



Avaya IQ

Administration

Release 4.1
March 2008

Notice

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

Documentation disclaimer

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

Link disclaimer

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

Warranty

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

<http://www.avaya.com/support>

License

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

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

License type(s)

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

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

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). Customer 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 Product that permits one user to interface with the Product.

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

Copyright

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

Third-party components

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

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

Preventing toll fraud

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

Avaya fraud intervention

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

<http://www.avaya.com/support>

Trademarks

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

All other trademarks are the property of their respective owners.

Downloading documents

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

<http://www.avaya.com/support>

COMPAS

This document is also available from the COMPAS database. The COMPAS ID for this document is 115656.

Avaya support

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

<http://www.avaya.com/support>

Contents

About administration	9
Overview of Avaya IQ administration	9
Administration road map	10
Security best practices for administration	11
Getting started with administration	13
Logging on	13
Duplicate logon sessions	16
Multiple administration sessions	16
Interface layout	17
Logging out	18
Changing passwords	18
Path	18
Description	18
Assistance for users with disabilities	19
Managing resources	21
About resources	22
About reporting group management	23
Reporting group management scenario	24
Managing reporting groups by function	25
Managing reporting groups by location	26
Administering reporting groups	26
Permissions required to administer reporting groups	27
Considerations when creating groups	28
Creating categories	28
Creating groups	28
Selecting resources for adding to a group	29
Adding resources to groups	30
Removing resources from groups	31
Copying groups to a different category	31
Moving groups to a different category	31
Copying categories to a different view	32
Moving categories to a different view	32
Removing groups	33
Removing categories	33
Administering users	34
User administration options	34
Adding users	35

Listing users	36
Searching for users	36
Editing user options	37
Cleaning up user accounts before deleting users.	37
Deleting users	37
About user roles	38
Role definitions	38
About application operations	39
Administrative tasks.	39
Maintenance tasks	40
Reporting tasks	41
Scheduling jobs	42
About data access permissions	42
Default roles	44
Planning your roles	47
Administering roles	49
Adding a new role	49
Editing general role options	50
Editing a role to add operations	50
Editing a role to add users	51
Editing a role to assign data access permissions.	51
Displaying group membership of a role	54
Displaying user role assignments	55
Administering permissions for a user	56
Unlocking user accounts	59
Unlocking an administration user account	59
Unlocking a reporting user account	59
Managing reporting preferences	61
Administering threshold definitions	61
Threshold definition options	62
Administering threshold definitions	65
Adding a threshold definitions	65
Changing a threshold definition	66
Deleting threshold definitions	66
Administering reporting behaviors.	67
Behavior definition options	69
Administering behavior definitions.	70
Administering service level targets.	72
Service level target options	72

Administering service level target definitions	73
About reporting names management	74
Administering agent activity states	75
Agent activity state options	76
Administering agent activity state definitions	78
Administering agent logout reason codes	79
Agent logout reasons options	79
Administering agent logout reasons	80
Administering reporting keywords	81
Keywords options	81
Administering keywords	82
Managing contact center preferences	83
Administering multiple agent queue assignments	83
Multiple agent queue assignment options	83
Adding multiple agent queue assignments	84
Changing multiple agent queue assignments	85
Removing multiple agent queue assignments	86
Administering agent call handling options	87
Agent call handling options	87
Call handling preferences (General tab)	88
Queue assignments (General tab)	88
Selected agents (Additional Agents)	89
Changing agent call handling options	90
Permissions required to administer agent call handling options	90
Interactions with unmeasured queues	90
Planning your call handling options	91
Using the agent editor	91
Administering routing point options	92
Managing system preferences	95
Administering login session properties	95
Path	95
Field descriptions	95
Changing the administration logon security banner	96
Administering connection properties	97
Administering database connection properties	97
Integrating with Active Directory	98
Prerequisites	98
Administering an LDAP connection	98

Administering a one-time job for initial synchronization	101
Administering Communication Manager connections	101
Administering Proactive Contact connections	102
Administering Reporting connections	102
Administering SNMP alarming	102
Administering advanced properties	103
Scheduling jobs	105
Scheduler job options	105
Creating an on-demand scheduled job.	107
Creating scheduled jobs using a resource editor	107
Viewing the status and history of scheduled jobs.	108
Editing a scheduled job	109
Disabling, enabling, and deleting scheduled jobs.	110
Managing scheduled jobs.	111
Routine maintenance	113
Monitoring logs and alarms.	114
Backup strategies	114
Backing up Avaya IQ data.	116
Backing up the operating system	117
Backing up the database	117
Sample backup scenarios.	118
General backup procedures	120
Oracle files required to perform backup procedures	121
RMAN setup and configuration	122
Configuring RMAN and FRA	123
Configuring an RMAN catalog	126
RMAN configuration for control files	131
Display RMAN configuration	131
RMAN auto-backup location and file format for control files	132
RMAN backup of control file naming convention	132
Validation of RMAN backup of control file naming convention	133
Full backup of database and archive logs (first on-line backup).	134
Full backup of database and archive logs with archive log purge	136
RMAN incremental differential backup.	136
RMAN incremental cumulative backup.	137
RMAN tablespace backup.	137
Creating a cron job to schedule your full backup	138

Verifying backup sets	140
List backup set.	140
Validate backup set	143
Verify backup sets have been created in the specified location	144
Testing the backups for restores	145
Cleaning up user accounts	146
About licensing	146
Acquiring and installing license files.	148
Acquiring a license file	148
Installing a license file.	149
Maintaining license files.	150
Checking status of a license	150
Replacing a license file	150
Installing updates	151
Editing properties	152
Changing the reporting email server.	152
Changing the reporting host used for aggregation	154
Adjusting parameters for communication with Proactive Contact cron jobs	155
Loading date and time zone data	156
Date and time zone command options	157
Using the date and time zone command	158
Verifying date, time, and NTP status	159
Changing the database user names or passwords	159
Changing the SDS password on Avaya IQ.	160
Changing a user name or password on Avaya IQ.	161
Database management	164
Data removal	164
Database schema and metadata sanity check.	165
Reinitializing user service.	166
Editing the service configuration.	166
Managing distributors	166
Managing trusted certificates.	166
Listing server certificates	167
Viewing server certificates	167
Adding server certificates.	167
Importing server certificates	168
Exporting server certificates	168
Deleting server certificates	169

Contents

Viewing pending certificates	169
Default server certificate settings	170
Listing trusted certificates	170
Viewing trusted certificates	170
Importing trusted certificates	171
Exporting trusted certificates	171
Deleting trusted certificates.	172
JKS synchronization	172
Appendix A: Administration worksheets.	173
Reporting group worksheets	175
Creating reporting groups	177
Choosing group members	179
Active Directory worksheet for LDAP integration	181
Index	183

About administration

Avaya IQ administration allows centralized control to your call center operation. You can administer resource permissions, reporting groups, call center features, and Avaya IQ features all from one interface.

This section includes the following topics:

- [Overview of Avaya IQ administration](#) on page 9
- [Administration road map](#) on page 10
- [Security best practices for administration](#) on page 11

Overview of Avaya IQ administration

Avaya IQ administration includes the following capabilities:

- Administration access through a Web browser user interface, so there is no client software installation and maintenance (see [Getting started with administration](#) on page 13)
- Host administration within the deployment, including administration of the links to Communication Manager and Proactive Contact systems which is done by Avaya or BusinessPartner provisioning personnel (see [Initial administration](#) on page 59 in *Avaya IQ Implementation*)
- Group your resources to reflect your business structure, from a broad to a fine level of granularity (see [About reporting group management](#) on page 23 and [Administering reporting groups](#) on page 26)
- Create user roles and permissions to control who has access to both administration and sensitive reporting data ([About user roles](#) on page 38, [Administering roles](#) on page 49, [About data access permissions](#) on page 42, and [Administering permissions for a user](#) on page 56)
- Administer call center resource attributes, such as agent queue (skill) assignment, and have those options synchronized with Communication Manager software (see [Administering multiple agent queue assignments](#) on page 83 and [Administering agent call handling options](#) on page 87)
- Integrate your corporate enterprise directory with Avaya IQ to manage employee access to Avaya IQ and eliminate redundant administration of user names ([Integrating with Active Directory](#) on page 98)
- Schedule administration changes to accommodate special or regular changes in business needs and strategy ([Scheduling jobs](#) on page 105)

- Multiple language support for synonyms of static values that display in reports (for example, yes or no, occupied or not occupied, and so on), auxiliary states (Aux. reason codes), logout reason codes, and result codes (call work codes from Communication Manager and completion codes from Proactive Contact) (see [Managing reporting preferences](#) on page 61)

Administration road map

When your Avaya IQ system is installed by Avaya or a BusinessPartner, the implementation personnel do all of the administrative procedures found in [Initial administration](#) on page 59 of *Avaya IQ Implementation*. After this administration has been done, you would typically not need to concern yourself with any of this administration.

After Avaya has turned over your Avaya IQ system to you, there is a typical order in which you will want to administer your system. This section describes this order for administration.

