICR provides enhanced customer service experience by identifying and determining caller intent through simple, intelligent, customer conversations using speech and self service. ICR provides the opportunity for customers to serve themselves and, when needed, determines the most optimal route to provide live assistance to that end consumer leveraging resources enterprise wide. Avaya has unified self and assisted service into a single smart call routing solution that dynamically manages available media and IT resources while enabling a personalized high-value service from start to finish.

Following diagram gives an overall picture of how you can implement ICR in your system.



With ICR, Avaya begins the transition to the next generation contact centers by leveraging Avaya's next generation enterprise communication architecture, Avaya Aura®. This user centric architecture focuses on any-media, any-application, and any-device from the ground up. Earlier contact center solutions have used computer telephony integration (CTI) to collaborate number of different applications and protocols into complex solutions. These

solutions were difficult to deploy, operate, and support. ICR removes the complexity, leveraging Session Initiation Protocol (SIP) for standards based integration and delivery of information or contact to any resource within or external to the enterprise.

As soon as a call arrives, a customer can be greeted intelligently based on business insights. While customers are waiting for live agents, Intelligent Customer Routing can present personalized up-sell or cross-sell messages, call-back options, and even opt-in services to pro-actively notify customers of transaction status before the call even occupies resources on an ACD.

For example:

- Determine if this customer has talked to anyone in the past regarding their need and if the customers would like to be connected to the same resource.
- Gather more information about a caller based on a request; location of home purchase for which the caller need a loan, existing loan number, and an order number.
- Offer an opportunity only to premium customers (and tell the customers that the opportunity is specific for them as highly valued customers) to pre-register for the service when the service becomes available.
- Ask customers about their experience with a previous purchase (could be a tool, a cell phone, a toaster, or a travel experience). Based on that feedback – react.
- Reference customers to a local help desk that will offer configuration and assistance free of charge. Send them an e-mail with a quick tips guide.

Related topics:

[Benefits](#) on page 8

[Features](#) on page 9

Benefits

Following are the benefits of using Avaya Intelligent Customer Routing:

- Manage calls faster and more intelligently, to enhance customer service experience and increase customer loyalty.
- Conduct productive or business useful activities while the caller is in queue. Calls are initially delivered to a portal and routed to an ACD only when agent assistance is required. Self-service no longer consumes ACD resources or requires Interactive Voice Response (IVR) agent licenses.
- Keep your existing agent endpoints, call-routing systems and other resources, thereby preserving existing investments.
- Lower ownership costs by saving money on deployment and maintenance due to streamlined management and improved call distribution.

- Scale beyond the capacity limitations of a single Automatic Call Distribution (ACD). Avaya ICR is applicable to both single site and multi site ACD customers.
- Disaster Management: When an ACD is down, the calls queued to that ACD are not lost, ICR re-queues the call to other available ACDs without the knowledge of the customer.
- Reduce the complexity of administering a solution. This includes Best Service Routing (BSR) as well as the self service and Wait Treatment Applications (WTA). You can perform BSR administration from a single console. This helps in reducing code complex vectors.
- Information transport is through Session Initiation Protocol (SIP). Leveraging the power of SIP, Avaya ICR lets customers connect with agents and subject experts anywhere in the enterprise.
- Application scripting is based on Voice XML (VXML) and Call Control XML (CCXML) standards and is consolidated onto a single, industry-standard, Eclipse-based application development environment called the Avaya Aura® Orchestration Designer.

Features

Intelligent Customer Routing or ICR provides features to efficiently handle customer calls for an organization. In ICR, calls are either completely served through self service applications or intelligently routed to a relevant call center across applicable geographic locations based on the best available source of real-time data.

You can use the following features to provide the necessary self service and routing:

Self Service First using Avaya Aura® Experience Portal

Self Service first is provided through Avaya Aura® Experience Portal as the first point of access to an organization. Calls connect to a Avaya Aura® Experience Portal application prior to connecting an Automatic Call Distribution (ACD).

Intelligent Routing

In a contact center, agents or experts are the most valuable and most expensive resources. Therefore organizations must effectively utilize agents or experts.

Using Avaya Voice Portal as the call control point, the Intelligent Customer Routing solution selects among a group of contact center locations and routes the caller to the most optimal contact center and the best-suited agent at that time. With the Best Service Routing (BSR) infrastructure ICR locates the best location for a call based on the shortest queue and skill availability.

ICR also has the ability to self service customers or place a virtual call, parked it on the ACD, and provide an enhanced wait treatment.

Enhanced or Advanced Wait Treatment

In ICR, while a call is queued to Communication Manager, an advanced wait treatment application is played for caller. This enables self service or predictive offers to be provided

while a call is in queue awaiting an agent to become available. This queue time can be used for activities such as:

- Information Gathering – gathers additional information necessary to provide to an agent upon call delivery.
- Issue resolution – provides information to, or gathers information from a customer in the interest of resolving an issue (zip code needed for order shipment).
- Up sell – offer customers opportunities based on previous activities or purchases or play special messages regarding new promotions as applicable to a customers profile.
- Opt-in Services – provide customer ability to sign up for new value added services such as SMS messages with bill due dates and amounts, and shipment information.
- Call back assist – provide call back options for a customer based on estimated (or predicted) queue wait times.
- The wait treatments can be configured to play based on the length of the wait time

When an agent becomes available, the caller is connected to the agent.

Reporting

Avaya ICR provides real-time monitoring and historical reporting.

In real-time monitoring, you can view the application and queued call status in real-time. In the status, you can view the calls for each applications, call for a particular skill, or calls for a particular call center.

In the historical reporting, you can view the details of calls that ICR Call Control Application (CCA) sessions handled and processed. The report includes information from the time a call arrives in the ICR CCA session up to the call exit from the ICR CCA session.

Pluggable Data Connector (PDC)

Pluggable Data Connector (PDC) is a connector between Self Service Application (SSA) and ICR Core.

ICR PDC is built to integrate ICR into Avaya Aura® Orchestration Designer. ICR PDC is a generic connector, which an application developer can use without knowledge of call centers and ICR Core. The purpose of ICR PDC is to provide a SIP URI, which is the routing destination for a skill.

Sample Applications

If you wish to use sample templates to start definition of segmentation and wait treatment, Avaya ICR provides the following sample Orchestration Designer VXML applications to demonstrate how caller segmentation, wait treatment, and self-service applications can be incorporated into an ICR application. These applications are reusable templates that can be further customized to meet customer scenarios.

- SSA - Self Service Application
- WTA - Wait Treatment Application
- EHA - Error Handling application

Avaya Aura® Experience Portal integration

Seamless integration with Avaya Aura® Experience Portal for:

- Administration, Configuration, Management, Serviceability and Licensing.
- User management and assigning ICR specific roles to users.
- Monitor alarms and different types of logs like audit logs, information logs, and error logs.
- Backup and restore operations.

Components

The ICR architecture consists of the following three components:

- [ICR Admin](#) on page 11
- [ICR Core](#) on page 12
- [ICR Call Control Application \(CCA\)](#) on page 12

ICR Admin

ICR Admin provides configuration and administration of:

- ICR components, such as core, skills, VDNs, call centers, and business hours and holidays. For each component, you can access the corresponding Web page and configure the associated parameters for that component. ICR Core uses call centre, skill, and VDN information to identify the best resource available for a call.
- ICR applications, such as Self Service Application (SSA), Wait Treatment Applications (WTAs), Error Handling Applications (EHAs), and Non Business Hours Application.
- ICR reports, such as standard report for Call Control Application (CCA) sessions.
- ICR application and queued calls
- ICR licenses for core and reports.
- ICR logs, such as audit logs, alarms and events.
- ICR user roles, such as ICR administration and ICR reporting.

In a single system setup or a multi-system setup, ICR Admin is deployed on a primary Experience Portal Manager (EPM) system.

ICR Core

ICR Core routes the calls to the best resource available. ICR Core consists of a skill selection module called Best Service Routing (BSR) to route calls to the Communication Manager (CM). BSR module utilizes Avaya's Vector capability that uses Expert Agent Selection (EAS) for making routing decisions and provides the best location or skilled agent to which the call can be queued.

In a single system setup, ICR Core is deployed on a primary Experience Portal Manager (EPM) system and in a multi-system setup, ICR Core is either deployed on an auxiliary Experience Portal Manager (EPM) system or on a standalone system.

ICR Call Control Application (CCA)

Call Control Application (CCA) is a CCXML application that coordinates all the call activities, move calls between dialogs, and queue calls at a contact center. When a call arrives, ICR CCA answers the call and launches the Self Service Application (SSA). The SSA handles the call and if the caller requires additional information with the self services, CCA launches the Wait Treatment Application (WTA) and a call is queued in the call center for an agent. The CCA re-queues a call to a different CM in case of a CM failure.

The Error Handling Application (EHA) handles errors in a call flow.

ICR Applications are Orchestration Designer based application. ICR provides following sample Application:

- SSA: Self service application
- WTA: Wait Treatment application
- EHA: Error Handling application

You can further customize the above sample applications according to your requirements.

In a single system setup, ICR CCA is deployed on a primary Experience Portal Manager (EPM) system and in a multi-system setup, ICR CCA is either deployed on an auxiliary Experience Portal Manager (EPM) system or on a standalone system.

Chapter 2: Deployment Scenarios for ICR

Deploying ICR

You can deploy the ICR components; ICR Core and ICR CCA either on a primary or an auxiliary Experience Portal Manager system or on a standalone system. However, you must deploy the ICR Admin component on a primary Experience Portal Manager system. Based on the scalability, load balancing and failover requirement, you can create multiple instances of ICR Core and ICR CCA.

Host the ICR Core and ICR CCA on the Tomcat Application server provided with the installer.

You can deploy sample ICR VXML applications along with ICR PDC on an application server provided by a customer. You can also change the sample VXML application according to your requirements.

ICR deployment models

Single system setup

In a single system setup, deploy ICR components, such as ICR Admin, ICR Core, and ICR CCA on a primary Experience Portal Manager system and deploy ICR Applications on the same system or on another application server.

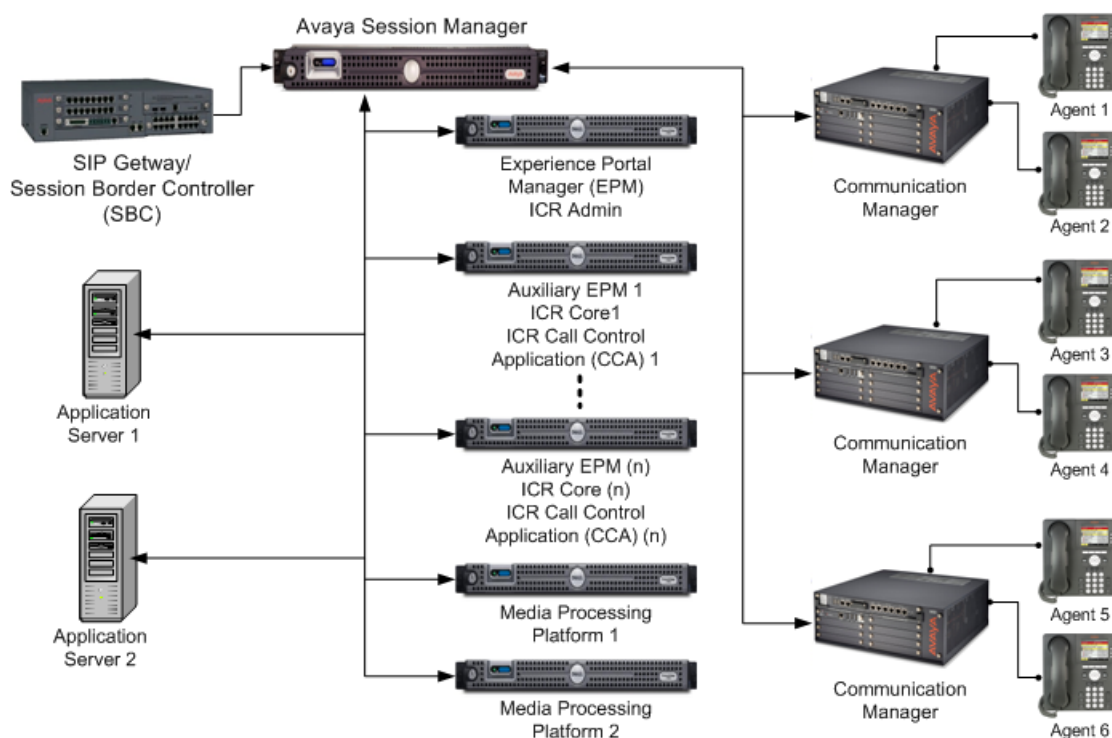
Multi-system setup

In a multi-system setup, deploy ICR component, such as ICR Admin on a Primary Experience Portal Manager system and deploy ICR Core and ICR CCA on one or more auxiliary Experience Portal Manager systems or on a standalone system.

Deploying ICR in the single site contact center environment

Single site contact center model consist of:

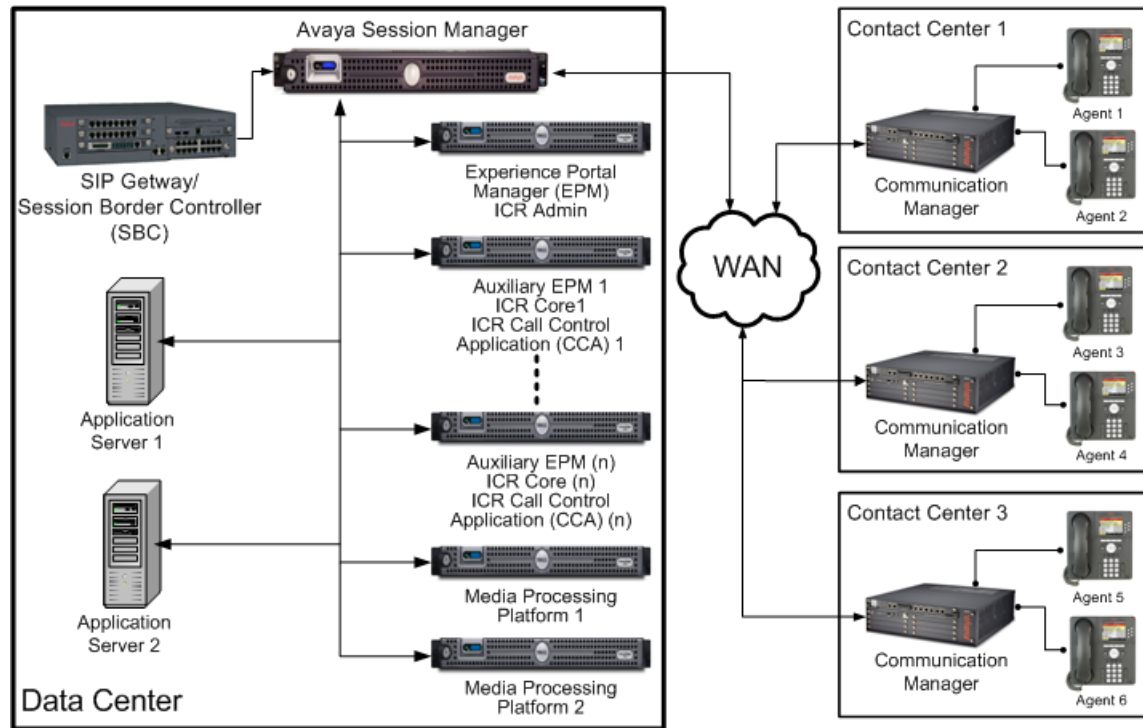
- SIP gateway or Session Border Controller (SBC)
- Session Manager
- Experience Portal Manager components
- ICR components
- One or more Communication Manager in one site



Deploying ICR in the single data center and multiple contact centers environment

A single data center model with multiple contact centers consist of a single data center having a common ingress point for all calls arriving in the system. This data center will comprise of

SIP gateway or Session Border Controller (SBC), Session Manager, Experience Portal Manager, ICR components hosted in one place. There will be multiple contact centers with multiple Communication Manager outside the data center.



Deploying ICR in the multiple data centers and multiple contact centers environment

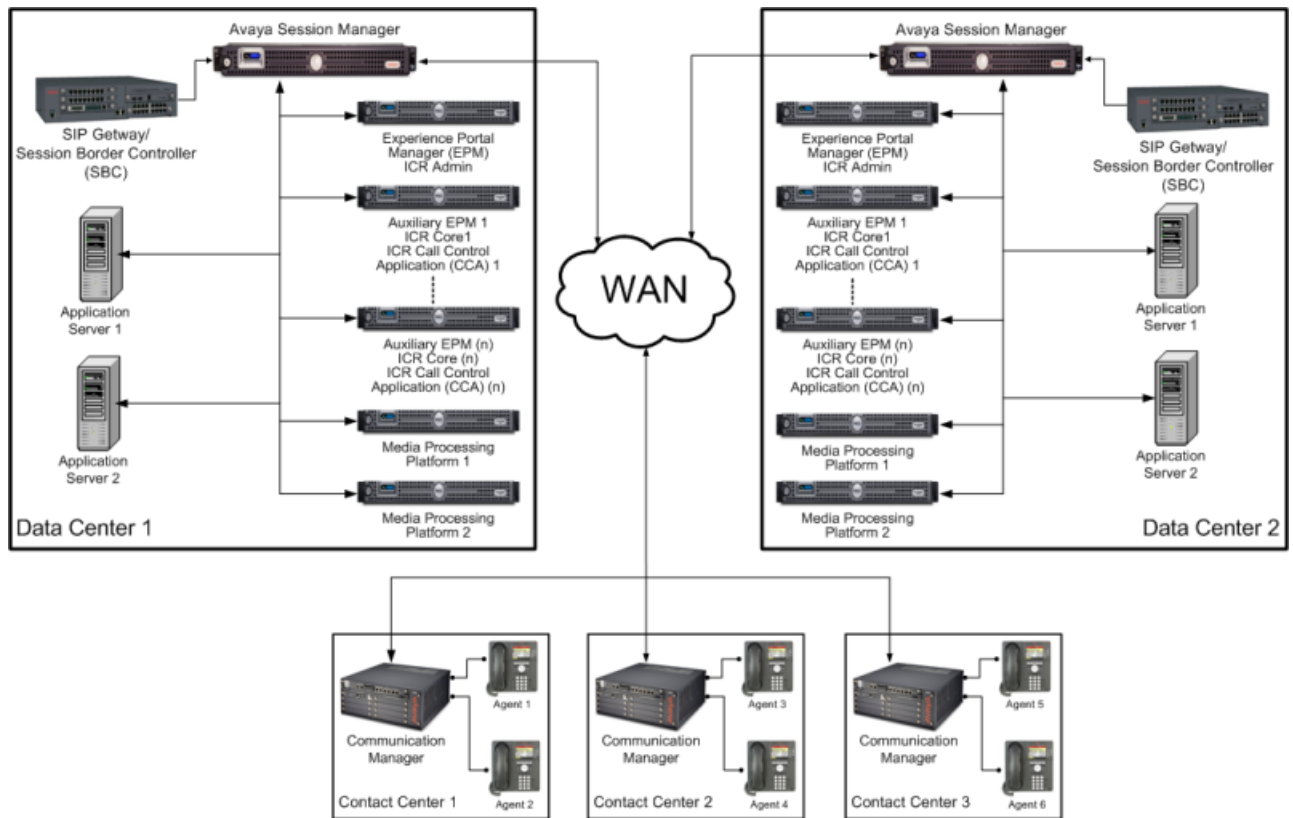
In a multiple data center model, multiple contact centers consists of each datacenter having ingress point for calls arriving in their system. These data center will comprise of SIP gateway or Session Border Controller (SBC), Session Manager, Experience Portal Manager, ICR components hosted in one place. There will be multiple contact centers with multiple Communication Manager outside data centers. The Avaya session manager across data centers will leverage distributed Session Manager model.

ICR Monitor and Standard Reports will be available in Experience Portal Manager using centralized reporting database.

Note:

For the configuration of external reporting database, refer to the Administration guide of Experience Portal Manager, available at the Avaya support site: <http://support.avaya.com>.

Deployment Scenarios for ICR



Chapter 3: Installing Intelligent Customer Routing (ICR)

Intelligent Customer Routing requirements

ICR is a managed application of Avaya Aura® Experience Portal. Therefore, hardware and software specifications applicable for Avaya Aura® Experience Portal are also applicable for ICR.

Following are the software requirements for ICR.

- Avaya Aura® Experience Portal version 6.0
- Avaya Aura® Session Manager (version 5.2 or 6.x)
- Avaya Aura® Communication Manager (version 5.2.1 and later)
- Avaya Aura® Session Border Controller
- Application Server
- Speech Server
- SIP Gateways or Session Border Controller (SBC)



Note:

For more information about the hardware requirements, see the *Minimum (Linux) server machine hardware requirements* topic in the Avaya Aura® Experience Portal documentation.

About ICR installation

ICR consists of the following components:

- ICR Admin
- ICR Call Control Application (CCA)
- ICR Core

To install the ICR components, run the ICR installer on a single system or install individual components on multiple systems.



Note:

When you install ICR without installing the ICR licenses, the License page of Avaya Aura® Experience Portal displays the license count of ICR Core and ICR Reporting as 1. This count indicates that you can use ICR for an initial trial period of 30 days. After the trial period, you must install the ICR license to continue using ICR. For more information about installing ICR licenses, see the ICR Administration guide.

Single system installation

You can install all the ICR components on a single system. However, you must install the ICR Admin component on the primary Experience Portal Manager system.



Note:

In the single system installation of ICR, you must configure different SIP listener ports for Media Processing Platform (MPP) and ICR Core. For ICR Core, you can modify the `ICRSipTCPPort` property in the `icrcore.properties` file available in the `$AVAYA_ICRCORE_HOME/tomcat/conf` directory.

Multi-system installation

You can install ICR components separately on multiple systems.

Following are the system requirements for multi-system installation:

- ICR Admin

You must install this component on a primary Experience Portal Manager system.

- ICR CCA and ICR Core

You can install these components on an auxiliary Experience Portal Manager system or a standalone Linux system.



Note:

If you installing ICR Core or ICR CCA on a standalone Redhat Enterprise Linux system, follow the prerequisites mentioned in the Chapter 2, “Customer-provided operating system installation” of the *Implementing Avaya Aura® Experience Portal on multiple servers guide*.



Important:

If you install ICR CCA and ICR Core on a standalone Linux system, the remote access using Secured Access Link (SAL) is not supported.

Silent installation

You can install ICR components in a silent mode. Silent installation is useful when you know the required install settings do not want to change the settings. Install ICR in a silent mode only when you know the install settings correctly.

Installing ICR Admin

Before you begin

Before installing ICR Admin, ensure that Avaya Aura® Experience Portal 6.0 is installed on that system.

If you are installing Avaya Aura® Experience Portal for the first time, see the *Avaya Aura® Experience Portal* documentation on the Avaya support site at: <http://support.avaya.com>.

Procedure

1. Mount the ICR installation media.
For information about mounting the installation media, see [Mounting the ICR media](#) on page 95
2. Type `./install_icr.bin` and press Enter to run the installer.
3. On the Introduction screen, press Enter.
4. On the License screen, press Enter.

Note:

Press Enter several times to browse through the complete license page.

The system displays Do you accept the terms of this license agreement?.

5. Type Y and press Enter to accept the license agreement.
6. On the Choose Install Path screen, press Enter to select the default path for installation.

You can provide an absolute directory path or use the default directory path.

7. On the Choose Install Set screen, type 1 in the Please choose the Features to be installed by this installer message and press Enter to select ICR Admin.

The system displays the selected feature with [X] besides the feature name.

Tip:

- By default, no components are selected. You can select or deselect the components by entering the choice.
- To go back to the previous page type back and press Enter.
- To select or deselect a feature, enter the number for the feature separated by a comma.
- To cancel the installation at any time, type quit and press Enter.

8. Press Enter to continue.

The system displays the Pre-Installation Summary screen with the summary information as shown below.

```
=====
Pre-Installation Summary
-----

Please Review the Following Before Continuing:

Product Name:
    ICR

Install Folder:
    /opt/Avaya/ICR

Product Features:
    ICRAdmin

Disk Space Information (for Installation Target):
    Required: 388,031,240 bytes
    Available: 40,685,842,432 bytes

PRESS <ENTER> TO CONTINUE:

=====
```

9. Press Enter to continue.

Before installing ICR, the installer checks for prerequisites and displays the summary of the results as shown below.

```
=====
ICR Admin Prerequisite Check status
-----

Prerequisite                Expected result      Found
Is EPM installed?           YES                  YES
Is EPM Version supported?    6.x                  6.0.0.0.2104
Is ICR Admin installed?      NO                   NO

PRESS <ENTER> TO CONTINUE:

=====
```

10. Press Enter to continue.
The installer starts installing ICR Admin.
11. Before starting the Experience Portal Manager services, the ICR Admin installer prompts for a confirmation. Press Enter to continue.
After the installer completes installing ICR Admin, the system displays a message for successful installation.
12. Press Enter to exit the installer.
13. Log out from the Linux session and log in to a new Linux session to make further configuration changes.
Updated environment variables are available in a new session.

Installing ICR CCA

Before you begin

Before installing ICR CCA, ensure that the system meets the following requirements:

- Avaya custom Linux or Red Hat Enterprise Linux 6.x.
- Minimum 4 GB RAM.

Procedure

1. Mount the ICR installation media.
For information about mounting the installation media, see [Mounting the ICR media](#) on page 95
2. Type `./install_icr.bin` and press Enter to run the installer.
3. On the Introduction screen, press Enter.
4. On the License screen, press Enter.

Note:

Press Enter several times to browse through the complete license page.

The system displays Do you accept the terms of this license agreement?

5. Type Y and press Enter to accept the license agreement.
6. On the Choose Install Path screen, press Enter to select the default path for installation.
The default installation path is `/opt/Avaya/ICR`.
7. On the Choose Install Set screen, the system displays the Please choose the Features to be installed by this installer message.

Tip:

- To go back to the previous page, type back and press Enter.
 - To select or deselect a feature, enter the number of a feature separated with a comma.
8. Type 2 and press Enter to select ICR CCA .
The system displays the selected feature with `[X]` besides the feature name.
 9. Press Enter to continue.

The system displays the Pre-Installation Summary screen, which displays the information similar to what is shown below:

```
=====
Pre-Installation Summary
```

```

-----
Please Review the Following Before Continuing:

Product Name:
    ICR

Install Folder:
    /opt/Avaya/ICR

Product Features:
    ICRCCA

Disk Space Information (for Installation Target):
    Required: 275,603,020 bytes
    Available: 1,929,621,504 bytes

PRESS ENTER TO CONTINUE:
=====

```

10. Press Enter to continue.

The installer checks for prerequisites before installing ICR CCA and shows a summary of the results similar to what is shown below.

```

=====
ICR CCA/ICR Core Prerequisite Check status
-----

```

Prerequisite	Expected result	Found
OS & Version:	AVAYA Linux/RHEL6.x	Red Hat Enterprise
Linux 6.0		
Memory:	4 GB	4.152 GB
Is ICR CCA installed?	NO	NO
Is ICR Core installed?	NO	NO

```

PRESS ENTER TO CONTINUE:
=====

```

11. Press Enter to continue.

The system displays EPM IP ADDRESS (DEFAULT: XXX.XXX.XXX.XXX):.

Here, XXX.XXX.XXX.XXX represents the IP Address of the Experience Portal Manager system.

12. Type the IP address of the primary Experience Portal Manager system and press Enter.

The installer starts installing ICR CCA.

 Note:

By default, ICR creates the install logs of ICR CCA in the ICRCCA_InstallLog.log and cca_install_script.log files located in the \$AVAYA_ICRCCA_HOME/logs directory. You can check the log files for any errors after installation.

The \$AVAYA_ICRCCA_HOME variable is available in the new Linux session and not in the same installation session.

13. Press Enter when the ICR CCA installer displays a message to start the ICR CCA service.

The installer completes the installation process and displays a message for successful installation.

14. Press Enter to exit the installer.

15. Log out from the Linux session and log in to a new Linux session to make further configuration changes.

 Important:

You must log in to a new Linux session because the updated environment variables are available only in the new session.

16. Restart the ICR CCA service if you have made any changes in the `icrcca.properties` file.

Enter the command: `/sbin/service icrcca restart`.

The installer configures the parameters in the `icrcca.properties` file located in the `$AVAYA_ICRCCA_HOME/tomcat/conf` directory. For more information about the `icrcca.properties` file, see [ICR CCA property file description](#) on page 78

 Note:

The Tomcat server installed for ICR CCA runs using the port 6080. Configure the CCXML URL on Experience Portal Manager system as `http://<machine_IP>:6080/ICRCCApp/jsp/start.jsp`

Here, the `<machine_IP>` is the IP address of the system where ICR CCA is running.

Installing ICR Core

Before you begin

Before installing ICR Core, ensure that the system meets the following requirements:

- Avaya custom Linux or Red Hat Enterprise Linux 6.x.
- Minimum 4 GB RAM.
- The IP address and host name of the Experience Portal Manager system exists in the `/etc/hosts` file so that ICR Core communicates with the primary Experience Portal Manager system.