User administration: Initially, your systems administrator should create roles, operations, and permissions for your operations manager and telecom manager. This information is described in the following sections:

- [Administering users](#) on page 34
- [About user roles](#) on page 38
- [About data access permissions](#) on page 42

Setting up reporting groups: This is maybe the most important work that your operations manager will do. The reporting groups define how you will see your reporting data to best operate your contact center. This information is described in the following sections:

- [About reporting group management](#) on page 23
- [Administering reporting groups](#) on page 26

Roles and permissions: For all of your report users, you will have to administer roles and permissions so that they can access the data on which they need to view reports. This information is described in the following sections:

- [About user roles](#) on page 38
- [Administering roles](#) on page 49
- [About data access permissions](#) on page 42
- [Administering permissions for a user](#) on page 56

Reporting preferences: Your operations manager should then administer your reporting preferences as described in [Managing reporting preferences](#) on page 61.

Day to day operations: In no particular order, you will also want to use the following administrative procedures:

- [Administering multiple agent queue assignments](#) on page 83
- [Administering agent call handling options](#) on page 87
- [Administering routing point options](#) on page 92
- [Scheduling jobs](#) on page 105

Routine maintenance procedures: You need to monitor the system to make sure it is working properly, you are collecting data from your sources, you are backing up your reporting data, and so on. These operations are described in the following sections:

- [Administering login session properties](#) on page 95
- [Unlocking user accounts](#) on page 59
- [Routine maintenance](#) on page 113

Security best practices for administration

Use the following best practices to help maintain a secure environment around Avaya IQ:

- Use role assignments to appropriately restrict access to operations. For more information, see [About user roles](#) on page 38.
- Use data access permissions to appropriately restrict access to resource data. For more information, see [Editing a role to add users](#) on page 51.
- Use the Login Session Properties to help prevent unauthorized access. For more information, see [Administering login session properties](#) on page 95.
- Do not create shared logins or allow use of shared logins. For accountability, each user must have a unique login ID. Instruct users to not share their login ID and password. For more information, see [Administering users](#) on page 34.
- Instruct users to check the displayed time and date of their last successful login. If the user reports unknown activity on their account, either change the password on that account, or delete the account and give the user a new account.
- Periodically review and update the list of administered users, their roles, and their permissions.
- Review administration audit logs on a regular basis to check the validity of administration changes.
- Review audit logs on a regular basis to ensure that the system is operating properly.
- Review security logs and alarms on a frequent basis to monitor possible security events.

About administration

- Make sure that backups are being done on Avaya IQ data and the database. See [Routine maintenance](#) on page 113.

Getting started with administration

This section contains procedures that will help you get started with administration. It will briefly describe how to log in and log out, change your password, and understand the user interface. This section includes the following topics:

- [Logging on](#) on page 13
- [Duplicate logon sessions](#) on page 16
- [Multiple administration sessions](#) on page 16
- [Interface layout](#) on page 17
- [Logging out](#) on page 18
- [Changing passwords](#) on page 18
- [Assistance for users with disabilities](#) on page 19

Logging on

Avaya IQ has a separate interface for administration and reporting. Users of both interfaces must log in separately to each interface. This section describes how to log in to each interface. Administrators need to instruct their report users how to log in to the reporting interface. If you have more than one Reporting host in your deployment, you may have to manually balance the number of report users you assign to each host.

Note:

When using a pop-up blocker in a browser, you must configure the pop-up blocker to allow pop-ups from the application host sites. Use the tools setting of your browser to control the allowed sites. When adding an allowed site to the list, use the IP address of the root host machine.

To log on to administration:

1. Set the resolution of your monitor to a minimum of 1024x768. Ideally, you should set your monitor resolution to 1280x1024.
2. Using your browser, enter:

`https://host_machine:port#/CS-OAM/`

The variable `host_machine` is the FQDN or IP address of the All Functions host or Administration host, and `port#` is the TCP port used for the connection (the default is 28443).

Note:

If the Security Banner option is enabled, you will see a warning message before you are allowed to log in. See [Administering login session properties](#) on page 95 for more information about this option.

3. Enter your logon ID and password.

4. Select **Logon**.

You are logged in to the administration interface. The locale settings for the login session are set automatically based on your browser settings.

Contact your system administrator if you cannot log in to the system.

To log on to reporting:

1. Set the resolution of your monitor to a minimum of 1024x768. Ideally, you should set your monitor resolution to 1280x1024.
2. Using your browser, enter:

`https://reporting_host:port#/avaya-ccr/`

The variable *reporting_host* is the FQDN or IP address of the All Functions host or a Reporting host, and *port#* is the TCP port used for the connection (the default is 18443)

3. Enter your logon ID and password.
4. Select **Logon**.

You are logged in to the reporting interface. The locale settings for the login session are set automatically based on your browser settings.

Contact your system administrator if you cannot log in to the system.

Responding to certificate messages

When logging on to administration or reporting, you may receive a certificate security message. To avoid having to respond to this message every time you log on, you can accept and install the certificate the first time you log on. The steps you take to accept and install the certificate are different depending on your browser version.

To accept a security certificate when using Internet Explorer 6.0:

1. When the Security Alert dialog is displayed, select **View Certificate**.

The Certificate dialog is displayed.

2. Select **Install Certificate**.

The Certificate Import Wizard dialog is displayed.

3. Select **Next** twice and then select **Finish**.

A Security Warning dialog is displayed.

4. Select **Yes**.
A confirmation dialog is displayed.
5. Select **OK**.
The Certificate dialog is displayed.
6. Select **OK**.
The Logon dialog is displayed.

To accept a security certificate when using Internet Explorer 7.0:

1. When the Certificate Error dialog is displayed, select **Continue to this website (not recommended)**.
The Address Bar turns pink. There will be a **Certificate Error** button next to the error message.
2. Select **Certificate Error**.
The Security Alert dialog is displayed.
3. Select **View Certificate**.
The Certificate dialog is displayed.
4. Select **Install Certificate**.
The Certificate Import Wizard dialog is displayed.
5. Select **Next** twice and then select **Finish**.
A Security Warning dialog is displayed.
6. Select **Yes**.
A confirmation dialog is displayed.
7. Select **OK**.
The Certificate dialog is displayed.
8. Select **OK**.
The Logon dialog is displayed.

To accept a security certificate when using Firefox 2.0:

1. When the Website Certified by an Unknown Authority dialog is displayed, select **Accept this certificate permanently**.
2. Select **OK**.
The Logon dialog is displayed.

Duplicate logon sessions



SECURITY ALERT:

Avaya recommends that every administration user have their own login IDs. Do not share login IDs. All changes by administration users are logged to help you determine if users are making unauthorized or invalid administration changes.

If a user attempts to log in to administration when that user is already logged in, the user will see a **Duplicate Logon** message.

This message confirms that the user is already logged in. If users see this message, one of two events have occurred:

- Someone has obtained the user's login ID and password and is illegally accessing the system. You should immediately delete that login ID and reissue a new login ID to the user.
- The user has forgotten that they were already logged in. The user can just continue with their login session. Remind users to log out when not using administration.

Multiple administration sessions

More than one administrator can access the system and make changes at the same time. For example, you can have several supervisors logged in to change agent queue and routing point administration to handle changing traffic conditions. In these situations, you may have conditions where one administrator overwrites changes made by another administrator or changes by one administrator prohibits changes by another administrator.

If you are making changes where updates are sent to a Communication Manager system, there is no contention management among multiple administrators. For example, if two supervisors are making changes for the same agent, the supervisor to submit the change last will overwrite the changes made by the other supervisor. The system does not notify the first supervisor that their changes were overwritten. You must communicate this potential condition to any of your personnel who are making these types of administrative changes. This condition might occur with the following operations:

- [Administering multiple agent queue assignments](#) on page 83
- [Changing agent call handling options](#) on page 90
- [Administering routing point options](#) on page 92

You should also be aware that if an administrator is making changes to these options using Communication Manager administration or Call Management System administration, there is no contention management for those operations.

If two or more users are making changes to local Avaya IQ features (information not communicated to a Communication Manager system), there is some limited contention handling. The first user to submit their changes will have the change accepted by the system. Any other users who were attempting to make a change to the same administrative object at the same time will get an error and must start over with the administration task. For example, if two users are making changes to the login session properties at the same time, the first user to submit the change will have the change accepted. The second user will get an error message. To successfully make a change on the same administrative object, the second user must leave that administrative object, reselect the object, reenter their changes, and resubmit their change.

Interface layout

After you log in to administration, you will see a navigation pane on the left and a work pane on the right. In the navigation pane, which can be resized, there are two tabs: Tasks and Enterprise.

Tasks: The **Tasks** tab gives you access to the following operations:

- User Management, which includes [Administering users](#) on page 34, [Unlocking user accounts](#) on page 59, and [Administering multiple agent queue assignments](#) on page 83.
- System Maintenance, which includes the Log Viewer and Alarm Manager. See *Avaya IQ Alarms and Logs* for more information.
- System Configuration, which includes [Changing passwords](#) on page 18, [Editing the service configuration](#) on page 166, [Reinitializing user service](#) on page 166, [Managing distributors](#) on page 166, and Log and Alarm Options. See *Avaya IQ Alarms and Logs* for more information.
- Utility, which includes Ping and [Scheduling jobs](#) on page 105.
- System Properties, which includes [Administering login session properties](#) on page 95.
- Connection Management, which includes [Administering connection properties](#) on page 97, [Integrating with Active Directory](#) on page 98, [Creating Communication Manager sources](#) on page 94 in *Avaya IQ Implementation*, and [Creating Proactive Contact sources](#) on page 96 in *Avaya IQ Implementation*.
- Security, which includes [Managing trusted certificates](#) on page 166.

Enterprise: The **Enterprise** tab gives you access to the following operations:

- Sites, which includes [Administering sites](#) on page 67 and [Administering hosts](#) on page 69 in *Avaya IQ Implementation*. These operations are typically done during system implementation and would not be used after your system is in operational mode.
- Resources, which includes [Managing resources](#) on page 21, [Managing reporting preferences](#) on page 61, and [Managing contact center preferences](#) on page 83.

The tool bar provides access to the following features:

Home: The **Home** button displays the Welcome to OAM dialog.

Help: The **Help** button opens the on-line help and version information about the product. In addition to the **Help** button on the tool bar, there are context-sensitive help icons on most dialogs. To navigate the help system, there are two ways to control your movement. As you step through different help topics, use the browser **Back** and **Forward** buttons to move back and forth through help topics you have been viewing. On the help system dialog, there are **Previous** and **Next** control buttons that move you through an ordered list of topics.

Log Off: The **Log Off** button logs you out of the administration interface.

Logging out

When finished with your login session, you should always log out. Logging out will keep unauthorized users from access administration.

To log out, select **Log Out** on the tool bar.

If you do not log out manually, your session will time out based on the session timeout values as described in [Administering login session properties](#) on page 95. Before your session is terminated, a warning message is displayed allowing you to continue or resume your session.

Changing passwords

This section describes how to change administrator passwords.

Path

System Configuration > Manage Administrative Data > Change Password

Description

Enter your user ID, old password, new password, and confirm your new password. Even though Avaya IQ does not enforce password rules, passwords should meet the following criteria:

- Passwords must be 8 to 14 characters long.
- Passwords must include a mix of the following character types:
 - Lower case letters

- Upper case letters
- Numerals
- Other keyboard symbol punctuation marks and non-alpha characters
- Passwords are case sensitive.
- Passwords cannot be identical to your previous 10 passwords.
- Do not use your last name, first name, or any other personal information.
- Passwords should be changed every 90 days.

After you submit the change, a success or failure message is displayed. If the change was not accepted, try again, making sure you enter the user ID and passwords correctly. Verify that the Caps Lock key is not on.

Assistance for users with disabilities

This section contains tips for users with disabilities. These tips may be used during administration sessions to help users better navigate the interface.

- The Firefox browser tends to render the administration interface better than the Internet Explorer browser. Users may have better experiences using Firefox.
- Users can use tabs to move through dialogs, though some tab operation may be less than optimal. In some dialogs, you have to tab through some fields that are not part of the dialog to get to all of the option fields.
- Icons in the interface have tool tips that are recognized by screen readers.

Managing resources

This section contains conceptual information about resource management and procedures about administering resources. This section includes the following topics:

- [About resources](#) on page 22
- [About reporting group management](#) on page 23
- [Administering reporting groups](#) on page 26
- [Administering users](#) on page 34
- [About user roles](#) on page 38
- [Administering roles](#) on page 49
- [Administering permissions for a user](#) on page 56
- [Unlocking user accounts](#) on page 59

The following topics have information related to managing resources:

- [Managing reporting preferences](#) on page 61
- [Administering connection properties](#) on page 97

About resources

The reliable operation of your contact center depends on many factors, including the efficiency of your agents, the ability of supervisors to recognize changes in call handling requirements, the way calls are routed, and so on. For you to create an efficient contact center you must have the ability to monitor the contact center operation and make adjustments to the resources that make up your call center. These resources include the following elements:

Users: Users of Avaya IQ are employees of your contact center that administer the reporting options and supervisors that run reports. Administrators use the administration interface to set up other users, reporting groups and definitions, and user roles. Report users can be agent supervisors who need to monitor the efficiency of agents or operations managers that must monitor the overall operation of the enterprise.

Agents: Agents are typically the front line interface to your customer, both for incoming and outgoing contacts. The performance of agents is the most critical factor in the operation of your contact center.

Queues: Queues are a virtual collection of agents that are designated to handle your incoming and outgoing calls. For example, you might have a queue of agents that are proficient at handling customer service calls or a queue of agents that are proficient at handling product sales. The agents assigned to queues can also change dynamically depending on your needs. Queues are known as "skills" in Communication Manager and "jobs" in Proactive Contact.

Routing points: Routing points are the published telephone numbers customers use to place calls to your contact center and the outgoing trunks used by Proactive Contact for outgoing calls. Routing points are known as "Vector Directory Numbers (VDNs)" in Communication Manager.

All of these resources are critical to the smooth operation of your contact center. For example, your agents may be working very efficiently, but your routing points are not getting calls to them quickly enough. Or, your routing points are organized logically based on target customers, but your queues are not set up to handle that logic.

To create valid reports that reflect an accurate measure of how these resources are operating, you must group those resources to best reflect the structure of your contact center operation. See [About reporting group management](#) on page 23 for more information about structuring your reporting groups.

About reporting group management

Reporting group management provides the following essential benefits:

- It allows you to group your agent, queue, and routing point resources in a manner that best suits your business model.
- It allows you to group those resources so that you can create reports that accurately reflect the operation of your contact center.
- It gives you the flexibility to group the same resources in different ways to satisfy the reporting requirements of different managers in your operation (for example, Directors, Supervisor Managers, Operations Managers).

With group management, you can select from all available resources to create your reporting groups. You can group your resources any way that works best for you, such as by function, location, or organization.

For example, you can group new agents in two ways:

- All new agents are assigned to one group so that you can closely monitor their performance in their new jobs.
- The new agents are also assigned to other agents groups based on their job assignment.

You can then run reports on all of the new agents as a group, and on the new agents as they function within their job assignment groups. When the new agents have proven that they can do their new job, you can remove them out of the special reporting group.



Important:

Avaya Proactive Contact uses special routing points and queues to acquire agents from Avaya Communication Manager for outbound work. These entities are administered on Communication Manager for the sole purpose of acquiring agents and are not directly involved in the processing and delivery of outbound contacts. In general, these entities are not associated with measures that are useful for monitoring contact center operations and performance. Avaya recommends that you do not include these acquire queues (skills) and routing points (VDNs) in reporting groups associated with a Proactive Contact system. Avaya recommends that you make a list of the acquire routing points used by your Proactive Contact system and the queue that is assigned to each acquire VDN. These queues are different from the queues that represent the actual outbound jobs and will not show significant data when shown in reports.

See [Reporting group management scenario](#) on page 24 for one example of how you can manage your resource groups. Once you have your reporting groups planned out, follow the instructions in [Administering reporting groups](#) on page 26 to set up your groups.

Reporting group management scenario

Acme Jet Pack Inc is a growing company in the jet pack aviation business. They have contact centers in Los Angeles, Tokyo, and London. The contact centers handle sales, repair, and support calls at all locations. Queues and routing points are shared within each functional group and at each location.

The contact center has two directors:

- Ms. Jones is responsible for each functional area across locations.
- Mr. Smith is responsible for the operation based on location.

Ms. Jones has three supervisor managers:

- Debra in sales
- Joe in repair
- Wallace in technical support

Each supervisor manager has three supervisors who are each responsible for a group of ten agents at a specific location. There is a total of 30 agents across all functions at each location.

Mr. Smith has three operations managers that are responsible for the operation at each location:

- Janice in Los Angeles
- Cal in Tokyo
- Susan in London

Since Ms. Jones and Mr. Smith have responsibilities in different areas, they have different reporting needs. To see how one might organize groups by function to support Ms. Jones, see [Managing reporting groups by function](#) on page 25. To see how one might organize groups to support Mr. Smith, see [Managing reporting groups by location](#) on page 26.

Managing reporting groups by function

Since Ms. Jones has responsibility for the contact center operation based on functional area, she would rather see the agents grouped by function: sales, repair, and support. The following graphic illustrates how you could group her agents, queues, and routing points:

View	Ms. Jones' Sales, Repair, and Support Functional Organizations		
Categories	Debra (Sales)	Joe (Repairs)	Wallace (Support)
Groups	Los Angeles Sales Agents 1-10	Los Angeles Repair Agents 1-10	Los Angeles Support Agents 1-10
	Tokyo Sales Agents 1-10	Tokyo Repair Agents 1-10	Tokyo Support Agents 1-10
	London Sales Agents 1-10	London Repair Agents 1-10	London Support Agents 1-10
	Debra's Sales Agents	Joe's Repair Agents	Wallace's Support Agents
	Debra's Sales Queues	Joe's Repair Queues	Wallace's Support Queues
	Debra's Sales Routing Points	Joe's Repair Routing Points	Wallace's Support Routing Points

In this example, each supervisor manager has the ability to report on the following grouped resources:

- Agents at each location by function (for example, London Support Agents 1-10)
- All agents by function regardless of location (for example, Joe's Repair Agents)
- All queues used by the functional group (for example, Debra's Sales Queues)
- All routing points used by the functional group (for example, Wallace's Support Routing Points)

These groups will allow Ms. Jones and her supervisor managers to report with the granularity they need based on functional responsibilities. For example, Debra can view reports on sales agents at different locations and all locations combined.