Procedure

1. Mount the ICR installation media.

For information about mounting the installation media, see [Mounting the ICR media](#) on page 95

2. Type `./install_icr.bin` and press Enter to run the installer.
3. On the Introduction screen, press Enter.
4. On the License screen, press Enter.

The system displays a prompt message: Do you accept the terms of this license agreement?

 Note:

Press Enter several times to browse through the complete license page.

5. Type Y and press Enter to accept the license agreement.
6. On the Choose Install Path screen, press Enter to select the default path for installation.
The default path of installation is: `/opt/Avaya/ICR`.
7. On the Choose Install Set screen, the system displays the message: Please choose the Features to be installed by this installer.

 Tip:

- To go back to the previous page, type back and press Enter.
- To select or deselect a feature, enter the number for a feature separated by a comma.

8. Type 3 and press Enter to select ICR Core .
The system displays the selected feature with `[X]` besides the feature name.
9. Press Enter to continue.
The system displays the Pre-Installation Summary screen, which displays the information similar to what is shown below:

```
=====
Pre-Installation Summary
-----

Please Review the Following Before Continuing:

Product Name:
    ICR

Install Folder:
    /opt/Avaya/ICR

Product Features:
    ICRCore

Disk Space Information (for Installation Target):
    Required:  427,953,696 bytes
    Available: 2,074,517,504 bytes

PRESS ENTER TO CONTINUE:
```


10. Press Enter to continue.

The installer checks for prerequisites before installing ICR Core and shows a summary of the results similar to what is shown below.

```
=====
```

ICR CCA/ICR Core Prerequisite Check status		

Prerequisite	Expected result	Found
OS & Version:	AVAYA Linux/RHEL6.x	Red Hat Enterprise
Linux 6.0		
Memory:	4 GB	4.152 GB
Is ICR CCA installed?	NO	NO
Is ICR Core installed?	NO	NO
PRESS ENTER TO CONTINUE:		

```
=====
```

11. Press Enter to continue.

The system displays EPM IP ADDRESS (DEFAULT: XXX.XXX.XXX.XXX):

Here, XXX.XXX.XXX.XXX represents the IP Address of the Experience Portal Manager system.

12. Type the IP Address of the primary Experience Portal Manager system and press Enter.
13. On the Avaya Aura® Experience Portal Product ID screen, type the correct product ID of Avaya Aura® Experience Portal.
- You can find the product ID of Avaya Aura® Experience Portal on the System Monitor page.
- From the Experience Portal Manager main menu in the left navigation pane, click **Real-Time Monitoring > System Monitor**.
 - In the **Server Name** column, click the **EPM** link.
 - In the **General Information** area, the **Product ID** field displays the product ID of Avaya Aura® Experience Portal.
14. Press Enter to continue.

The installer starts the ICR Core installation process.

 Note:

By default, ICR creates the Core logs in the `$AVAYA_ICRCORE_HOME/tomcat/logs` directory and the installer log file `ICRCore_InstallLog.log` in the `$AVAYA_ICRCORE_HOME` directory. You can check the log files for any errors after installation.

The `$AVAYA_ICRCORE_HOME` variable is available in the new Linux session and not in the same installation session.

15. Press Enter when ICR Core installer displays a message to start the ICR Core service.

The installer completes the installation process and displays a message for successful installation.

16. Press Enter to exit the installer.

17. Verify that the `httpd` service is configured for an auto start.

Enter the following command to check the `httpd` service auto start status:

```
chkconfig httpd --list
```

Command output:

```
httpd      0:off  1:off  2:on   3:on   4:on   5:on   6:off
```

In the command output, check that the levels 2 to 5 displays the status as “on”.

If the status for the level 2 to 5 is “off”, configure the `httpd` service for auto start using the following command:

```
chkconfig httpd on
```

18. Reboot the system.

19. After the system starts, enter the following command to verify that the ICR Core service is running.

```
service icrcore status
```

The installer configures the parameters in the `icrcore.properties` file located in the `$AVAYA_ICRCORE_HOME/tomcat/conf` directory.

For more information on `icrcore.properties` file, see [ICR Core property file description](#) on page 75.

Installing ICR on a single system

About this task

ICR consists of three components.

- ICR Admin
- ICR Core
- ICR CCA

You can install the complete ICR on a single Avaya Aura® Experience Portal system, where primary Experience Portal Manager is running.

 Note:

- Running all the ICR components on single system can have an impact on ICR performance. Therefore, you must install ICR on a single system in a development environment.
- When installing ICR on a single system, you must configure different SIP listener ports for Media Processing Platform (MPP) and ICR Core. For ICR Core, you can modify the `ICRSipTCPPort` property in the `icrcore.properties` file located in the `$AVAYA_ICRCORE_HOME/tomcat/conf` directory. For MPP, you can modify the SIP listener ports on the VoIP Connection page of Experience Portal Manager.
- On the Avaya Session Manager, create the SIP entity link only for MPP and mark the link as trusted. Do not create a separate SIP entity link for ICR Core because ICR Core and MPP resides on a single system.

Procedure

1. Mount the ICR installation media.
For information about mounting the installation media, see [Mounting the ICR media](#) on page 95
2. Type `./install_icr.bin` and press Enter to run the installer.
3. On the Introduction screen, press Enter.
4. On the License screen, press Enter.
The system displays a prompt message: Do you accept the terms of this license agreement?

 Note:

Press Enter several times to browse through the complete license page.

5. Type Y and press Enter to accept the license agreement.
6. On the Choose Install Path screen, press Enter to select the default path for installation.
The default path for installation is `/opt/Avaya/ICR`.
7. On the Choose Install Set screen, the system displays the message: Please choose the Features to be installed by this installer.
The system displays the selected feature with an X next to the feature name.

 Tip:

- To go back to the previous page, type back and press Enter.
- To select or deselect a feature, enter the number representing the feature separated by a comma.
- To cancel installation, type quit and press Enter.

8. Type 1, 2, 3 and press Enter to select ICR Admin, ICR CCA, and ICR Core application.

The system displays the selected feature with *[X]* besides the feature name.

9. Press Enter to continue.

The system displays the Pre-Installation Summary screen, which displays the information similar to what is shown below:

```
=====
Pre-Installation Summary
-----

Please Review the Following Before Continuing:

Product Name:
    ICR

Install Folder:
    /opt/Avaya/ICR

Product Features:
    ICRAdmin,
    ICRCCA,
    ICRCore

Disk Space Information (for Installation Target):
    Required: 731,811,129 bytes
    Available: 2,039,353,344 bytes

PRESS ENTER TO CONTINUE:

=====
```

10. Press Enter to continue.

The installer checks for prerequisites before installing ICR Admin and shows a summary of the results as shown below.

```
=====
ICR Admin Prerequisite Check status
-----

Prerequisite          Expected result      Found
Is EPM installed?      YES                  YES
Is EPM Version supported? 6.x                  6.0.0.0.2104
Is ICR Admin installed? NO                     NO

PRESS ENTER TO CONTINUE:

=====
```

11. Press Enter to continue.

The installer checks for prerequisites before installing ICR Core and ICR CCA, and shows a summary of the results as shown below.

```
=====
=====
ICR CCA/ICR Core Prerequisite Check status
-----

Prerequisite          Expected result      Found
OS & Version:         AVAYA Linux/RHEL6.x  Red Hat Enterprise Linux 6.0
```

```

Memory:                4 GB                4.152 GB
Is ICR CCA installed?  NO                  NO
Is ICR Core installed? NO                  NO

PRESS <ENTER> TO CONTINUE:

=====
=====

```

12. Press Enter to continue.

The system displays EPM IP ADDRESS (DEFAULT: XXX.XXX.XXX.XXX) :

Here, xxx.xxx.xxx.xxx represents the IP Address of the Experience Portal Manager system on which you are installing ICR Core.

13. Type the IP Address of the primary Experience Portal Manager system and press Enter.
14. On the Avaya Aura® Experience Portal Product ID screen, type the Product ID of the Avaya Aura® Experience Portal system.
You can find the product ID of Avaya Aura® Experience Portal on the System Monitor page.
 - a. From the Experience Portal Manager main menu in the left navigation pane, click **Real-Time Monitoring > System Monitor**.
 - b. In the **Server Name** column, click the **EPM** link.
 - c. In the **General Information** area, the **Product ID** field displays the product ID of Avaya Aura® Experience Portal.
15. Press Enter to continue.
The installer starts installing ICR Admin.



Note:

By default, ICR create the Admin logs in the ICRAdmin_InstallLog.log and icr_install_script.log files located in the \$AVAYA_ICRADMIN_HOME/logs directory. Check the log files for any post installation errors.

The \$AVAYA_ICRADMIN_HOME variable is available in the new Linux session and not in the same installation session.

16. Press Enter when ICR Admin displays a message to start the ICR Admin service.
The installer completes the installation process of ICR Admin and displays a message for successful installation.
17. Press Enter when ICR CCA installer displays message to start the ICR CCA service.
The installer completes the installation process of ICR CCA and displays a message for successful installation.
18. Press Enter to continue.

 Note:

By default, ICR create the CCA logs in the `ICRCCA_InstallLog.log` and `cca_install_script.log` files located in the `$AVAYA_ICRCCA_HOME/logs` directory. Check the log files for any post installation errors.

The `$AVAYA_ICRCCA_HOME` variable is available in the new Linux session and not in the same installation session.

19. Press Enter when ICR Core displays a message to start the ICR Core service.
The installer completes the installation process of ICR Core and displays a message of successful installation.
20. Press Enter to continue.

 Note:

By default, ICR create the Core logs in the `ICRCore_InstallLog.log` file located in the `$AVAYA_ICRCORE_HOME` directory. Check the log file for any post installation errors.

21. Press Enter to exit the installer.
22. Reboot the system.
You must reboot the system and log in to the new Linux session as the updated environment variables are available only in the new session.
23. Configure the `icrcca.properties` file located in the `$AVAYA_ICRCCA_HOME/tomcat/conf` directory.
For more information on `icrcca.properties` file, see [ICR CCA property file description](#) on page 78.
24. Restart the ICR CCA service for the changes made in the `icrcca.properties` file to take effect.
Enter the command: **service icrcca restart**.

 Note:

Tomcat server installed for CCA runs using port 6080. Configure the CCXML URL on Experience Portal Manager as `http://<machine_IP>:6080/ICRCCApp/jsp/start.jsp`

Here, the `<machine_IP>` is the IP address of the system where ICR CCA is running.

25. Configure the `icrcore.properties` file located in the `$AVAYA_ICRCORE_HOME/tomcat/conf` directory.
For more information on `icrcore.properties` file, see [ICR Core property file description](#) on page 75.
26. Restart the ICR Core service for the changes made in the `icrcore.properties` file to take effect.

Enter the command: **service icrcore restart.**

Installing ICR Core on multiple systems

About this task

To install multiple ICR Core, first install ICR Core on a system and configure the Terracotta server in high availability mode.

Procedure

1. Install ICR Core.
For more information, see [Installing ICR Core](#) on page 23.
 2. Configure Terracotta server on each system where you installed ICR Core.
For more information, see [Configuring Terracotta server in the high availability mode](#) on page 31
-

Related topics:

[Configuring Terracotta server in the high availability mode](#) on page 31

Configuring Terracotta server in the high availability mode

About this task

ICR uses a cache to store the skill related information, for example best queue VDN for a skill, polled from multiple ACDs. So, when a call comes, ICR Core checks the cache for the available information instead of polling information from ACD. This reduces the time required to collect the required information.

ICR uses a third party server called Terracotta server for managing cache. Terracotta server is installed automatically on a system where you install ICR Core. Therefore, each ICR Core system has a local Terracotta server. However, you can configure Terracotta server in high availability mode with no point of failure. In high availability mode, multiple ICR Core systems share the same cache to find the required information. For example, If there are two ICR Core systems, you can configure the Terracotta server on one system as active and on another system as passive mode. In this configuration, both ICR Core systems share the cache from the active Terracotta server.

This topic gives step by step information about configuring Terracotta server in high availability mode.

**Note:**

Before you configure Terracotta server for high availability, stop all the ICR Core and Terracotta server instances.

Procedure

1. Log in to the ICR Core system on which you want to configure Terracotta in the high availability mode.
2. Log on to the Linux system either locally as a root user or remotely as a non-root user and change the user to root by using the **su -** command.
3. If you are an Avaya Services representative and if you are using Avaya Enterprise Linux or if the Avaya Service accounts are installed on this Core system:
 - Log on to the local Linux system as a sroot user.
 - Or log on remotely as a non-root user and change the user to sroot by entering the **su - sroot** command.
4. Enter the following command to stop ICR Core instances on each system.
/sbin/service icrcore stop
5. Enter the following command to stop the Terracotta server instances on each system.
/sbin/service terracottaSrv stop
6. On the ICR Core system, which you want to make an active Terracotta server open the directory configured in the `$AVAYA_ICRCORE_HOME` environment variable:
 - a. From the directory, back up the `icr-tc-config.xml` configuration file:
Enter the following command:
cp icr-tc-config.xml icr-tc-config.xml.old
 - b. Open the `icr-tc-config.xml` configuration file to edit.
 - c. In the configuration file, search for the `<server>` tag.
 - d. In the `<server>` tag:
 - Change the value of the *host* attribute with the IP address of the ICR Core system .
 - Keep the default value of the *name* attribute as it is.

For example:

```
=====
===
<server host="192.168.0.1" name="Server1">
  <dso>
    <persistence>
      <mode>Permanent-store</mode>
    </persistence>
  </dso>
</server>
```



```
=====
===
```

- e. In the same configuration file, add another `<server>` tag for the ICR Core system on which you want to host another instance of Terracotta server.

You can copy and paste the existing `<server>` tag.

- f. In the new `<server>` tag:

- Change the value of the *host* attribute to the IP address of another ICR Core system.
- Change the value of the *name* attribute to `Server2`.

For example:

```
=====
===
<server host="192.168.0.2" name="Server2">
  <dso>
    <persistence>
      <mode>Permanent-store</mode>
    </persistence>
  </dso>
</server>
=====
===
```

- g. In the same configuration file, search for the `<ha>` tag and remove the commenting mark given to the tag.

For example:

```
=====
===
<ha>
  <mode>networked-active-passive</mode>
  <networked-active-passive>
    <election-time>5</election-time>
  </networked-active-passive>
</ha>
=====
===
```

- h. Save the changes and close the file.
- i. Go to the `$AVAYA_ICRCORE_HOME/bin` directory.
- j. Open the startup configuration script file `start-tc-server.sh` to edit.
- k. Verify that the string `Server1` is present in the following code line.
- ```
$icrhome/terracotta-server/bin/start-tc-server.sh -n Server1 -f
$icrhome/icr-tc-config.xml > $TEMP_FILE 2>&1 &
```
- l. Start the Terracotta server that you named as `Server1`.  
Enter the following command:
- ```
/sbin/service terracottaSrv start
```
- m. Verify whether the Terracotta server started in the active mode.

Open the `avaya.service.terra.log` file available in the `$AVAYA_ICRCORE_HOME` directory. In the log file, you can see the message: Terracotta Server instance has started up as ACTIVE node.

7. On the ICR Core system, which you want to make the passive Terracotta server, go to the `$AVAYA_ICRCORE_HOME/bin` directory:
 - a. Open the startup configuration script file `startICRCore.sh` to edit.
 - b. In the file, change the `TC_CONFIG_PATH` variable value to the IP address and port number of the first instance of the Terracotta server.
For example, `export TC_CONFIG_PATH=192.168.0.1:9510`
The value given to the variable is the IP address and port number of the system running the first instance of the Terracotta server.
 - c. Save the changes and close the file.
 - d. Go to the `$AVAYA_ICRCORE_HOME` directory.
 - e. Back up the `icr-tc-config.xml` configuration file.
Enter the following command:

```
cp icr-tc-config.xml icr-tc-config.xml.old
```
 - f. Copy the `icr-tc-config.xml` file available in the `$AVAYA_ICRCORE_HOME` directory on the ICR Core system named *Server1* to the ICR Core system named *Server2*.
 - g. After copying the file to *Server2*, ensure that the file ownership and group ownership for the `icr-tc-config.xml` file on *Server2* are `avayavp:avayavpgroup`.



Note:

If the file ownership and group ownership are not `avayavp:avayavpgroup`, run the **`chown avayavp:avayavpgroup icr-tc-config.xml`** command on *Server2* to change the file and group ownerships.

- h. Go to the `$AVAYA_ICRCORE_HOME/bin` directory.
- i. Open the startup configuration script file `start-tc-server.sh`.
- j. Change the string *Server1* to *Server2* in the following code line.
For example:

```
$icrhome/terracotta-server/bin/start-tc-server.sh -n Server2 -f $icrhome/icr-tc-config.xml > $TEMP_FILE 2>&1 &
```
- k. Save the changes and close the file.
- l. Start the Terracotta server that you named as *Server2*.
Enter the following command:

```
/sbin/service terracottaSrv start
```

- m. Verify whether the Terracotta server started in the passive mode.
Open the `avaya.service.terra.log` file available in the `$AVAYA_ICRCORE_HOME` directory. In the log file, you can see the message `Moved to State [PASSIVE-STANDBY]`.
8. (Optional) If required, configure more Terracotta servers in the passive mode.
 - a. Stop the all the running instances of Terracotta and ICR Core servers. In this case, Server1, Server2, and Server3.
 - b. On the Server1, open the `icr-tc-config.xml` configuration file to edit.
 - c. In the file, add a new `<server>` tag and change the *host* and *name* attributes to point to Server3.
For example:


```
=====
===
<server host="192.168.0.3" name="Server3">
  <dso>
    <persistence>
      <mode>Permanent-store</mode>
    </persistence>
  </dso>
</server>
=====
===
```
 - d. From Server1, copy the `icr-tc-config.xml` file available in the `$AVAYA_ICRCORE_HOME` directory to all the systems that hosts Terracotta server.
In this case, Server2 and Server3.
 - e. On the Server3 system, perform the sub-steps mentioned in the step 7.
9. Start each Terracotta server and ICR Core system in order.
Enter the following commands:


```
/sbin/service terracottaSrv start
/sbin/service icrcore start
```

Installing ICR using silent installer

Before you begin

If you are installing Avaya Aura® Experience Portal for the first time, see the *Avaya Aura® Experience Portal* documentation on the Avaya support site at <http://support.avaya.com>.

**Note:**

Install ICR Admin only on a system running Experience Portal Manager.

Procedure

1. Mount the ICR installation media.
For information about mounting the installation media, see [Mounting the ICR media](#) on page 95
2. Copy `icr_silent_install.properties` file from the mount point directory to a temporary directory on the system.
3. Edit the `icr_silent_install.properties` file.

The content of the file are:

```
# Replay feature output
# -----
# This file was built by the Replay feature of InstallAnywhere.
# It contains variables that were set by Panels, Consoles or Custom Code.

#Choose Install Folder
#-----
USER_INSTALL_DIR=/opt/Avaya/ICR

#All selected ICR components will be installed under this directory
#Choose Product Features
#-----
CHOSEN_INSTALL_FEATURE_LIST=ICRAAdmin, ICRCCA, ICRCore
CHOSEN_INSTALL_SET=Typical

#Install
#-----
-fileOverwrite_/opt/Avaya/ICR/ICR_Uninstaller/Uninstall_ICR.lax=Yes

#Avaya Aura Experience Portal Product ID
#-----
AVAYA_AURA_EXPERIENCE_PORTAL_PRODUCT_ID_1=1234567890

#Inputs to install ICR Core and ICR CCA.
#EPM IP Address
#-----
EPM_IP_ADDRESS_1=127.0.0.1
```

The details of the fields present in the `icr_silent_install.properties` file are:

USER_INSTALL_DIR	The default location is <code>/opt/Avaya/ICR</code> . You can provide a custom install path. Ensure that the path is not <code>/root/</code> .
CHOSEN_INSTALL_FEATURE_LIST	The default selection for installation is <code>ICRAAdmin, ICRCCA, ICRCore</code> . You can set the component to install

	based on the requirement. To change the components remove the components that you do not want to install.
CHOSEN_INSTALL_SET	The default value is Typical. Do not change the default value.
AVAYA_AURA_EXPERIENCE_PORTAL_PRODUCT_ID_1	This is the Product ID of the Avaya Aura® Experience Portal system
EPM_IP_ADDRESS_1	Provide the IP address of the primary Experience Portal Manager system.

 Note:

The installer installs ICR using the values from the `icr_silent_install.properties` file.

4. Type `./install_icr.bin -i silent -f <Location_of_the_icr_silent_install.properties_file>/icr_silent_install.properties` and press Enter.

Where,

i Mode of install

f File location of the `icr_silent_install.properties` file.

 Note:

If you install ICR using the silent installer, uninstalling ICR components uninstalls all the components installed using silent installer.

Chapter 4: Configuring Avaya Aura® Communication Manager

Log in to the CM server

Log in to the CM server and select the SAT terminal type as **SUNT**.

For details on connecting to CM server using Putty, refer to *Administering Avaya Aura® Communication Manager* document from the Support site at <http://support.avaya.com>.

Adding Session Manager IP Address

Configure Communication Manager to communicate with Session Manager. Add the Session Manager IP address to Communication Manager node-names list.

Procedure

1. Log in to the Communication Manager system and select the SAT terminal type as **SUNT**.
2. On the SAT session, in the Command : prompt, type `change node-names ip` and press Enter.
The system displays the IP NODE Names screen.
3. Use the **up** or **down** arrow key and scroll to a blank line.
4. In the **Name** column, type the name of the Session Manager server.
5. In the **IP address** field, type the IP address of the Session Manager Security Module.



Note:

Do not use the management IP address in the **IP address** field.

The IP NODE Names screen displays the information as provided below:

change node-names ip		IP NODE NAMES	Page 1 of 2
Name	IP Address		
ASM_Server_Name	192.168.1.11		
default	0.0.0.0		

```

procr          192.168.1.12
procr6         ::

( 5 of 5   administered node-names were displayed )
Use 'list node-names' command to see all the administered node-names
Use 'change node-names ip xxx' to change a node-name 'xxx' or add a node-
name

```

6. Press F3 key to save the changes.

Creating a signaling-group

Configure signaling-group on Communication Manager.

Procedure

1. On the SAT session, in the Command: terminal, type `add signaling-group n` and press Enter.

The system displays the **SIGNALING GROUP** screen.

The *n* is the signaling-group number.

2. Use the **up** or **down** arrow key and scroll to the **Group Type** option.
3. In the **Group Type** option, type SIP and press tab key.

The **SIGNALING GROUP** screen displays the information as provided below:

```

add signaling-group n                                     Page 1 of 1

                                SIGNALING GROUP

Group Number: 2                      Group Type: sip
IMS Enabled? n                      Transport Method: tcp
Q-SIP? n                               SIP Enabled LSP? n
                                      Enforce SIPS URI for SRTP? y
Peer Detection Enabled? y  Peer Server: Others

Near-end Node Name: procr              Far-end Node Name: ASM_SERVER_NAME
Near-end Listen Port: 5060             Far-end Listen Port: 5060
                                      Far-end Network Region:

Far-end Domain:

Incoming Dialog Loopbacks: eliminate  Bypass If IP Threshold Exceeded? n
DTMF over IP: rtp-payload              RFC 3389 Comfort Noise? n
Session Establishment Timer(min): 3    Direct IP-IP Audio Connections? y
Enable Layer 3 Test? n                 IP Audio Hairpinning? n
H.323 Station Outgoing Direct Media? n Initial IP-IP Direct Media? n
                                      Alternate Route Timer(sec): 6

F1=Cancel F2=Refresh F3=Submit F4=Clr Fld F5=Help F6=Update F7=Nxt Pg
F8=Prv Pg

```


4. Update the following values:

Group Type	SIP
Transport Method	TLS or TCP.  Note: Ensure that you set the same value for transport method while configuring Entity link on Session Manager
Near-end Node Name	procr  Tip: This is the Communication Manager node name.
Near-end Listen Port	An unused port number for the near-end listen port.
Far-end Node Name	 Tip: This is the node name configured for Session Manager.
Far-end Listen Port	An unused port number for the far-end listen port.
Far-end Network Region	The number of the network region that is assigned to the far-end of the signaling group. The region is used to obtain the codec set used for negotiation of trunk bearer capability.
Far-end Domain	The name of the IP domain that is assigned to the far-end of the signaling group.

5. Press F3 key to save the changes.

Creating a Trunk group

Procedure

1. On the SAT session, in the Command : terminal, type `add trunk-group n` and press Enter. The *n* is the trunk group number. The **TRUNK GROUP** screen appears.
2. Use the **up** or **down** arrow key and scroll to Group Type option. In the *Group Type* option, type SIP. Press **TAB** key.
3. The **TRUNK GROUP** screen displays the information similar to the one provided below.

```
add trunk-group n                                     Page 1 of 22
                                     TRUNK GROUP
Group Number: 2          Group Type: sip          CDR Reports: y
Group Name: trunk to ASM  COR: 1          TN: 1          TAC: #2
Direction: two-way      Outgoing Display? n
Dial Access? n          Night Service:
Queue Length: 0
Service Type: tie          Auth Code? n
                               Signaling Group: 2
                               Number of Members: 255
```

4. Update the following values:

Group Type	sip
Signaling Group	Signaling Group  Note: This value must be configured with the Signaling Group value created previously.
Number of Members	This value will be the number of ports for this SIP connection
Service Type	Tie
TAC	Enter the Trunk Access Code as per dial plan

5. Press F7 key to go to the next page. There are no changes required on screen 2.
6. Press F7 key to go to the next page. In Page 3 of 22, the following information is displayed:

```
TRUNK FEATURES                                     Page 3 of 22
ACA Assignment? n          Measured: none
                               Maintenance Tests? y
```

```

Numbering Format: public
                        UUI Treatment: shared
                        Maximum Size of UUI Contents: 128
                        Replace Restricted Numbers? n
                        Replace Unavailable Numbers? n

                        Modify Tandem Calling Number: no
Send UCID? y

Show ANSWERED BY on Display? y

```

7. Update the following values:

UUI Treatment	This value must be set to <i>shared</i> .
Send UCID	Set to Yes

8. Press F3 key to save the changes.

Creating Hunt group

Procedure

- On the SAT session, in the Command : terminal, type `add hunt-group n` and press Enter. The *n* is the hunt group number. The HUNT GROUP screen appears.
Use the **up** or **down** arrow key to scroll.
- Update the following values:

Group Number	Numeric value
Group Extension	Extension of the group
ACD?	Y
Vector?	Y
Queue?	Y

The HUNT GROUP screen displays the information similar to the one provided below.

```

add hunt-group n
                                HUNT GROUP
                                Page 1 of 4

Group Number: 1
Group Name: english
                                ACD? y
                                Queue? y

```

```

Group Extension: 2000                      Vector? y
Group Type: ucd-mia
      TN: 1
      COR: 1                      MM Early Answer? n
Security Code:                      Local Agent Preference? n
ISDN/SIP Caller Display:

      Queue Limit: unlimited
Calls Warning Threshold:      Port:
Time Warning Threshold:      Port:

```

3. Press F7 to go to the next page.
4. Use the **up** or **down** arrow key to scroll. Type the value of the parameter skill? as Y.
The HUNT GROUP screen displays the information similar to the one provided below.

```

add hunt-group n                      Page 2 of 4
                                     HUNT GROUP
                                     Skill? y      Expected Call Handling Time (sec): 180
                                     AAS? n      Service Level Target (% in sec): 80 in 20
                                     Measured: internal
Supervisor Extension:

Controlling Adjunct: none

VuStats Objective:
Timed ACW Interval (sec):
Multiple Call Handling: none

```

5. Press F3 to save the changes.

Creating a Vector for polling VDN

ICR uses this vector for the Best Service Routing (BSR) polling.

Procedure

1. On the SAT session, in the Command: terminal, type `change vector n` and press Enter.
The system displays the CALL VECTOR screen.
The *n* is the number of the vector being created.
2. Use the **up** or **down** arrow key and scroll to *01* option.
3. Type *Consider* and press the TAB key.
This value is added to consider the hunt-group for agents already configured in Communication Manager.

4. Type the required value in the *skill* option and press the **TAB** key.
5. Type the required value in the *pri m adjust-by* option and press the **TAB** key.
6. Use the **up** or **down** arrow key and scroll to *02* option.
7. Type *reply-best* and press Enter.
8. Use the **up** or **down** arrow key and scroll to *03* option.
9. Type *stop* and press Enter.

The system displays the following information:

```
change vector n                                Page 1 of 6
                                           CALL VECTOR
Number: 1                                Name: polling vector
                                           Lock? n
Basic? y EAS? y G3V4 Enhanced? y ANI/II-Digits? y ASAI Routing? y
Prompting? y LAI? y G3V4 Adv Route? y CINFO? y BSR? y Holidays? y
Variables? y 3.0 Enhanced? y
01 consider skill 1 pri m adjust-by 0
02 reply-best
03 stop
04
05
06
07
08
09
10
11
12
                                           Press 'Esc f 6' for Vector Editing
```

10. Press F3 key to save the changes.

Creating a Vector for Queuing VDN

This vector is used to queue the call.