Though no operations managers directly report to Ms. Jones, administration of these groups is done by Mr. Smith's operations managers. For example, Janice would set up the Los Angeles sales, repair, and support agents. Cal would do the same for the Tokyo groups, and Susan for the London groups. One or more of the operations managers would then set up each supervisor manager's agent, queue, and routing point groups.

Managing reporting groups by location

Since Mr. Smith has responsibility for the contact center operation based on location, he would rather see the agents grouped by their location rather than their function. The following graphic illustrates how you could group his resources based on location:

View	Mr. Smith's Resources by Location		
Categories	Janice Los Angeles	Cal Tokyo	Susan London
Groups	All Los Angeles Agents (Sales, Repair, Support)	All Tokyo Agents (Sales, Repair, Support)	All London Agents (Sales, Repair, Support)
	All Los Angeles Queues (Sales, Repair, Support)	All Tokyo Queues (Sales, Repair, Support)	All London Queues (Sales, Repair, Support)
	All Los Angeles Routing Points (Sales, Repair, Support)	All Tokyo Routing Points (Sales, Repair, Support)	All London Routing Points (Sales, Repair, Support)

In this example, each operations manager has the ability to report on the following groups:

- All agents by location (for example, All Los Angeles Agents)
- All queues by locations (for example, All Tokyo Queues)
- All routing points by location (for example, All London Routing Points)

These groups will allow Mr. Smith and his operations managers to report on all resources based on location. The administration of these groups is done by Mr. Smith's operations managers.

Administering reporting groups

The main reason for creating a resource group is to report on specific groups of agents, queues, and routing points. The secondary reason for creating resource groups is to help manage groups of users, roles, and operations. For more information about these different resources and how they are used, see the following topics:

- [About resources](#) on page 22
- [Administering users](#) on page 34
- [About user roles](#) on page 38

Once you have planned out your resource groups as described in these sections, you can administer your resource groups. Administering resource groups consists of creating categories under views, creating groups under categories, and adding resources to groups. See the following procedures:

- [Permissions required to administer reporting groups](#) on page 27
- [Considerations when creating groups](#) on page 28
- [Creating categories](#) on page 28
- [Creating groups](#) on page 28
- [Selecting resources for adding to a group](#) on page 29
- [Adding resources to groups](#) on page 30
- [Removing resources from groups](#) on page 31
- [Copying groups to a different category](#) on page 31
- [Moving groups to a different category](#) on page 31
- [Copying categories to a different view](#) on page 32
- [Moving categories to a different view](#) on page 32
- [Removing groups](#) on page 33
- [Removing categories](#) on page 33

**Tip:**

Avaya recommends that you create all your categories and groups before you add any resources to the groups. By inspecting your view, category, and group setup, you can verify that you have created the proper reporting structure for your operation. If you change your reporting structure after you have added resources, you may have to add your resources again.

Permissions required to administer reporting groups

To administer resource groups, the administrator must have the following permissions:

- To create a category, the administrator must have read, add, and change permissions on the parent view.
- To create a group, the administrator must have read, add, and change permissions on the parent category.
- To add resources to a group, the administrator must have read and change permissions on the group.
- To copy a category, the administrator must have change permission on the originating category, and add and change permission on the destination category.

- To copy a group, the administrator must have change permission on the originating group, and add and change permission on the destination group.
- To move a category, the administrator must have delete permission on the originating category and change permission on the destination category.
- To move a group, the administrator must have delete permission on the originating group and change permission on the destination group.

Considerations when creating groups

This section contains considerations when you create groups.

- To report on vectors, you can create routing point groups that contain VDNs that point to a vector. Reports run on these groups are comparable to Call Management System vector reports.

Creating categories

To create a category:

1. Under the **Enterprise** tab, expand the **Resources** folder.
2. Select one of the views.
3. Select **New**.

The Create New Category dialog is displayed.

4. Enter a name and description for the category.
5. Select **OK**.

Creating groups

To create a group:

1. Under the **Enterprise** tab, expand the **Resources** folder.
2. Expand one of the views.
3. Select a category under the expanded view.
4. Select **New**.

The Create New Group dialog is displayed.

5. Enter a name and description for the group. Under the **Type** field, select the resource type that matches the group you are creating:

- Agent Activity States
 - Agents
 - Operations
 - Queues
 - Roles
 - Routing points
 - Users
6. Select **OK**.

Selecting resources for adding to a group

This section describes the hierarchy of resources used during the procedure [Adding resources to groups](#) on page 30.

The **Enterprise** tab includes the following default views:

- All Resources
- Functional
- Location
- Organizational
- User Defined

Note:

You can rename all views except for the All Resources view. The default names are used in these procedures.

The All Resources view contains the Communication Manager and Proactive Contact resources (agents, queues, and routing points) that are used for reporting. The All Resources view also contains the resources for defining operations, roles, reporting definitions, and users.

Initially, you can only select resources from the All Resources view when creating your reporting groups. Once you have added resources to reporting groups in any of the other views, you can add resources from any of those reporting groups. Since the resources from the All Resources view are essentially linked to the reporting groups, you are selecting the same resources whether you get them from the All Resources view or from the reporting groups you created.



Important:

You cannot add agent, queue, or routing point resources from the reporting groups you create to any of the agent, queue, or routing point groups in the All Resources view. Consider the agent, queue, and routing point resources under the All Resources view as a read-only resource. You cannot add these types of resources to the All Resources view.

When adding resources from the All Resources view, use the path **Enterprise > Resources > All Resources > ResourceName**, where **ResourceName** can be any of the following resources:

- Application Operations
- Reporting
- Roles
- User Management
- One or more Communication Manager systems
- One or more Proactive Contact systems

When adding resources from any groups you have created, use the path **Enterprise > Resources > ViewName > CategoryName > GroupName**.

Adding resources to groups



Tip:

Avaya recommends that you create all your categories and groups before you add any resources to the groups. By inspecting your view, category, and group setup, you can verify that you have created the proper reporting structure for your operation. If you change your reporting structure after you have added resources, you may have to add your resources again.

To add resources to groups:

1. Under the **Enterprise** tab, select **Expand All**.
2. Select a group under the expanded view.
3. Select **Add**.

The Add Resources dialog is displayed.

4. Under the **Resource Selector** pane, select a group from which you want to select a resource.

The Resource Selector pane redisplayes showing the resources assigned to that group.

5. Select the resources you want to add to the group. If there is more than one page of resources, you can either step through each page to select the resources you want to add to the group or you can use the search function to find a particular resource.
6. Select **Allow Duplicates** if you want to add the resources that are already added to other groups under same view.
7. After you have selected the resources you want to add to the group, select **OK**.

The resources added to the group are displayed.

Removing resources from groups

To remove resources from groups:

1. Under the **Enterprise** tab, select **Expand All**.
2. Select a group under the expanded view.
3. Select the resources you want to remove from the group.
4. Select **Remove**.

A confirmation message is displayed.

5. Select **OK**.

The remaining resources added to the group are displayed.

Copying groups to a different category

To copy a group:

1. Under the **Enterprise** tab, select **Expand All**.
2. Select the category that contains the group you want to copy.
3. In the Resource View, highlight the group you want to copy. Do not double-click the group.
4. Select **Copy**.

The **Select Destination for Copy** dialog is displayed.

5. Change the name and description if needed.
6. Under the **Select Destination For Copy** pane, expand the resource tree until the desired category is displayed.
7. Select the category where you want to copy the group.
8. Select **Allow Duplicates**.
9. Select **OK**.

The group is copied to the category.

Moving groups to a different category

To move a group:

1. Under the **Enterprise** tab, select **Expand All**.
2. Select the category that contains the group you want to move.

3. In the Resource View, highlight the group you want to move. Do not double-click the group.
4. Select **Move**.
The **Move to New Location** dialog is displayed.
5. Under the **Select Destination For Move** pane, expand the resource tree until the desired category is displayed.
6. Select the category where you want to move the group.
7. Select **Allow Duplicates**.
8. Select **OK**.

The group is moved to the category.

Copying categories to a different view

To copy a category:

1. Under the **Enterprise** tab, select **Expand All**.
2. Select the view that contains the category you want to copy.
3. In the Resource View, highlight the category you want to copy. Do not double-click the category.
4. Select **Copy**.
The **Select Destination for Copy** dialog is displayed.
5. Change the name and description if needed.
6. Under the **Select Destination For Copy** pane, expand the resource tree until the desired view is displayed.
7. Select the view where you want to copy the category.
8. Select **Allow Duplicates**.
9. Select **OK**.