Procedure

1. On the SAT session, in the Command : terminal, type `change vector n` and press Enter. The *n* is the number of the vector being created for Queuing. The **CALL VECTOR** screen appears.

**Note:**

You must provide a Name for the vector.

2. Use the **up** or **down** arrow key and scroll to *01* option. Type *queue-to* and press the TAB key. This value is added to queue the hunt-group for agents already configured in CM.
3. Type the required value in the *skill* option and press the **TAB** key.
4. Type the required value in the *prim adjust-by* option and press the **TAB** key.
5. Use the **up** or **down** arrow key and scroll to *02* option. Type *stop* and press Enter.
6. A screen similar to the one provided below is displayed:

```

change vector n                                     Page 1 of 6
                                CALL VECTOR
Number: 2                                Name: Queue Vector
                                Lock? n
Basic? y  EAS? y  G3V4 Enhanced? y  ANI/II-Digits? y  ASAI Routing? y
Prompting? y  LAI? y  G3V4 Adv Route? y  CINFO? y  BSR? y  Holidays? y
Variables? y  3.0 Enhanced? y
01 queue-to      skill 1      pri m
02 stop
03
04
05
06
07
08
09
10
11
12

                                Press 'Esc f 6' for Vector Editing
  
```

7. Press F3 key to save the changes.

**Note:**

The queuing vector must not have any music or ring-back treatments setup, or the EPM will prematurely REFER the call media path down to the Communication Manager before an agent is ready to answer.

Creating a Polling VDN

About this task

This VDN is used as a polling VDN while configuring skill on the ICR configuration page.

Procedure

1. On the SAT session, in the Command : terminal, type `add vdn n` and press Enter. The *n* is the number of the VDN created. The VECTOR DIRECTORY NUMBER screen appears.
2. Use the **up** or **down** arrow key to scroll. In the first page, provide the following information:
 - VDN name
 - Vector number that this VDN will use. Set the value of this field to the value of the Vector that was created in [Creating a Vector for polling VDN](#) on page 44.
3. The first screen of VECTOR DIRECTORY NUMBER displays the information similar to the one provided below.

```

add vdn n                                     Page 1 of 3
                                VECTOR DIRECTORY NUMBER

                                Extension: n
                                Name*: polling vdn
                                Destination: Vector Number      1

                                Allow VDN Override? n
                                    COR: 1
                                    TN*: 1
                                    Measured: none

                                VDN of Origin Annc. Extension*:
                                    1st Skill*:
                                    2nd Skill*:
                                    3rd Skill*:

* Follows VDN Override Rules

```

4. Press F7 to go to the next page.
5. Use the **up** or **down** arrow key to scroll. In the second page, provide the following information:
 - BSR Available Agent Strategy. This is used for multiple skills configured in the VDN.
 - BSR Tie Strategy. This is used in case a tie happens.
6. Set all the other options to *N*.
7. The second screen of VECTOR DIRECTORY NUMBER displays the information similar to the one provided below.

```

add vdn n                                     Page 2 of 3
                                VECTOR DIRECTORY NUMBER

                                AUDIX Name:
                                Return Destination*:
                                VDN Timed ACW Interval*:
                                BSR Application*:

```

```

BSR Available Agent Strategy*: 1st-found
BSR Tie Strategy*: system

Observe on Agent Answer? n

Send VDN as Called Ringing Name Over QSIG? n

Display VDN for Route-To DAC*? n
VDN Override for ASAI Messages*: no

BSR Local Treatment*? n

Reporting for PC Predictive Calls? n
Pass Prefixed CPN to VDN/Vector*? system
* Follows VDN Override Rules

```

8. Press F3 to save the changes.

Creating a Queue VDN

About this task

This VDN is used as a Queue VDN while configuring skill on ICR configuration page.

Procedure

1. On the SAT session, in the Command: terminal, type `add vdn n` and press Enter. The `n` is the number of the VDN created. The VECTOR DIRECTORY NUMBER screen appears.
2. Use the **up** or **down** arrow key to scroll. In the first page, provide the following information:
 - Queue VDN name
 - Vector number that this VDN will use. Set the value of this field to the value of the Vector that was created in [Creating a Vector for Queuing VDN](#) on page 45.
3. The first screen of VECTOR DIRECTORY NUMBER displays the information similar to the one provided below.

```

add vdn n
                                     Page 1 of 3
                                VECTOR DIRECTORY NUMBER

                                Extension: n
                                Name*: queuing vdn
                                Destination: Vector Number      1

                                Allow VDN Override? n
                                COR: 1
                                TN*: 1
                                Measured: none

```



```

VDN of Origin Annc. Extension*:
                        1st Skill*:
                        2nd Skill*:
                        3rd Skill*:

```

* Follows VDN Override Rules

4. Press F7 to goto the next page.
5. Use the **up** or **down** arrow key to scroll. In the second page, provide the following information:
 - BSR Available Agent Strategy. This is used for multiple skills configured in the VDN.
 - BSR Tie Strategy. This is used in case a tie happens.
6. Set all the other options to *N*.
7. The second screen of VECTOR DIRECTORY NUMBER displays the information similar to the one provided below.

```

add vdn n
                                Page 2 of 3
                                VECTOR DIRECTORY NUMBER
                                AUDIX Name:
                                Return Destination*:
                                VDN Timed ACW Interval*:
                                BSR Application*:
                                BSR Available Agent Strategy*: 1st-found
                                BSR Tie Strategy*: system
                                Observe on Agent Answer? n
                                Send VDN as Called Ringing Name Over QSIG? n
                                Display VDN for Route-To DAC*? n
                                VDN Override for ASAI Messages*: no
                                BSR Local Treatment*? n
                                Reporting for PC Predictive Calls? n
                                Pass Prefixed CPN to VDN/Vector*? system
                                * Follows VDN Override Rules

```

8. Press F3 to save the changes.

Adding the Queuing VDN to public unknown numbering plan

You must add the Queuing VDN to the Public Unknown numbering plan of Communication Manager so that, when responding to SIP commands associated to this VDN, Communication Manager can send the number in the messages.

Procedure

1. On the SAT session, in the Command : terminal, type `change public-unknown-numbering 0` and press Enter.
The system displays the NUMBERING - PUBLIC/UNKNOWN FORMAT screen.

2. Use the **up** or **down** arrow key to scroll.

On the first page, provide the following information:

- Ext Len
- Ext Code
- Trk Grp(s)
- Total CPN Len

The first screen of NUMBERING - PUBLIC/UNKNOWN FORMAT displays the information similar to what is provided below.

```
change public-unknown-numbering 0                                     Page 1 of 2
                                NUMBERING - PUBLIC/UNKNOWN FORMAT
                                Total
Ext Len  Ext Code  Trk Grp(s)  CPN Prefix  CPN Len
5      8
Total Administered: 1
Maximum Entries: 240

Note: If an entry applies to
a SIP connection to Avaya
Aura(tm) Session Manager,
the resulting number must
be a complete E.164 number.
```

3. Press F3 key to save the changes.

Adding the IP Network Region

You must define the Authoritative Domain name on the IP-network-region form.

Procedure

1. On the SAT session, in the Command : prompt, type `change ip-network-region 1` and press Enter. The IP NETWORK REGION screen appears.
2. Use the **up** or **down** arrow key to scroll. In the first page, provide the following information:

Define the Authoritative Domain name.

3. The first screen of IP NETWORK REGION displays the information similar to the one provided below.

```
change ip-network-region 1                                     Page 1 of 20
                                IP NETWORK REGION
```

```

Region: 1
Location:          Authoritative Domain: avaya.com
Name:
MEDIA PARAMETERS      Intra-region IP-IP Direct Audio: yes
                      Codec Set: 1          Inter-region IP-IP Direct Audio: yes
                      UDP Port Min: 2048      IP Audio Hairpinning? n
                      UDP Port Max: 3329
DIFFSERV/TOS PARAMETERS
  Call Control PHB Value: 46
  Audio PHB Value: 46
  Video PHB Value: 26
802.1P/Q PARAMETERS
  Call Control 802.1p Priority: 6
  Audio 802.1p Priority: 6
  Video 802.1p Priority: 5
H.323 IP ENDPOINTS    AUDIO RESOURCE RESERVATION PARAMETERS
H.323 Link Bounce Recovery? y      RSVP Enabled? n
Idle Traffic Interval (sec): 20
Keep-Alive Interval (sec): 5
Keep-Alive Count: 5

```

4. Press F3 key to save the changes.

Adding the IP codec set

You must add the IP codec set in Communication Manager to establish successful RTP path with the customer.

Procedure

1. On the SAT session, in the Command : prompt, type `change ip-codec-set n` and press Enter. The *n* is the ip codec set number. The IP Codec Set screen appears.
2. Use the **up** or **down** arrow key to scroll. In the first page, provide the following information:
 - Audio Codec
 - Silence Suppression
 - Frames Per Packet
 - Packet Size in milliseconds
3. The first screen of IP Codec Set displays the information similar to the one provided below.

```

change ip-codec-set 1                                     Page 1 of 2

                                IP Codec Set

  Codec Set: 1

  Audio      Silence      Frames      Packet
  Codec      Suppression   Per Pkt     Size(ms)

```

1:	G.729	n	2	20
2:	G.711A	n	2	20
3:	G.729A	n	2	20
4:	G.711MU	n	2	20
5:				
6:				
7:				

4. Press the F3 key to save the changes.

Chapter 5: Configuring Avaya Aura® Session Manager

Logging on to System Manager Web interface

The System Manager Web interface is the main interface of Avaya Aura System Manager. You must log on to the System Manager Web console before you can perform any tasks.

Before you begin

A user account to log on to the System Manager Web interface. If you do not have a user account, contact your system administrator to create your account.

Procedure

1. On the browser, open the System Manager URL (<https://<Fully Qualified Domain Name>/SMGR>).
2. In the **User ID** field, enter the user name.
3. In the **Password** field, enter the password.
4. Click **Log On**.

If your user name and password:

- Match an authorized System Manager user account, the System Manager home page appears with the System Manager *version_number*. The System Manager home page displays a navigation menu. This menu provides access to shared services with which you can perform various operations supported by System Manager. The tasks you can perform depends on your user role.
- If you enter incorrect login credentials on the System Manager login page, System Manager displays an error message and prompts you to re-enter the user name and password so that you can log in again.

Adding a SIP domain

Procedure

1. Log in to the System Manager Web interface with the Administration user role.
 2. From the System Manager main menu:
 - For System Manager 5.2, select **Network Routing Policy > SIP Domains**
 - For System Manager 6.x, select **Routing > Domains**
 3. On the Domain Management page, click **New**.
 4. Enter the domain name and notes for the new domain or sub-domain.
 5. Select “sip” as the domain type from the drop-down list.
 6. Click **Commit**.
-

Adding SIP Entities/Elements

Adding SIP Entity for SIP Gateway or Session Border Controller (SBC)

Procedure

1. Log in to the System Manager Web interface with the Administration user role.
2. From the System Manager main menu:
 - For System Manager 5.2, select **Network Routing Policy > SIP Entities**
On the SIP Entities Details page, click **New** to add the SIP Entity details.
 - For System Manager 6.x, select **Routing > SIP Elements**
On the SIP Elements Details page, click **New** to add the SIP Element details.
3. On the Details page, add the SIP Entities/ SIP Elements information.

Parameter	Value
Name	Name of the SIP Gateway or Session Border Controller. This name must be unique and can have between 3 and 64 characters.
FQDN or IP Address	IP address of the SIP Gateway or Session Border Controller configured in the signaling-group on CM.
TYPE	Gateway
Notes	Additional notes about the SIP entity.
Location	SIP entity location. Select from previously defined locations.
Time Zone	Default time zone to be used for the entity.
SIP Link Monitoring	Select the process for SIP Link monitoring.

4. Click **Commit** to save the configurations.

Adding SIP Entities for Communication Manager

Procedure

1. Log in to the System Manager Web interface with the Administration user role.
2. From the System Manager main menu:
 - For System Manager 5.2, select **Network Routing Policy > SIP Entities**
On the SIP Entities Details page, click **New** to add the SIP Entities information for Communication Manager.
 - For System Manager 6.x, select **Routing > SIP Elements**
On the SIP Elements Details page, click **New** to add the SIP Elements information for Communication Manager.
3. On the Details page, add the SIP Entities or SIP Elements information.

Parameter	Value
Name	Name of the CM server. This name must be unique and can have between 3 and 64 characters.

Parameter	Value
FQDN or IP Address	IP address of the CLAN/Procr configured in the signaling-group on CM
TYPE	CM
Notes	Additional notes about the SIP entity.
Location	SIP entity location. Select from previously defined locations.
Time Zone	Default time zone to be used for the entity.
SIP Link Monitoring	Select the process for SIP Link monitoring.

- Click **Commit** to save the configurations.
Perform these steps to create SIP Entities for all the required CM servers.

Adding SIP Entity for Avaya Aura® Experience Portal

Procedure

- Log in to the System Manager Web interface with the Administration user role.
- From the System Manager main menu:
 - For System Manager 5.2, select **Network Routing Policy > SIP Entities**
On the SIP Entities Details page, click **New** to add the SIP Entities information for Avaya Aura® Experience Portal.
 - For System Manager 6.x, select **Routing > SIP Elements**
On the SIP Elements Details page, click **New** to add the SIP Elements information for Avaya Aura® Experience Portal.
- On the Details page, add the SIP Entities or SIP Elements information.

Parameter	Value
Name	Name of the Avaya Aura® Experience Portal server. This name must be unique and can have between 3 and 64 characters.
FQDN or IP Address	IP address of Media Processing Platform. If you have multiple Media Processing Platform then add all Media

Parameter	Value
	Processing Platform with a single FQDN under Local Host Name configured.
TYPE	Avaya Aura® Experience Portal
Notes	Additional notes about the SIP entity.
Location	SIP entity location. Select from previously defined locations.
Time Zone	Default time zone to be used for the entity.
SIP Link Monitoring	Select the process for SIP Link monitoring.

- Click **Commit** to save the configurations.

Adding SIP Entities for ICR Core

Procedure

- Log in to the System Manager Web interface with the Administration user role.
- From the System Manager main menu:
 - For System Manager 5.2, click **Network Routing Policy > SIP Entities**
On the SIP Entities Details page, click **New** to add the SIP Entities information for ICR Core.
 - For System Manager 6.x, click **Routing > SIP Elements**
On the SIP Elements Details page, click **New** to add the SIP Elements information for ICR Core.
- On the Details page, add the SIP Entities or SIP Elements information.

Parameter	Value
Name	Name of the ICR Core Server. This name must be unique and can have between 3 and 64 characters.
FQDN or IP Address	IP address of ICR system. If you have multiple ICR then add all the ICR systems with a single FQDN under the configured Local Host Name.
TYPE	The SIP entity type.

Parameter	Value
	Click Other .
Notes	Additional notes about the SIP entity.
Location	SIP entity location. Select from the previously defined locations.
Time Zone	Default time zone to be used for the entity.
Credential name	Enter a regular expression string in the Credential name. The Credential name is used for TLS connection validation. You can validate the TLS connection by searching Credential name in the SIP entity identity certificate.
SIP Link Monitoring	Select the process for SIP Link monitoring.

4. Click **Commit** to save the configurations.

Adding SIP Entity links

Adding SIP Entity Link for SIP Gateway or SBC

Procedure

1. Log in to the System Manager Web interface with the Administration user role.
2. From the System Manager main menu:
 - For System Manager 5.2, select **Network Routing Policy > Entity Links**
On the Entity Links page, click **New** to add the Entity Links information.
 - For System Manager 6.x, select **Routing > Element Links**
On the Element Links page, click **New** to add the Entity Links information.
3. On the Links page, add the SIP Entity Links or SIP Element Links information.

Name	Description
Name	Name of the SIP Entity Link for SIP gateway or SBC. This name must be unique and can have between 3 and 64 characters.
SIP Entity 1	Select a SIP entity from the drop-down list. This entity must always be a Session Manager instance.
Protocol	Protocol to be used for the entity link.
Port	Port to be used for SIP entity 1.
SIP Entity 2	This entity is created for SIP gateway or SBC
Port	Port to be used for SIP gateway or SBC.
Trusted	Specifies that the link between the two SIP entities is trusted. Select the Check box
Notes	Any details or notes that you wish to add.

4. Click **Commit** to save the configurations.

Adding SIP Entity Link for Communication Manager

Procedure

1. Log in to the System Manager Web interface with the Administration user role.
2. From the System Manager main menu:
 - For System Manager 5.2, select **Network Routing Policy > Entity Links**
On the Entity Links page, click **New** to add the Entity Links information for Communication Manager.
 - For System Manager 6.x, select **Routing > Element Links**
On the Element Links page, click **New** to add the Element Links information for Communication Manager.
3. On the Links page, add the SIP Entity Links or SIP Element Links information.

Name	Description
Name	Name of the SIP Entity Link for Communication Manager server. This name must be unique and can have between 3 and 64 characters.
SIP Entity 1	Select a SIP entity from the drop-down list. This entity must always be a Session Manager instance.
Protocol	Protocol to be used for the entity link.
Port	Port to be used for SIP entity 1.
SIP Entity 2	Select a SIP entity from the field. This is the entity created for CM.
Port	Enter the port for Communication Manager.
Trusted	Specifies that the link between the two SIP entities is trusted. Select this option.
Notes	Any details or notes that you wish to add.

4. Click **Commit** to save the configurations.

Adding SIP Entity Link for Avaya Aura® Experience Portal

Procedure

1. Log in to the System Manager Web interface with the Administration user role.
2. From the System Manager main menu:
 - For System Manager 5.2, select **Network Routing Policy > Entity Links**.
On the Entity Links page, click **New** to add the Entity Links information for Avaya Aura® Experience Portal.
 - For System Manager 6.x, select **Routing > Element Links**.
On the Element Links page, click **New** to add the Element Links information for Avaya Aura® Experience Portal.
3. On the Links page, add the SIP Entity Links or SIP Element Links information.

Name	Description
Name	Name of the SIP Entity Link for Avaya Aura® Experience Portal server. This name must be unique and can have between 3 and 64 characters.
SIP Entity 1	Select a SIP entity from the drop-down list. This entity must always be a Session Manager instance.
Protocol	Protocol to be used for the entity link.
Port	Port to be used for SIP entity 1.
SIP Entity 2	Select a SIP entity from the field. This is the entity created for MPP.
Port	Port to be used for SIP entity 2.
Trusted	Specifies that the link between the two SIP entities is trusted. Select this option.
Notes	Any details or notes that you wish to add.

4. Click **Commit** to save the configurations.

Adding SIP Entity Link for ICR Core Server

Procedure

- Log in to the System Manager Web interface with the Administration user role.
- From the System Manager main menu:
 - For System Manager 5.2, select **Network Routing Policy > Entity Links**.
On the Entity Links page, click **New** to add the Entity Links information for ICR server node.
 - For System Manager 6.x, select **Routing > Element Links**.
On the Element Links page, click **New** to add the Element Links information for ICR server node.
- On the Links page, add the SIP Entity Links or SIP Element Links information.

Name	Description
Name	Name of the SIP Entity Link for ICR Core server.

Name	Description
	This name must be unique and can have between 3 and 64 characters.
SIP Entity 1	Select a SIP entity from the drop-down list. This entity must always be a Session Manager instance.
Protocol	Protocol to be used for the entity link.
Port	Port to be used for SIP entity 1.
SIP Entity 2	Select a SIP entity from the field. This is the entity created for ICR Core server
Port	Port to be used for SIP entity 2.
Trusted	Specifies that the link between the two SIP entities is trusted. Select this option.
Notes	Any details or notes that you wish to add.

4. Click **Commit** to save the configurations.

Defining Policies and Time of Day

Adding Routing Policy for Communication Manager

Procedure

1. Log in to the System Manager Web interface with the Administration user role.
2. From the System Manager main menu:
 - For System Manager 5.2, select **Network Routing Policy > Routing Policies**
 - For System Manager 6.x, select **Routing > Policies**
3. On the Routing Policies page, click **New** to add the Routing Policy information for Communication Manager.
4. On the Routing Policy Details page, under General, provide the value for *Name* field. You can also provide generic information for reference in the *Notes* field.
5. Under SIP Entity as Destination, click **Select**.

6. From the list of SIP Entities, select the Communication Manager SIP Entity.
 7. Under Time of Day, click **Add**.
 8. From the Time Ranges List page, select the required Time Range.
 9. Click **Select**.
The selected Time Range displays on the Routing Policy Details page.
 10. Click **Commit** to save the configuration.
-

Adding Routing Policy for Avaya Aura® Experience Portal

Procedure

1. Log in to the System Manager Web interface with the Administration user role.
 2. From the System Manager main menu:
 - For System Manager 5.2, select **Network Routing Policy > Routing Policies**
 - For System Manager 6.x, select **Routing > Policies**
 3. On the Routing Policies page, click **New** to add the Routing Policy information for Avaya Aura® Experience Portal.
 4. On the Routing Policy Details page, under General, provide the value for *Name* field. You can also provide generic information for reference in the *Notes* field.
 5. Under SIP Entity as Destination, click **Select**.
 6. From the list of SIP Entities, select the Avaya Aura® Experience Portal SIP Entity.
 7. Under Time of Day, click **Add**.
 8. From the Time Ranges List page, select the required Time Range.
 9. Click **Select**.
The selected Time Range displays on the Routing Policy Details page.
 10. Click **Commit** to save the configuration.
-

Dial Patterns

Adding dial plan for Avaya Aura® Experience Portal and Communication Manager

About this task

**Note:**

You must configure a minimum of two dial patterns.

- Pattern to route calls to Experience Portal Manager for incoming calls to Avaya Aura® Experience Portal.
- Pattern to route calls to agents and for polling/queuing VDN's to Communication Manager.

Procedure

1. Log in to the System Manager Web interface with the Administration user role.
2. From the System Manager main menu:
 - For System Manager 5.2, select **Network Routing Policy > Dial Patterns**
 - For System Manager 6.x, select **Routing > Dial Patterns**
3. On the Dial Patterns page, click **New** to add a new Dial Pattern for Avaya Aura® Experience Portal.

Under General, provide the value for the fields provided in the table.

Name	Description
Pattern	Dial pattern to match. The pattern can have between 1 and 36 characters. Roll over the field for the valid pattern.
Min	Minimum number of digits to be matched.
Max	Maximum number of digits to be matched.
SIP Domain	Domain for which you want to restrict the dial pattern.
Notes	Other details that you wish to add.

4. Under Originating Locations and Routing Policies, click **Add**.

5. Under Originating Location, select the originating location.
6. Under Routing Policies, select the routing policy.
7. Click **Select**.
8. Click **Commit** to save the configuration.

Adding ICR user on System Manager

About this task

Configure the User Name and Password for the ICR Core Server. If ICR Core server is not marked as trusted while configuring Entity Link between ICR Core server and SM then the created SIP user is used during BSR polling. By default, the SIP user name is avaya and password avaya123. This information is stored in `../ICR/ICRCore/tomcat/conf/icrcore.properties` file. Administrator can configure another SIP user and edit the property file.

Procedure

1. Log in to the System Manager Web interface with the Administration user role.
2. From the System Manager main menu:
 - For System Manager 5.2, select **User Management > User Management**.
 - For System Manager 6.x, select **Users > Manage Users**.
3. On the User Management page, under Users, click **New**.
4. Under General, provide the following information.

Name	Description
Last Name	avaya
First Name	avaya
Description	
User Type	Select as Communication User

5. Under Identity, provide the following information.

Name	Description
Login Name	Enter login name as avaya
Authentication Type	Select as Basic
SMGR Login Password	Enter the password as avaya123

Name	Description
Password	avaya123
Confirm Password	avaya123
Shared Communication Profile Password	avaya123
Confirm Password	avaya123

6. Under Communication Profiles section, under Communication Address, click **New**. Add the user name as avaya.
 7. In the **Type** field, select **Avaya SIP**.
 8. Add appropriate values to set **Fully Qualified Address**.
 9. Click **Add**.
 10. In the Communication Profile section, select **Session Manager Profile**.
 11. From the field, select the **Primary Session Manager** and **Secondary Session Manager** (if required).
 12. Click **Commit** to save the user's information.
-

Chapter 6: Configuring Avaya Aura® Experience Portal

About configuring Avaya Aura® Experience Portal

ICR Core reads the SIP proxy server configuration from the VoIP Connections Web page of Avaya Aura® Experience Portal. ICR is a managed application of Avaya Aura® Experience Portal. Therefore, Media Processing Platform (MPP) and Speech servers are already configured on Avaya Aura® Experience Portal.

Related topics:

[Adding a SIP connection for Session Manager](#) on page 67

Adding a SIP connection for Session Manager

Procedure

1. Log on to an Experience Portal Manager Web page using an account with the Administration or ICR Administration role.
2. From the Experience Portal Manager main menu in the left navigation pane, click **System Configuration > VoIP Connections**.
3. On the VoIP Connections page, click the **SIP** tab.
4. Click **Add**.
5. On the Add SIP Connection page, enter the values in the following fields.

Field	Description
Name	Enter appropriate name for SIP connection.
Enable	Default value is Yes.
Proxy Transport	TCP or TLS as per configuration.
Proxy Services Address	Enter the IP address of Security module of Session Manager.

Field	Description
DNS SRV Domain	Enter the domain name of the DNS server. For example, abc . com.
SIP Domain	Enter the domain of Session Manager.
Maximum Simultaneous Calls	The maximum number of calls that this trunk can handle at one time.

6. Click **Save**.

Chapter 7: Installing Pluggable Data Connector

Pluggable Data Connector (PDC)

The PDC is a connector between Self Service Application (SSA) and ICR Core. ICR PDC is built to integrate into Orchestration Designer. ICR PDC is a generic connector which an application developer can use without knowledge of call centers and ICR Core. The purpose of ICR PDC is to provide a SIP URI, which is the routing destination for a skill.

ICR PDC also does the load balancing of skill selection requests that arrives across multiple ICR Cores.

Prerequisite

Orchestration Designer to create and build applications.

If you are installing Orchestration Designer for the first time, see the *Orchestration Designer* documentation from the Avaya support site at <http://support.avaya.com>.

Copying PDC to the plugins folder in Orchestration Designer

Procedure

Copy `com.avaya.icr.PDC.ui.jar` file from ICRPDC folder on the CD to `<Eclipse_Home>/plugins` folder.



Note:

Close the Eclipse application before copying the file to the plugins folder.

Importing sample applications in Eclipse

Procedure

1. Copy the `SampleApps.zip` file from the ISO image of ICR to a temporary location.
2. Unzip the `SampleApps.zip` file in a directory to extract the sample applications.
After you unzip the `SampleApps.zip` file, the directory contains the following sample applications:

Sample Application Name	Description
SSA	This folder contains sample application for Sample Self Service Application.
WTA	This folder contains two sample Wait Treatment Applications. • WTAUpdateAAI: Demonstrates how to collect additional information from a caller and pass that information to CCA. • WTAWaitTimeAnnouncement: Demonstrates how to prompt estimated wait time and queue position.
EHA	This folder contains two sample Error Handling Applications. • EHAGeneric: Prompts generic error messages to a caller. • EHAOutOFHours: Prompts error message for calls coming in out of business hours.

3. Open the Eclipse application.
4. In the Eclipse application, click **File > Import**.
5. Select **Existing Project into WorkSpace** and click **Next**.
6. Enable the **Select root directory** option.
7. Click **Browse**.



Note:

Browse to the directory where you have extracted the sample applications.

8. Select the SSA folder.

9. Click **Finish**.
 10. On the Runtime Version Mismatch window, click **OK**.
 11. Perform the above steps to import all the sample applications that you extracted.
-

Enabling Pluggable Data Connector plug-in for the SSA application

Procedure

1. Open the Eclipse application.
2. In the Eclipse SDK application, select the Sample Self Service Application (SSA).
3. Select **Project > Properties**.
4. On the Properties for SSA window, in the right pane, under Orchestration Designer, click the **Pluggable Connectors** tab.
5. From the list of connectors, select *ICR Connector*.
6. Click **OK**.
7. Open the main flow of the SSA application.
8. Double-click **GetDestinationInformation** data node.



Note:

ICR connector appears in the Palette pane. The `Get Destination` method of ICR connector accepts the `Skill` as an input parameter.

9. Application Developer can drag and drop `Get Destination` method to any data node in the application as per the business need.
-

Chapter 8: Application Server

About application server

Deploy ICR CCA dependent applications, such as SSA, WTAs, and EHAs on an application server. For information about deploying the dependant application, see the *Application Deployment* topic in the Orchestration Designer developer guide.

After you complete deploying the application server, fetch the ICR Core certificates. For more information, see [Importing ICR Core certificate on the application server](#) on page 73.