The category is copied to the view.

Moving categories to a different view

To move a category:

1. Under the **Enterprise** tab, select **Expand All**.
2. Select the view that contains the category you want to move.

3. In the Resource View, highlight the category you want to move. Do not double-click the category.
4. Select **Move**.
The **Move to New Location** dialog is displayed.
5. Under the **Select Destination For Move** pane, expand the resource tree until the desired view is displayed.
6. Select the view where you want to move the category.
7. Select **Allow Duplicates**.
8. Select **OK**.

The category is moved to the view.

Removing groups

When you remove a reporting group, the group is removed from any future administration, but the group remains in the database so that you can still report on the historical data associated with the group.

To remove a group:

1. Under the **Enterprise** tab, select **Expand All**.
2. Select the category that contains the group you want to remove.
3. In the Resource View, highlight the group you want to remove. Do not double-click the group.
4. Select **Delete**.

A confirmation message is displayed.

5. Select **OK**.

The group is removed from the category.

Removing categories



CAUTION:

Removing a category removes all groups under the category. If any of the groups are still valid for another category, move those groups before you remove the category.

To remove a category:

1. Under the **Enterprise** tab, select **Expand All**.

2. Select the view that contains the category you want to remove.
3. In the Resource View, highlight the category you want to remove. Do not double-click the category.
4. Select **Delete**.
A confirmation message is displayed.
5. Select **OK**.
The category is removed from the view.

Administering users

Report and administration users can be added to an Avaya IQ system in two ways:

Integrating with an enterprise directory: Avaya IQ supports integration with an enterprise directory. When your system was originally installed by Avaya or your BusinessPartner, you were given the option to integrate a Windows Active Directory service with Avaya IQ. If all of your users are from your enterprise directory, you do not have to administer users manually. None of the procedures shown in this section can be applied to users integrated from an enterprise directory.

Adding users manually with Avaya IQ user management: If you cannot integrate with an enterprise directory service, you must manually add users to the Common User Service with the procedures described in this section.

This section includes the following topics:

- [User administration options](#) on page 34
- [Adding users](#) on page 35
- [Listing users](#) on page 36
- [Searching for users](#) on page 36
- [Editing user options](#) on page 37
- [Cleaning up user accounts before deleting users](#) on page 37
- [Deleting users](#) on page 37

User administration options

User ID (required): This is the login ID for the user. Once a user ID has been added, it cannot be changed. You must delete the user ID and add a new user ID.

Common Name (required): This is the first name of the user.

Surname (required): This is the last name of the user.

User Password (required): This is the password assigned to a user that is created using the Avaya IQ user management process.

Note:

Once you have assigned an initial password, you can force users to change their password on first login if you enable the **Initial Password Change** option as described in [Administering login session properties](#) on page 95. Instruct users to follow the same suggested password criteria.

When a user is created using the Avaya IQ user management process, the system does not enforce any password rules. Even though password rules are not enforced by Avaya IQ, Avaya recommends that you create a password that meets the following criteria:

- Passwords should be 8 to 14 characters long.
- Passwords should include a mix of the following character types:
 - Lower case letters
 - Upper case letters
 - Numerals
 - Other keyboard symbol punctuation marks and non-alpha characters
- Do not use the person's last name, first name, or any other personal information.

Confirm Password (required): This is a confirmation of the user password.

Avaya Role (required): Use the default of **userservice.useradmin** for all users.

All other fields: Populate any other fields as needed.

Adding users

To add users:

1. Under the **Tasks** tab, select **User Management > Administer Users > Create User**.
2. Administer the user attributes as described in [User administration options](#) on page 34.
3. Select **Apply**.
4. After adding all users, under the **Enterprise** tab, select **Resources > All Resources > User Management > Enterprise Users**.
5. Verify that all users are displayed. If the users are not displayed, select **Refresh**.



Important:

Any users shown here from integration with an enterprise directory are display only. You cannot make any changes to users here and have the changes sent to the enterprise directory.

6. Add the user to a role. See [Editing a role to add users](#) on page 51 for more information.

Listing users

To list all of the administered users:

1. Under the **Tasks** tab, select **User Management > Administer Users > List All Users**.
2. After the search results are displayed, you can select one of the users and do the following tasks:
 - Select **Edit** to change the user attributes as described in [User administration options](#) on page 34.
 - Select **Delete** to delete a user. After the Confirm Action screen is displayed, select **Delete User** to delete the user or **Cancel** to cancel your action.
 - Select **Details** to display the attributes for the user. After the details are displayed, you can do the following tasks:
 - Select **Edit** to change the user attributes as described in [User administration options](#) on page 34.
 - Select **Delete** to delete a user. After the Confirm Action screen is displayed, select **Delete User** to delete the user or **Cancel** to cancel your action.

Searching for users

To search for a particular user:

1. Under the **Tasks** tab, select **User Management > Administer Users > Search users**.
2. Select a **Search Attribute** and enter a **Search Value**.
3. Select **Search** to start the search.

Note:

The search function will not match on partial user IDs, common names, or surnames unless you add an asterisk (*) before or after the partial string.

4. After the search results are displayed, you can do the following tasks:
 - Select **Edit** to change the user attributes as described in [User administration options](#) on page 34.

- Select **Delete** to delete a user. After the Confirm Action screen is displayed, select **Delete User** to delete the user or **Cancel** to cancel your action.
- Select **Details** to display the attributes for the user. After the details are displayed, you can do the following tasks:
 - Select **Edit** to change the user attributes as described in [User administration options](#) on page 34.
 - Select **Delete** to delete a user. After the Confirm Action screen is displayed, select **Delete User** to delete the user or **Cancel** to cancel your action.

Editing user options

Once users have been added, you might want to change attributes for the user, including the user password.

To change user attributes:

1. Under the **Tasks** tab, select **User Management > Administer Users > List All Users**.
2. Highlight one of the displayed users.
3. Select **Edit** to make changes to the user.
4. Administer the user attributes as described in [User administration options](#) on page 34.
5. Select **Apply**.
6. In the confirmation dialog, select **Apply Changes** or **Cancel**.

Cleaning up user accounts before deleting users

Follow the procedures in [Cleaning up user accounts](#) on page 146 before you delete any users.

Deleting users

To delete a user:

1. Under the **Tasks** tab, select **User Management > Administer Users > List All Users**.
2. Select one of the users.
3. Select **Delete** to delete a user.
4. After the Confirm Action screen is displayed, select **Delete User** to delete the user or **Cancel** to cancel your action.

About user roles

User roles provide the following capabilities:

- Control access to reporting and administration operations and data
- Ability to assign the same set of permissions to one or more users that perform similar tasks

This section includes the following topics:

- [Role definitions](#) on page 38
- [About application operations](#) on page 39
- [About data access permissions](#) on page 42
- [Default roles](#) on page 44
- [Planning your roles](#) on page 47

Role definitions

With role definitions you define the operations assigned to a role, the users that are assigned to roles, and what data can be accessed when using a role. Ultimately, you are controlling how your users gain access to operations and data. The following components make up role definitions:

Operations: Operations are the tasks that users are allowed to perform and are the basis for the roles you will create. Since there are many operations, you will want to group similar operations into roles that make sense for your business. This will help simplify administration of users because you can assign users that do the same job to the same role. For example, most report users will need access to the same operations, so you can create a role that includes the most popular reporting operations. See [About application operations](#) on page 39 for a brief definition of each operation. [Planning your roles](#) on page 47 shows an example of how you might set up your role definitions for controlling access to operations.

Users: Users can be assigned to a single role or to multiple roles. When you assign two or more roles to a user, the user will gain the cumulative permissions of all of the assigned roles. If you delete a role, the permissions of that role will be removed from any users assigned to that role. See [Administering users](#) on page 34 and [Editing a role to add users](#) on page 51 for more information.

Data Access Permissions: Data access permissions define the data that users can view, add, edit, or delete. For example, if a user must analyze reports for a particular routing point, that user must have permission to view the routing point. If a supervisor must make skill changes for a set of agents, the supervisor must have edit permissions for those agents and view permissions to the queues. If you assign a role to have proper access permissions, anyone

assigned to that role will have those data access permissions. This allows you to assign similar permissions to a role and then apply that role to several users that do the same job with the same data access permissions. This will save you time because you will not have to assign permissions for every user. Only assign data access permissions to a role if all assigned users, or the large majority of the assigned users, have the save data access permissions. Otherwise, assign data access permissions to individual users. See [About data access permissions](#) on page 42 for more information about data access permissions.

About application operations

Application operations control access to reporting and administration tasks. For example, if a user needs to edit agent call handling and queue options, you must give the user access to the Administer Agent Call Handling and Queues operation. For more efficient management of operations, operations are assigned to roles, which is explained in the following sections:

- [About user roles](#) on page 38
- [Administering roles](#) on page 49
- [Editing a role to add operations](#) on page 50

An operation can consist of a single task, one or more tasks, related reports, or a reporting feature. The following sections list all the reporting and administration operations grouped in related categories:

- [Administrative tasks](#) on page 39
- [Maintenance tasks](#) on page 40
- [Reporting tasks](#) on page 41
- [Scheduling jobs](#) on page 42

Administrative tasks

Administer Agent Call Handling and Queues: This operation allows users to administer agent call handling preferences as described in [Agent call handling options](#) on page 87.