Importing ICR Core certificate on the application server

Procedure

1. Start the application server.
2. On the application server, open the run-time config application in a browser.
For example: `http://localhost:8080/runtimeconfig`.
3. Log on to the Orchestration Designer system with administrator privileges.
4. In the left pane, click **Certificates**.
5. At the bottom of the page, click **Fetch**.
6. On the Fetch certificate page, enter the values for the following fields in the **Fetch New Certificate** area.
 - **Name**: The name of the certificate.
 - **Location**: The IP address or host name of the ICR Core system. For example, For example: `https://<IP_Address_of_the_ICR_Core_system>`.
7. Click **Continue**.
8. Click **Save**.
9. Restart the application server.
The Application server must be able to communicate with ICR Core server.



Note:

Add the IP address and the host names of the ICR Core system in the `/etc/hosts` file of the application server.

Chapter 9: Configuring ICR properties

ICR Core property file description

This table provides information about the ICR Core properties provided in the `icrcore.properties` file. The `icrcore.properties` file is present in the `$AVAYA_ICCORE_HOME/tomcat/conf` directory.

Property name	Description	Default Value	Possible Value
ICRAdminURL	The IP address of Experience Portal Manager system where the ICR Admin component is deployed. The property is used to fetch the ICR configuration.	The IP address of the primary Experience Portal Manager system that you entered when installing ICR Core.	The IP address of the primary Experience Portal Manager system.
VPRemoteLogWebService	The property for Experience Portal Manager system logging.	<code>https://%Primary_EPM_IP_ADDRESS%/axis/services/LogServer-1.0</code>	The IP address of the primary Experience Portal Manager system.
VPProductID	The Product ID of Avaya Aura® Experience Portal. This property is required for pushing log messages from ICR Core to Experience Portal Manager.	The product ID of the primary Experience Portal Manager system that you entered when installing ICR Core.	The product ID of the primary Experience Portal Manager system.
VPRetryAfter	The delay, in milliseconds, after which ICR Core retries sending logs to Experience Portal Manager, if the earlier execution is	30000	

Property name	Description	Default Value	Possible Value
	failed to send the logs.		
Optional properties			
ICRSipDebug	This property enables SIP debug message to be printed in the AvayaICRDebug . log file located in the \$AVAYA_ICRCORE_HOME/tomcat/ log directory.	OFF	DEBUG
ICRKeystore	Certificate storage location.	\$AVAYA_ICRCORE_HOME/tomcat/conf/keystore	NA
ICRKeyStorePassword	Certificate storage password.	changeit	NA
ICRTrustStore	Certificate storage location.	\$AVAYA_ICRCORE_HOME/tomcat/conf/truststore	NA
ICRTrustStorePassword	Certificate storage password.	changeit	NA
ICRSipUserName	Sip account configured on System Manager.	avaya	Enter the SIP user name configured on System Manager, if other than avaya.
ICRSipPassword	Sip account password configured on System Manager.	avaya123	Enter the password configured on System Manager for SIP user.
ICRBsrRequestTimeout	Time in milliseconds to wait for all responses of polling request that ICR Core sends.	8000	Change depending upon network delay
ICRCacheUpdateTimeout	Time in milliseconds to wait for cache update.	1000	No change required

Property name	Description	Default Value	Possible Value
ICRSchedulerDelay	Time in milliseconds to check availability of ACD/Proxy. The value specifies the delay after which BSR skill module starts the health check for Communication Manager and Avaya Aura® Session Manager, which are marked as out of service.	60000	
ICRSipTCPPort	TCP Port that ICR Core uses for SIP communication with proxy.	5060	TCP port for SIP communication with proxy server.
ICRSipTLSPort	TLS port that ICR Core uses for SIP communication with Proxy.	5061	TLS port for SIP communication with proxy server.
ICRLogThrottlingTimeout	Time in milliseconds to suppress successive logs.	60000	
ICRDNSPollingTime	The time interval in seconds after which ICR Core query the DNS server for SIP proxy servers if you have configured the SIP connection as DNS SRV domain.	3600	
ICRACDSchedulerEnabled	The value that indicates ICR Core whether to monitor ACD health or not.  Note: If you configured multiple IP addresses of ACD, for example Enterprise Survivable Server (ESS) or CLAN, on Avaya Aura®	false	true

Property name	Description	Default Value	Possible Value
	Session Manager using the Local Host Name Resolution option, you must set the <code>ICRACDScheduleEnabled</code> parameter to false.		
<code>ICRSocketConnectionTimeout</code>	The time in milliseconds that indicates how long ICR Core must wait for successfully establishing a socket connection with the proxy server. On failing to establish a socket connection, ICR Core considers next available proxy server, if configured.	5000	No change required

**Note:**

After making changes in the `icrcore.properties` file, you must restart ICR Core for the changes to take effect. Run the **service icrcore restart** command to restart the ICR Core.

ICR CCA property file description

This table provides information about the ICR CCA properties provided in the `icrcca.properties` file. The `icrcca.properties` file is present in the `$AVAYA_ICRCCA_HOME/tomcat/conf` directory.

Property name	Description	Default Value	Possible Value
<code>ICRAppConfigWSURL</code>	URL of ICR Admin		
<code>debug</code>	Enables ICR CCA to log the <code><log></code> elements in the CCXML - <code>SessionSlot-XXX.log</code> file.	false	true

Property name	Description	Default Value	Possible Value
	 Important: Setting the debug property to true enables Media Processing Platform (MPP) to create Application Detail Rrecords (ADR) on MPP. This results into increase in the disk space utilization and degrades the performance of ICR. Therefore, you must set this property to true only for the testing purpose.		
scheduleInterval	Time in seconds after which CCA checks modification of ICR CCA application configuration.	120	Enter value in seconds as per customer requirement
Prov_timeout	Time in seconds for which CCA waits for the <i>182 Queued</i> response for a no media call.	90s	 Note: Always this value must be ≥ 90 .
ewtUpdatePercent	If the percentage difference between two successive EWT values is greater than this value, ICR CCA terminates and launches the same WTA. This value is used in conjunction with ewtUpdateDiff property.	20	
ewtUpdateDiff	If the difference between two successive EWT values is greater than the configured value then, ICR CCA terminates and	30	

Property name	Description	Default Value	Possible Value
	launches the same WTA.		
ewtSpikePercent	If the Percentage difference between two successive EWT values is greater than the configured value then, ICR CCA terminates and launches a new WTA based on the EWT-WTA mapping.	60	
ewtSpikeDiff	If the difference between two successive EWT values is greater than the configured value then, ICR CCA terminates and launches a new WTA based on the EWT-WTA mapping.	180	
queuePositionUpdateDiff	If the difference between two successive QueuePosition values is greater than the configured value, ICR CCA terminates and launches the same WTA.	10	
queuePositionSpikeDiff	If the difference between two successive QueuePosition values is greater than the configured value, ICR CCA terminates and launches a new WTA based on the EWT-WTA mapping.	60	
agenttimeout	Merge time-out or Blind transfer time-out in seconds	120	

Property name	Description	Default Value	Possible Value
requeuePriority	Priority at which calls are re-queued.	1	• 4 = low • 3 = medium • 2 = high • 1 = top • 0 = redirect

**Note:**

After making changes in the `icrcca.properties` file, you must restart ICR CCA for the changes to take effect. Run the **service icrcca restart** command to restart the ICR CCA.

ICR Admin property file description

This table provides information about the ICR Admin properties available in the `VP_ICRAdmin.properties` file. The `VP_ICRAdmin.properties` file is present in the `$CATALINA_HOME/lib/extensions/ICR/config/` directory.

Property name	Description	Default Value	Possible Value
securityTrustStore	Directory path of the TrustStore file.	/opt/Tomcat/tomcat/conf/truststore	
securityTrustStorePwd		changeit	Change the password
securityKeyStore		/opt/Tomcat/tomcat/conf/keystore	
securityKeyStorePwd		changeit	Change the password
HeartbeatInterval		60	
HeartbeatRetries		3	
NodeDelimiter		#	
AttributeDelimiter		,	
QueuedCallConsolidatorSeq		sessionid,ucid,skillid,callcentername,destination,qpos,ewt,callingno,mppName	
AppCallConsolidatorSeq		sessionid,ucid,appname,apptype,ssaapp	

Property name	Description	Default Value	Possible Value
		name,wtaappname ,ehaappname,called no,callingno	
QueuedCallURLFormat		/mpp/sconfig/ fetchCallDetail.php? fetchType=queuedcall	
AppCallURLFormat		/mpp/sconfig/ fetchCallDetail.php? fetchType=appcall	
SummaryCallURLFormat		/mpp/sconfig/ fetchCallDetail.php? fetchType=summary call	
CreateDBFURLFormat		/mpp/sconfig/ createCallDetails.php	
ReportPollingInterval	Polling time in milliseconds for MPP. If any request comes before this interval, ICR displays cached data.	5000	
ReportingConnReadTimeoutInterval	Time for which ICR Admin waits for MPP to fetch call details.	150	
ReportPollingWaitTime	Time for which the UI hangs and wait for a response from ICR Report Manager to consolidate a report.	1500	
ReportCacheClearInterval	Cache clearing time in minutes.	10	
ICRContextRoot		/VP_ICRAdmin/	
RemoteVpPollingDuration		600000	
RemoteVPReportPath		report/	
ICRAdminThrottlingTimeout		10	

Property name	Description	Default Value	Possible Value
EnableRealTimeRawDataLog		false	
RemoteDBQueryTimeOut		10	
RemoteDBQueryTimeOut		10	
sipInfoSeparator	Separator used in EPMSIP table, which stores SIP connection information.		
CleanMPPURLFormat	The URL that ICR Admin use to delete the orphan records after the schedule time configured in the CleanMPPStaleDataInterval property.	/mpp/sconfig/deleteOldCallDetails.php? ssa=360&wta=15&eha=15 In the URL: • The ssa=360 parameter indicates the ICR Admin cleans the orphan records of SSA after 360 minutes. • The wta=15 parameter indicates the ICR Admin cleans the orphan records of WTA after 15 minutes. • The eha=15 parameter indicates the ICR Admin cleans the orphan records of EHA after 15 minutes.	No change required.
CleanMPPStaleDataInterval	The time interval in minutes after which ICR Admin calls MPP for cleaning the orphan records in a database.	15	



Note:

After making changes in the `VP_ICRAdmin.properties` file, you must restart the Experience Portal Manager service.

Chapter 10: Uninstalling Intelligent Customer Routing

Uninstalling ICR components installed on a standalone system

Procedure

1. Log on to the ICR system as a root user.
2. On the screen, type **cd /opt/Avaya/ICR/ICR_Uninstaller** and press Enter.
3. Type **./uninstall_ICR**.
4. On the Uninstall ICR screen, press Enter.
5. On the Uninstall Options screen, type the number corresponding to the required following options and press Enter.
 - **1:** Completely remove all features and components.
 - **2:** Choose specific features that were installed by InstallAnywhere.
6. Type 1 to continue uninstalling all the ICR features and components or type 2 to choose specific features to uninstall.
7. Press Enter to continue the uninstallation.

```
=====
=====
Choose Product Features
-----

ENTER A COMMA_SEPARATED LIST OF NUMBERS REPRESENTING THE FEATURES YOU WOULD
LIKE TO SELECT, OR DESELECT. TO VIEW A FEATURE'S DESCRIPTION, ENTER
'?<NUMBER>'. PRESS WHEN YOU ARE DONE:

    1- [ ] ICRAdmin
    2- [ ] ICRCCA
    3- [ ] ICRCore

Check the features that you want to uninstall. Unchecked features will
remain installed.:
=====
=====
```

8. Type the number corresponding to the features that you want to uninstall and press Enter.

Type the numbers separating with a comma.

```
=====
=====
Are you sure you want to uninstall feature(s) ICRCCA?
-----

This will uninstall feature(s) ICRCCA. Select "OK" to continue or "Cancel"
to
exit.

->1- OK
    2- Cancel

ENTER THE NUMBER OF THE DESIRED CHOICE, OR PRESS <ENTER> TO ACCEPT THE
DEFAULT:
=====
=====
```

9. On the Uninstall Confirmation screen, type 1 to confirm the unistallation or type 2 to cancel the uninstallation process.
10. Press Enter.

 Note:

The uninstaller stops all the running services for the selected ICR components and removes the selected components installed by the installer. However, the uninstaller does not remove the files and folders created during the installation.

After the uninstaller completes the uninstallation process, the system displays a message for successful uninstallation.

11. Log out from the Linux session and open a new Linux session to reinstall ICR. The updated environment variables are available in a new session.

Uninstalling ICR installed in a silent mode

Procedure

1. Log on to the ICR system as a root user.
2. On the screen, type **cd /opt/Avaya/ICR/ICR_Uninstaller** and press Enter.
3. Type **./uninstall_ICR** to uninstall all the ICR components saliently.
4. Type **./uninstall_ICR -i console** to select components for uninstalling.
5. On the Uninstall ICR screen, press Enter.

6. On the Uninstall Options screen, type the number corresponding to the required following options and press Enter.
 - **1:** Completely remove all features and components.
 - **2:** Choose specific features that were installed by InstallAnywhere.
7. Type 1 to continue uninstalling all the ICR features and components or type 2 to choose specific features to uninstall.
8. Press Enter to continue the uninstallation.

```
=====
=====
Choose Product Features
-----

ENTER A COMMA_SEPARATED LIST OF NUMBERS REPRESENTING THE FEATURES YOU WOULD
LIKE TO SELECT, OR DESELECT. TO VIEW A FEATURE'S DESCRIPTION, ENTER
'?<NUMBER>'. PRESS WHEN YOU ARE DONE:

    1- [ ] ICRAAdmin
    2- [ ] ICRCCA
    3- [ ] ICRCore

Check the features that you want to uninstall. Unchecked features will
remain installed.:
=====
=====
```

9. Type the number corresponding to the features that you want to uninstall and press Enter.

Type the numbers separating with a comma.

```
=====
=====
Are you sure you want to uninstall feature(s) ICRCCA?
-----

This will uninstall feature(s) ICRCCA. Select "OK" to continue or "Cancel"
to
exit.

    ->1- OK
        2- Cancel

ENTER THE NUMBER OF THE DESIRED CHOICE, OR PRESS <ENTER> TO ACCEPT THE
DEFAULT:
=====
=====
```

10. On the Uninstall Confirmation screen, type 1 to confirm the unistallation or type 2 to cancel the uninstallation process.
11. Press Enter.



Note:

The uninstaller stops all the running services for the selected ICR components and removes the selected components installed by the installer. However, the uninstaller does not remove the files and folders created during the installation.