Administer Certificate Defaults: This operation allows users to set up defaults for trusted certificates as described in [Managing trusted certificates](#) on page 166.

Administer Connections: This operation allows users to configure connections to external data sources and databases as described in [Administering connection properties](#) on page 97.

Administer Login Session Properties: This operation allows users to set login session properties as described in [Administering login session properties](#) on page 95.

Administer Multiple Agent Queue Assignments: This operation allows users to administer queue assignments one queue at a time for one or more agents as described in [Administering multiple agent queue assignments](#) on page 83.

Administer Reporting Behaviors: This operation allows users to administer behavior definitions for reports as described in [Administering reporting behaviors](#) on page 67.

Administer Reporting Strings: This operation allows users to administer text strings used in reports as described in [About reporting names management](#) on page 74.

Administer Reporting Thresholds: This operation allows users to administer threshold definitions used in reports as described in [Administering threshold definitions](#) on page 61.

Administer Roles: This operation allows users to define roles as described in [About user roles](#) on page 38.

Administer Routing Point Options: This operation allows users to administer routing point options as described in [Administering routing point options](#) on page 92.

Administer Server Certificates: This operation allows users to administer trusted certificates as described in [Managing trusted certificates](#) on page 166.

Administer Service Levels: This operation allows users to administer service level definitions used in reports as described in [Administering service level targets](#) on page 72.

Administer Sites and Hosts: This operation allows users to administer sites and hosts as described in [About sites, hosts, and sources](#) on page 67 in *Avaya IQ Implementation*.

Administer Users: This operation allows users to manage enterprise users that have access to reports or administration as described in [Administering users](#) on page 34.

Manage Administrative Data: This operation allows users to perform several administrative tasks associated with the user service. These tasks are described in [Changing passwords](#) on page 18, [Reinitializing user service](#) on page 166, [Editing the service configuration](#) on page 166, and [Managing distributors](#) on page 166.

Synchronize JKS: This operation allows users to synchronize the Java Key Store (JKS) as described in [Managing trusted certificates](#) on page 166.

Unlock User Accounts: This operation allows users to unlock user accounts that have been disabled from failed login attempts as described in [Unlocking user accounts](#) on page 59.

View Pending Certificate Requests: This operation allows users view pending certificate requests as described in [Managing trusted certificates](#) on page 166.

Maintenance tasks

All of these tasks are described in *Avaya IQ Alarms and Logs*.

Administer Log and Alarm Options: This operation allows users to set alarm and log retention periods.

Run Alarm Manager: This operation allows users to access the alarm manager and run alarm reports.

Run Log Viewer: This operation allows users to access the log viewer and run log reports.

Run Ping Test: This operation allows users to send a ping test message to another host to confirm network connectivity.

Reporting tasks

Administer Scheduled Reports: This operation allows users to schedule reports as described in *Avaya IQ Standard Reports*.

Export Data: This operation allows users to see the Data Export reports and Data Export templates folders, and give users access to the contents in the Data Export Templates folder. Data Export is described in *Avaya IQ Data Export*.

Log In to Reporting Interface: This operation allows users to access the Avaya IQ reporting interface as described in [Logging on](#) on page 13.

Run Custom Reports: This operation allows users to run custom reports as described in *Avaya IQ Report Designer*.

Run Data Export Reports: This operation allows users to run data export reports as described in *Avaya IQ Data Export*.

Run Data Monitoring Reports: This operation allows users to run data monitoring reports as described in *Avaya IQ Standard Reports*.

Run Report Designer: This operation allows users to run Report Designer as described in *Avaya IQ Report Designer*.

Run Standard Historical Reports: This operation allows users to run standard historical reports as described in *Avaya IQ Standard Reports*.

Run Standard Real-time Reports: This operation allows users to run standard real-time reports as described in *Avaya IQ Standard Reports*.

Use Data Export Templates: This operation allows users to use data export templates as described in *Avaya IQ Data Export*.

Write Custom Reports : This operation allows users to design custom reports as described in *Avaya IQ Report Designer*.

Write Data Export Reports: This operation allows users to design data export reports as described in *Avaya IQ Data Export*.

Scheduling jobs

Administer Scheduled Jobs: This operation allows users to add, change, delete, enable, and disable a new scheduled job. This operation is also required for users who need to schedule changes using the Agent Editor, Routing Point Editor, and Multiple Agent Queue Assignments Editor. This task is described in [Scheduling jobs](#) on page 105.

About data access permissions

Avaya IQ allows you to control access to data used by reporting and administration. This access is controlled by administering data access permissions at the role level and, if needed, at the user level. Any data access permissions that a user inherits by a role can be overwritten by the data access permissions to users. This section describes what data has data access permissions and the different levels of permissions. You must use these different levels of permissions to provide the desired level of access for your users.

To simplify management of data access permissions, data can be organized into the following hierarchy: Views, Categories, and Groups. Data access permissions control access to any data associated with these views, categories, and groups. For example, the system has the following default views:

- All Resources
- Functional
- Location
- Organizational
- User Defined

Under All Resources, the system also has defined default categories and groups for operations, sources (Communication Manager and Proactive Contact), reporting administration, roles, and users. You can set data access permissions at any level in the hierarchy. This is also true for all of the other views where you have administered reporting categories and groups.

For example, the following hierarchy of reporting groups can be defined:

Functional ([view](#))

Sales Department ([category](#))

Sales Agents ([group](#))

You can assign view, edit, delete, and add data access permissions to the Functional view and apply those permissions automatically to the Sales Department category and Sales Agents group. If you wish to limit access to the Sales Agents group, you can assign a different set of permissions at each level in the hierarchy. The administration of data access permissions is very flexible. You need to plan out exactly who needs access to what data before you administer data access permissions.

These data access permissions apply to any report, reporting task, or administration task that attempts to use the data. For example, for a report user to run a report on a group of agents, the report user must have view permissions for that group of agents. In another example, if a supervisor needs to administer call handling preferences for that same set of agents, the supervisor must have edit permissions on that group of agents.

You can assign the following permissions to roles and to users:

View: View permissions allow users to view data for resources. For example, you have a supervisor that needs to run reports on a group of agents but you do not want the supervisor to change any administration for those agents. You can give the supervisor view permission to the group of agents, but the supervisor would not have ability to add, edit, or delete anything associated with that group of agents.

Edit: Edit permissions allow users to view and edit parameters of existing resources, categories, or groups. For example, you have a supervisor who needs to change queue assignments for a group of agents. You can give the supervisor edit permission to the reporting group that includes those agents so that he or she can change queue assignments for the agents in the reporting group.

Note:

Supervisors only need view permissions on queues to make an agent assignment.

Add: Add permissions allow users to view, edit, and add new resources, categories, or groups. For example, you have a manager who needs to group queues to run some special reports. You can give the manager add permission to the reporting category so that he or she can add new queue reporting groups.

Delete: Delete permissions allow users to view, edit, add, and delete existing resources. For example, you have a manager who needs to rearrange reporting groups. You can give the manager delete permission to the reporting category so that he or she can delete reporting groups that are no longer needed. The manager can also remove agents from groups.

For user permissions, there are two additional options:

User Override: When administering permissions for a user, this option overrides any role permissions that are assigned to the user. For example, a user may have a role that gives them only view permissions to agents. With User Override, you can override the role permission assignment and also grant edit permissions to the user. The override option is valuable when you have a large group of users where the majority of the group only needs limited permissions, but one or two of the users in the group require additional permissions.

No Permissions: This option allows you to quickly remove all permissions for a user. This can be useful if there is a behavior issue with a user and you want to remove all of their access without removing their user ID.

Note:

Operations permission changes made to a user do not take effect until after the user logs out of the system and then back into the reporting or administration application. Data access permissions only require a refresh of the browser cache.

Default roles

Default roles have been defined for Avaya IQ to help you get started with administration. The Avaya provisioning team or your BusinessPartner will initially assign your system administrators to a role that can administer all features of Avaya IQ. These system administrators can then assign the default roles or define new roles for users on your system.

Default user roles are grouped into two main categories:

Enterprise: This category includes roles for all enterprise users on your system. These roles will also be used by BusinessPartners during implementation. These users were added when you integrated with an enterprise directory system or when you manually created or administered users. See more about assigning users in [Administering users](#) on page 34.

The enterprise users category has two default roles:

- System Administrator
- Installer

For this release of Avaya IQ, you should use only the System Administrator role. The Installer role is not used at this time.

Services: This category includes roles for login IDs used by Avaya services personnel who work on the initial implementation and provide ongoing support of your system. These roles are not displayed to the customer's enterprise users and cannot be edited by enterprise users.

The services users category has two default roles:

- Services Admin (sroot login ID)
- Services Tech (craft login ID)

The default roles have access to the following operations. See [About application operations](#) on page 39 for a brief definition of each operation.

Operation	Enterprise (Customer)		Services (Avaya)	
	System Administrator (avaya)	Installer	Services Admin (sroot)	Services Tech (craft)
Administer Server Certificates				
Administer Certificate Defaults	X		X	
View Pending Certificate Requests	X		X	
Connection Management				
Administer Connections	X		X	
Contact Center Preferences				
Administer Agent Call Handling and Queues	X		X	
Administer Routing Point Options	X		X	
RBAC				
Administer Roles	X		X	
Reporting				
Administer Reporting Behaviors	X		X	
Administer Reporting Strings	X		X	
Administer Reporting Thresholds	X		X	
Administer Scheduled Reports	X		X	
Administer Service Levels	X		X	
Export Data	X		X	
Log In to Reporting Interface	X		X	
Run Custom Reports	X		X	
Run Data Export Reports	X		X	
Run Data Monitoring Reports	X		X	
Run Report Designer	X		X	

Operation	Enterprise (Customer)		Services (Avaya)	
	System Administrator (avaya)	Installer	Services Admin (sroot)	Services Tech (craft)
Run Standard Historical Reports	X		X	
Run Standard Real-time Reports	X		X	
Unlock Report User Accounts	X		X	
Use Data Export Templates	X		X	
Write Custom Reports	X		X	
Write Data Export Reports	X		X	
Security				
Administer Server Certificates	X		X	
Synchronize JKS	X		X	
Subsystem				
Administer Sites and Hosts	X		X	
System Configuration				
Administer Log and Alarm Options	X	X	X	X
Manage Administrative Data	X		X	
System Maintenance				
Run Alarm Manager	X	X	X	X
Run Log Viewer	X		X	X
System Properties				
Administer Login Session Properties	X		X	X
User Management				
Administer Multiple Agent Queue Assignments	X		X	
Administer Users	X		X	
Unlock Administration User Accounts	X		X	

Operation	Enterprise (Customer)		Services (Avaya)	
	System Administrator (avaya)	Installer	Services Admin (sroot)	Services Tech (craft)
Utility				
Administer Scheduled Jobs	X		X	
Run Ping Test	X		X	

Planning your roles

With all of the operations you can assign to roles, you have great flexibility in how you create roles for your users. Based on the operations listed in [Default roles](#) on page 44, this section describes typical roles performed by contact center users, the operations required to fulfill these roles, and to which users you would assign the roles.

Operations Manager: The operations manager has overall responsibility for the operation of the contact center. They would need access to the following operations:

- Administer Agent Call Handling and Queues
- Administer Multiple Agent Queue Assignments
- Administer Routing Point Options
- Administer Reporting Behaviors
- Administer Reporting Strings (includes Agent Activity States, Agent Logout Reasons, and Keywords)
- Administer Reporting Thresholds
- Administer Scheduled Jobs
- Administer Service Levels

An operations manager would also need view and edit data access permissions to all reporting views and categories.

User Manager: Users that create and manage other users on the system would need access to the following operations:

- Administer Login Session Properties
- Administer Roles
- Administer Scheduled Jobs
- Administer Users

Managing resources

- Manage Administrative Data
- Unlock Administration User Accounts
- Unlock Report User Accounts

A user manager would also need view and edit data access permissions to operations, enterprise roles, and enterprise users.

Agent and Report Data Monitor: Users that monitor agent and report data would need access to the following operations:

- Log In to Reporting Interface
- Run Data Monitoring Reports

Agent Administrator: Users that administer agent work assignments need access to the following operations:

- Administer Agent Call Handling and Queues
- Administer Multiple Agent Queue Assignments
- Administer Scheduled Jobs

Basic Report User: Users that run basic reports would need access to the following operations:

- Log In to Reporting Interface
- Run Custom Reports
- Run Report Scheduler
- Run Standard Historical Reports
- Run Standard Real-time Reports

Report Designer: Users that create custom reports would need access to the following operations:

- Log In to Reporting Interface
- Run Report Designer
- Write Custom Reports

Data Export User: Users that export data for external applications need access to the following operations:

- Export Data
- Log In to Reporting Interface
- Run Data Export Reports
- Run Report Scheduler
- Use Data Export Templates

- Write Data Export Reports

Administering roles

Once you have determined the user roles you need on your system, you can add those roles to the Enterprise Roles group. The Services Roles group is designated for Avaya services personnel. You cannot add roles to the Services Roles group.

Creating a role includes the following procedures:

- [Adding a new role](#) on page 49
- [Editing general role options](#) on page 50
- [Editing a role to add operations](#) on page 50
- [Editing a role to add users](#) on page 51
- [Editing a role to assign data access permissions](#) on page 51

In addition to these tasks, you can also do the following procedures:

- [Displaying group membership of a role](#) on page 54
- [Displaying user role assignments](#) on page 55

Adding a new role

To add a new role:

1. Under the **Enterprise** tab, select **Resources > All Resources > Roles > Enterprise Roles**.
The Resource Management-Enterprise Roles dialog is displayed.
2. Select **New**.
The Create New Role dialog is displayed.
3. Enter a name and description for the role. The **Managed Resource Group** option defaults to Roles.
4. Select **OK**.

Editing general role options

To change the name and description of an existing role:

1. Under the **Enterprise** tab, select **Resources > All Resources > Roles > Enterprise Roles**.

The Resource Management dialog is displayed showing all existing roles.

2. Select the role you want to edit.
3. Select **Edit**.

The Resource Editor dialog is displayed for the selected role.

4. Select the **General** tab.
5. Change the name or description for the role.
6. Select **Apply**.

The **General** tab refreshes showing the new information.

7. When finished changing role information, select **Close** to leave role administration.

Editing a role to add operations

Operations control which administration and reporting tasks users can access. Before you add operations to roles, make sure that you understand each of the operations as shown in [Role definitions](#) on page 38, [Planning your roles](#) on page 47, and [About application operations](#) on page 39.

To add one or more operations to a role:

1. Under the **Enterprise** tab, select **Resources > All Resources > Roles > Enterprise Roles**.

The Resource Management dialog is displayed showing all existing roles.

2. Select the role you want to edit.
3. Select **Edit**.

The Resource Editor dialog is displayed for the selected role.

4. Select the **Operations** tab.

A list of operations is displayed, including those that are already assigned to the role and those available for assignment.

5. Do one of the following steps:

- If you want to assign a limited number of operations, select the operations from the **Available Operations** area. Continue with Step 6.

- If you want to assign all operations to a role, select **Assign All Operations**. Only users in a role that has **Assign All Operations** assigned can select this option. A confirmation message is displayed. Continue with Step 7.
6. Select the shuttle up arrow.
The selected operations are moved to the **Assigned Operations** area and are automatically added to the role.
 7. When finished adding operations to a role, select **Close** to leave role administration.

Editing a role to add users

To add one or more users to a role:

1. Under the **Enterprise** tab, select **Resources > All Resources > Roles > Enterprise Roles**.

The Resource Management dialog is displayed showing all existing roles.

2. Select the role you want to edit.
3. Select **Edit**.

The Resource Editor dialog is displayed for the selected role.

4. Select the **Users** tab.
5. Select **Add**.

The Resource Selector dialog is displayed.

6. Browse through the available resources to view the list the available enterprise users.
7. Select one or more users to add to this role.
8. Select **OK**.

The users assigned to the role are displayed in the **Users** tab.

9. When finished adding users to a role, select **Close** to leave role administration.

Editing a role to assign data access permissions

Before assigning data access permissions to a role, review the information about the different permission levels in [About data access permissions](#) on page 42.

Note:

No user can change permissions for the default System Administrator role. The System Administrator role is protected so that at least one user can access all resources to make changes for any resource. You can only change permissions for roles that you have created.

To set permissions for a role:

1. Under the **Enterprise** tab, select **Resources > All Resources > Roles > Enterprise Roles**.

The Resource Management dialog is displayed showing all existing roles.

2. Select the role you want to edit.
3. Select **Edit**.

The Resource Editor dialog is displayed for the selected role.

4. Select the **Permissions** tab.

The Access Permissions Assigned To Role dialog is displayed.

5. Select **Add**.

The **Folder** selection dialog is displayed.

6. Select the views to which you want to apply data permissions access. You may select more than one view.

7. Select **Add**.

The Folder selection dialog refreshes showing the views you did not select.

8. Select **Close**.

The Access Permissions Assigned To Role dialog refreshes showing the views that you selected.

9. From the displayed list, select the view to which you want to assign data access permissions.

The dialog refreshes showing the permissions you can assign to the view.

10. Select the permissions you want to assign to the view. Note the following interactions:
 - When you select **View**, only view is enabled.
 - When you select **Edit**, view and edit are enabled.
 - When you select **Add**, view, edit, and add are enabled.
 - When you select **Delete**, view, edit, add, and delete are enabled.

Note:

When you remove all permissions for a view, the view will disappear from the list of available views. This is true even when you do not use the remove button above the permissions table. To see the missing view, you will need to add the view back into the list using an **Add** operation. The children of the added view will also be restored.