After the uninstaller completes the uninstallation process, the system displays a message for successful uninstallation.

12. Log out from the Linux session and open a new Linux session to reinstall ICR.
The updated environment variables are available in a new session.
-

Appendix A: ICR CCA properties configuration for EWT or queue position update and spike

ICR CCA recognizes the Estimated Wait Time (EWT) update and spike based on the increase in the EWT or queue position received from Automatic Call Distribution (ACD).

ICR CCA receives the updated EWT and queue position from ACD after every 60 seconds. ICR CCA compares the updated EWT and queue position values with the update and spike properties configured in the `icrcca.properties` file and determines whether to terminate the running Wait Treatment Application (WTA) and relaunch the same WTA or launch another WTA.



Note:

- The spike condition for EWT or queue position occurs only when the update condition for respective EWT or queue position matches. Therefore, you must keep the EWT update and queue position update values less than the EWT spike and queue position spike values.
- When both the update and spike conditions for EWT or queue position matches, ICR considers the increase in EWT or queue position as spike.

In ICR, configure the following properties for ICR CCA to determine the EWT or queue position update and spike. You can find the properties in the `icrcca.properties` file located in the `$AVAYA_ICRCCA_HOME/tomcat/conf` directory.

EWT update

ICR CCA determines the EWT update based on the difference between two successive EWT values and percentage difference between two successive EWT values.

- **ewtUpdatePercent:** If the percentage difference between two successive EWT values is greater than the value set in the `ewtUpdatePercent` property, ICR CCA terminates the running WTA and relaunches the same WTA. ICR CCA uses the `ewtUpdatePercent` property in conjunction with `ewtUpdatedDiff` property.

For example: The `ewtUpdatePercent` property is set to 20. For a call in queue, the first EWT that ICR CCA receives from ACD is 100 and for the same call, the second EWT that ICR CCA receives from ACD is 150.

As per the above example, the percentage difference between two EWT values is 50%, which is greater than the value 20 set in the `ewtUpdatedDiff` property. Therefore, ICR CCA terminates the running WTA and relaunch the same WTA if the increase in EWT also meets the `ewtUpdatedDiff` property configuration as mentioned below.

- **ewtUpdateDiff:** If the difference between two successive EWT values is greater than the value set in the `ewtUpdatedDiff` property, ICR CCA terminates the running WTA and relaunches the same

WTA. ICR CCA uses the `ewtUpdateDiff` property in conjunction with `ewtUpdatePercent` property.

For Example: The `ewtUpdatePercent` property is set to 20 and the `ewtUpdateDiff` property is set to 30. For a call in queue, the first EWT that ICR CCA receives from ACD is 100 and for the same call, the second EWT that ICR CCA receives is 150.

As per the above example, the difference between second EWT value and first EWT value is 50, which is greater than the value set in the `ewtUpdateDiff` property and percentage difference between first and second EWT value is 50%, which is also greater than the value set in the `ewtUpdatePercent` property. Therefore ICR CCA will terminate the running WTA and relaunch the same WTA.

EWT spike

ICR CCA determines the EWT spike based on the difference between two successive EWT values and percentage difference between two successive EWT values.

- **ewtSpikePercent:** If the percentage difference between two successive EWT values is greater than the value set in the `ewtSpikePercent` property, ICR CCA terminates the running WTA. After that ICR CCA launches a new WTA configured in **EWT range mapping for Skill-WTA** or relaunched the same WTA. ICR CCA uses the `ewtSpikePercent` property in conjunction with the `ewtSpikeDiff` property.

Examples:

- The `ewtSpikePercent` property is set to 1000. For a call in queue, the first EWT that ICR CCA receives from ACD is 120 and for the same call, the second EWT that ICR CCA receives is 300.

As per the above example, there is 250% increase in EWT, which is less than the value set in the `ewtSpikePercent` property. Therefore, ICR CCA does not consider the increase in EWT as spike.

- The `ewtSpikePercent` property is set to 1000. For a call in queue, the first EWT that ICR CCA receives from ACD is 120 and for the same call, the second EWT that ICR CCA receives is 1800.

As per the above example, there is 1500% increase in EWT, which is greater than 1000. Therefore, ICR CCA considers the increase in EWT as spike and terminates the running WTA if the increase in EWT also meets the `ewtSpikeDiff` property configuration as mentioned below. After that ICR CCA launches a new WTA based on the EWT range that you specify in **EWT range mapping for Skill-WTA** or relaunched the same WTA.

- **ewtSpikeDiff:** If the difference between two successive EWT values is greater than the value set in the `ewtSpikeDiff` property, ICR CCA terminates the running WTA and launches a new WTA based on the EWT range that you specify in **EWT range mapping for Skill-WTA** or relaunched the same WTA. ICR CCA uses the `ewtSpikeDiff` property in conjunction with the `ewtSpikePercent` property.

Examples:

- The `ewtSpikePercent` property is set to 1000 and the `ewtSpikeDiff` property is set to 100. For a call in queue, the first EWT that ICR CCA receives from ACD is 5 and for the same call, the second EWT that ICR CCA receives is 80.

As per the above example, there is 1600% increase in the new EWT value but the spike difference is 75, which is less than the value set in the `ewtSpikeDiff` property. Therefore, ICR CCA does not consider the increase in EWT as spike.

- The `ewtSpikePercent` property is set to 1000 and the `ewtSpikeDiff` property is set to 100. For a call in queue, the first EWT that ICR CCA receives from ACD is 30 and for the same call, the second EWT that ICR CCA receives is 400.

As per the above example, there is 1333% increase in the new EWT value and spike difference is 370, which is greater than the value set in the `ewtSpikeDiff` property. Therefore, ICR CCA considers the increase in EWT as a spike. After that ICR CCA terminates the running WTA and launches a new WTA configured in **EWT range mapping for Skill-WTA** or relaunches the same WTA.

Queue position update

Similar to EWT update, ICR CCA determines the queue position update using the following property.

queuePositionUpdateDiff: If the difference between two successive queue position values is greater than the value set in the `queuePositionUpdateDiff` property, ICR CCA terminates the running WTA and relaunches the same WTA.

For Example: The `queuePositionUpdateDiff` property is set to 10. For a call in queue, the current queue position that ICR CCA receives from ACD is 50 and for the same call, the new queue position that ICR CCA receives from ACD is 80.

As per the above example, the difference in two queue position values is 30, which is greater than the value set in the `queuePositionUpdateDiff` property. Therefore, ICR CCA terminates the running WTA and relaunches the same WTA.

Queue position spike

Similar to EWT spike, ICR CCA determines the queue position spike using the following property.

queuePositionSpikeDiff: If the difference between two successive queue position values is greater than the value set in the `queuePositionSpikeDiff` property, ICR CCA terminates the running WTA and launches a new WTA based on the EWT range that you specify in **EWT range mapping for Skill-WTA** or relaunches the same WTA.

For example: The `queuePositionSpikeDiff` property is set to 60. For a call in queue, the current queue position that ICR CCA receives from ACD is 50 and for the same call, the new queue position that ICR CCA receives from ACD is 180.

As per the above example, the difference between two queue position values is 130, which is greater than the value set in the `queuePositionSpikeDiff` property. Therefore, ICR CCA terminates the running WTA and launches a new WTA based on the EWT range that you specify in **EWT range mapping for Skill-WTA** or relaunches the same WTA.

ICR CCA properties configuration for EWT or queue position update and spike

Appendix B: Ports used by ICR

ICR Core service

Port Number	Protocol	Process	Used For
9009	TCP	Java	Apache tomcat AJP connection.
9005	TCP	Java	Apache tomcat shutdown.
5060/5061	TCP	Java	SIP communication with a Proxy server.
9090	TCP	Java	Communication between ICR Core and ICR Admin.

ICR Management service

Port Number	Protocol	Process	Used For
9109	TCP	Java	Apache tomcat AJP connection.
9005	TCP	Java	Apache tomcat shutdown.

Terracotta server

Port Number	Protocol	Process	Used For
9510/9520	TCP	Java	Communication between Terracotta server and ICR Core.

ICR CCA service

Port Number	Protocol	Process	Used For
6009	TCP	Java	Apache tomcat AJP connection.
6005	TCP	Java	Apache tomcat shutdown.

Ports used by ICR

Port Number	Protocol	Process	Used For
6080	TCP	Java	HTTP connection handler.

Appendix C: Mounting the ICR media

Before running the ICR installer, you must mount the ICR media from an ISO image format or from a CD or DVD.

The appendix provides the steps to mount the ICR media both from an ISO image and from a CD or DVD. However, you can use any one method to mount the ICR media.

Mounting the ISO image of the ICR installer

About this task

If you want to install ICR using the ISO image of an ICR installer, perform the following steps to mount the ISO image of the ICR installer.

Procedure

1. Download the ISO image of the ICR 6.0 software installer from the Avaya support Web site.
2. Log in to an Experience Portal Manager system on which you want to install ICR.
 - a. Log on to the Linux system either locally as a root user or remotely as a non-root user and change the user to root by using the **su** - command.
 - b. If you are an Avaya Services representative and if you are using Avaya Enterprise Linux or if the Avaya Service accounts are installed on this Core system:
 - Log on to the local Linux system as a sroot user.
 - Or log on remotely as a non-root user and change the user to sroot by entering the **su** - sroot command.
3. Copy the ISO image in a local directory on the system.
4. Create a directory to mount the ISO image.
Enter the command: **mkdir** <Mount_Point_Directory>.
5. Mount the ISO image.
Enter the command: **mount** -o loop
<Absolute_Path_Of_ISO_Image_File> <Mount_Point_Directory>.

The system mounts the files from the ISO image of the ICR software installer to the mount point directory.

6. Change the directory to the mount point directory.

Enter the command: **cd** <Mount_Point_Directory>.

Mounting the ICR installer CD or DVD

About this task

If you create an ICR installer CD or DVD using the ISO image, perform the following steps to mount the ICR installer CD or DVD.



Note:

If you are unable to mount the installer CD or DVD using the commands given in this topic, see the server documentation for the appropriate mount command.

Procedure

1. Log in to an Experience Portal Manager system on which you want to install ICR.
 - a. Log on to the Linux system either locally as a root user or remotely as a non-root user and change the user to root by using the **su** - command.
 - b. If you are an Avaya Services representative and if you are using Avaya Enterprise Linux or if the Avaya Service accounts are installed on this Core system:
 - Log on to the local Linux system as a sroot user.
 - Or log on remotely as a non-root user and change the user to sroot by entering the **su** - sroot command.
2. In the CD or DVD drive of the system, insert the ICR 6.0 software installation CD or DVD.



Tip:

The instructions given in this procedure assumes that you access the ICR installation CD or DVD by mounting the appropriate CD or DVD drive on the target system. To access the installation CD or DVD files from a shared network directory or a local directory, copy the files from the ICR installation CD or DVD to the respective directory. However, all the users on the system must be able to connect to that directory because the Avaya Aura[®] Experience Portal installation script changes users during execution. If the directory is only readable by the root or sroot user or the directory name contains spaces, the installation script can encounter errors and cannot complete successfully.

3. Mount the ICR 6.0 software installation CD or DVD.

The mount command depends on the system hardware and operating system.

If you are working with Avaya Enterprise Linux, enter the command **mount /mnt/cdrom** to mount the CD or DVD.

Here, */mnt/cdrom* is the mount point usually associated with the CD or DVD device in the *fstab* file.

4. If you are working with Red Hat Enterprise Linux Server 6.0, enter the following commands to mount the CD or DVD:

- *mkdir /media/cdrom*



Note:

Run this command only if the */media/cdrom* mount point is not created.

- *mount /dev/cdrom /media/cdrom*



Warning:

When Red Hat Enterprise Linux Server 6.0 automatically mounts the CD or DVD, the files on the CD or DVD are not executable. You must manually mount the ICR6.0 software installation CD or DVD using the above commands.

5. Change to the mount point directory.

Enter the command: **cd <Mount_Point_Directory>**.

Index

A

AAEP [60](#), [62](#), [63](#)
 AAEP to CM [64](#)
 about application server [73](#)
 about ICR installation [17](#)
 add IP codec set [51](#)
 add IP network region [50](#)
 add queue VDN to public [50](#)
 adding [67](#)
 SIP connection for Session Manager [67](#)
 Architecture [11](#)

B

backup and restore [9](#)
 benefits [8](#)

C

CCA [12](#)
 CM [59](#)
 Communication Manager [55](#), [56](#)
 components [11](#), [12](#)
 ICR Admin [11](#)
 ICR CCA [12](#)
 ICR Core [12](#)
 configuration [89](#)
 cca properties for EWT and queue position update
 and spike [89](#)
 configuring Avaya Aura® Experience Portal [67](#)
 configuring multiple ICR Core servers for the high
 availability mode [31](#)
 copy sample application [69](#)
 create Queuing vector [45](#)
 create vector [44](#)

D

deploying ICR [13](#)
 Dial Plan [64](#)

E

enable sample application [71](#)
 Enhanced/Advanced Wait Treatment [9](#)

EPM [9](#)

F

features [9](#)

G

G860 gateway [54](#), [58](#)

H

hunt group [43](#)

I

ICR CCA property file [78](#), [81](#)
 ICR configuration [11](#)
 ICR Core [57](#)
 ICR deployment [14](#), [15](#)
 multiple data centers and multiple contact centers [15](#)
 single data center and multiple contact centers ... [14](#)
 single site contact center [14](#)
 ICR deployment models [13](#)
 ICR installation [26](#)
 on a single system [26](#)
 ICR server node [61](#)
 ICR silent install [35](#)
 ICR user [65](#)
 import ICR core certificate [73](#)
 importing sample application in Eclipse [70](#)
 install ICR Admin [19](#)
 install ICR CCA [21](#)
 install ICR Core [23](#)
 installing ICR Core on multiple systems [31](#)
 introduction [7](#)

L

licensing [11](#)
 log on to System Manager [53](#)
 login to CM [39](#)

M		
mounting	96	
ICR installer CD or DVD	96	
mounting ICR media	95	
mounting the ISO image of ICR installer	95	
N		
node names	39	
P		
PDC	9	
pluggable data connector	69	
polling VDN	46	
ports used by ICR	93	
properties file for	75	
ICR Core (icrcore.properties)	75	
Q		
queuing VDN	48	
R		
reports	9	
		requirements
		software and hardware
		Routing Policy
		S
		sample applications
		EHA
		SSA
		WTA
		signaling group
		SIP domain
		SIP Entities
		SIP Entity
		SIP Entity link
		SIP Entity Link
		T
		trunk group
		U
		uninstalling ICR
		from a standalone system
		installed in a silent mode
		user roles