11. At this point, you must set the **Populate Children** option:
 - If **Populate Children** is selected, the same permissions will be assigned to the view and all its children. Resource permissions are always set to the group level

permissions, so the **Populate Children** option is not relevant for groups. Avaya recommends that you use the **Populate Children** option.

- If **Populate Children** is not selected, only those children that have matching permissions as the view will receive the updated permissions for the selected view. For example, a role has view only permissions for the Location view and for its Munich category, and view and edit permissions for the Bangalore category. When applying view, edit and add permissions to the Location view, the role will have view, edit and add permissions for Location view and Munich category. The role will maintain view and edit permissions for Bangalore.

12. Select **Apply**.

The dialog refreshes showing the categories assigned to the view.

13. Depending on the option you selected, continue with one of the following:

- If you selected the **Populate Children** option, you are finished administering data access permissions to this view. Return to Step 9 and continue with the next view.
- If you did not select the **Populate Children** option, continue with Step 14.

14. Double-click the view for which you just applied data access permissions.

The dialog refreshes showing the categories assigned to the view for which you have permission to view.

15. Select the category to which you want to assign data access permissions. You have to add like categories if none are listed.

The dialog refreshes showing the permissions you can assign to the category.

16. Select the permissions you want to assign to the category. Note the following interactions:

- When you select **View**, only view is enabled.
- When you select **Edit**, view and edit are enabled.
- When you select **Add**, view, edit, and add are enabled.
- When you select **Delete**, view, edit, add, and delete are enabled.

Note:

When you remove all permissions for a category, the category will disappear from the list of available categories. This is true even when you do not use the remove button above the permissions table. To see the missing category, you will need to add the category back into the list using an **Add** operation. The children of the added category will also be restored.

17. At this point, you must set the **Populate Children** option:

- If **Populate Children** is selected, the same permissions will be assigned to the category and all its children. Resource permissions are always set to the group level permissions, so the **Populate Children** option is not relevant for groups. Avaya recommends that you use the **Populate Children** option.

- If **Populate Children** is not selected, only those children that have matching permissions as the category will receive the updated permissions for the selected view. For example, a role has view only permissions for the Sales category and for its Sales Queues group, and view and edit permissions for the Sales Routing Point group. When applying view, edit and add permissions to the Sales category, the role will have view, edit and add permissions for Sales category and Sales Queues group. The role will maintain view and edit permissions for the Sales Routing Point group.
18. Select **Apply**.

The dialog refreshes showing the groups assigned to the category.
 19. Depending on the option you selected, continue with one of the following:
 - If you selected the **Populate Children** option, you are finished administering data access permissions to this category. Return to Step 15 and continue with the next category.
 - If you did not select the **Populate Children** option, continue with Step 20.
 20. Double-click the category for which you just applied data access permissions.

The dialog refreshes showing the groups assigned to the category for which you have permission to view.
 21. Select the group to which you want to assign data access permissions. You have to add like views if none are listed.

The dialog refreshes showing the permissions you can assign to the group.
 22. Select the permissions you want to assign to the group. Note the following interactions:
 - When you select **View**, only view is enabled.
 - When you select **Edit**, view and edit are enabled.
 - When you select **Add**, view, edit, and add are enabled.
 - When you select **Delete**, view, edit, add, and delete are enabled.
 23. Repeat Steps 21 and 22 for each group.
 24. Select **Back** within the dialog twice to return to the view level. Repeat Steps 9 through 23 for the next view.
 25. When finished adding permissions to a role, select **Close** to leave role administration.

Displaying group membership of a role

To display the role groups to which a role is assigned:

1. Under the **Enterprise** tab, select **Resources > All Resources > Roles > Enterprise Roles**.

The Resource Management dialog is displayed showing all existing roles.

2. Select the role you want to edit.
3. Select **Edit**.

The Resource Editor dialog is displayed for the selected role.

4. Select the **Member of** tab.

The display shows the role groups to which the role is a member.

5. When finished displaying the membership, select **Close** to leave role administration.

Displaying user role assignments

This operation displays the following information about users assigned to a role:

- Users assigned to a role
- Users that have User Override permission for any role

To display role assignments:

1. Under the **Enterprise** tab, select **Resources > All Resources > Roles > Enterprise Roles**.

The Resource Management dialog is displayed showing all existing roles.

2. Select the role you want to edit.
3. Select **Edit**.

The Resource Editor dialog is displayed for the selected role.

4. Select the **Access** tab.

The display refreshes showing all of the roles that have been assigned data access permissions to the role being edited. The permissions assignment is displayed with the role. Only roles you have permissions to view are listed.

5. Select a role.

The **Display all users assigned to the selected role** option is the default selection. All of the enterprise users assigned to the role are displayed in the bottom table along with their data access permissions relevant to the role being edited.

6. Select **Display all users directly assigned access to the resource**.

Any users that have User Override permissions for any role are displayed.

7. When finished displaying user role information, select **Close** to leave role administration.

Administering permissions for a user

Before assigning permissions to a user, review the information about the different permission levels in [About data access permissions](#) on page 42.

To assign permissions to a user:

1. Under the **Enterprise** tab, select **Resources > All Resources > User Management > Enterprise Users**.

The Resource Management dialog is displayed showing all existing users.

2. Select the user you want to edit.
3. Select **Properties**.

The Resource View dialog is displayed for the selected user.

4. Select the **Permissions** tab.

The Access Permissions Assigned To User dialog is displayed.

5. Select **Add** in the **Resources** pane.

The **Folder** selection dialog is displayed.

6. Select the views to which you want to apply data access permissions. You may select more than one view.

7. Select **Add**.

The Folder selection dialog refreshes showing the views you did not select.

8. Select **Close**.

The Access Permissions Assigned To User dialog refreshes showing the views that you selected.

9. From the displayed list, select the view to which you want to assign data access permissions.

The dialog refreshes showing the permissions you can assign to the view.

10. Select the permissions you want to assign to the view. Note the following interactions:
 - When you select **View**, only view is enabled.
 - When you select **Edit**, view and edit are enabled.
 - When you select **Add**, view, edit, and add are enabled.
 - When you select **Delete**, view, edit, add, and delete are enabled.

Note:

When you remove all permissions for a view, the view will disappear from the list of available views. This is true even when you do not use the remove button above the permissions table. To see the missing view, you will need to add the view back into the list using an **Add** operation. The children of the added view will also be restored.

11. At this point, you must set the **Populate Children** option:
 - If **Populate Children** is selected, the same permissions will be assigned to the view and all its children. Resource permissions are always set to the group level permissions, so the **Populate Children** option is not relevant for groups. Avaya recommends that you use the **Populate Children** option.
 - If **Populate Children** is not selected, only those children that have matching permissions as the view will receive the updated permissions for the selected view. For example, a role has view only permissions for the Location view and for its Munich category, and view and edit permissions for the Bangalore category. When applying view, edit and add permissions to the Location view, the role will have view, edit and add permissions for Location view and Munich category. The role will maintain view and edit permissions for Bangalore.
12. Select **Apply**.
The dialog refreshes showing the categories assigned to the view.
13. Depending on the option you selected, continue with one of the following:
 - If you selected the **Populate Children** option, you are finished administering data access permissions to this view. Return to Step 9 and continue with the next view.
 - If you did not select the **Populate Children** option, continue with Step 14.
14. Double-click the view for which you just applied data access permissions.
The dialog refreshes showing the categories assigned to the view.
15. Select the category to which you want to assign data access permissions. You have to add like views if none are listed.
The dialog refreshes showing the permissions you can assign to the category.
16. Select the permissions you want to assign to the category. Note the following interactions:
 - When you select **View**, only view is enabled.
 - When you select **Edit**, view and edit are enabled.
 - When you select **Add**, view, edit, and add are enabled.
 - When you select **Delete**, view, edit, add, and delete are enabled.

Note:

When you remove all permissions for a category, the category will disappear from the list of available categories. This is true even when you do not use the remove button above the permissions table. To see the missing category, you will need to add the category back into the list using an **Add** operation. The children of the added category will also be restored.

17. At this point, you must set the **Populate Children** option:

- If **Populate Children** is selected, the same permissions will be assigned to the category and all its children. Resource permissions are always set to the group level permissions, so the **Populate Children** option is not relevant for groups. Avaya recommends that you use the **Populate Children** option.
- If **Populate Children** is not selected, only those children that have matching permissions as the category will receive the updated permissions for the selected view. For example, a role has view only permissions for the Sales category and for its Sales Queues group, and view and edit permissions for the Sales Routing Point group. When applying view, edit and add permissions to the Sales category, the role will have view, edit and add permissions for Sales category and Sales Queues group. The role will maintain view and edit permissions for the Sales Routing Point group.

18. Select **Apply**.

The dialog refreshes showing the groups assigned to the category.

19. Depending on the option you selected, continue with one of the following:

- If you selected the **Populate Children** option, you are finished administering data access permissions to this category. Return to Step 15 and continue with the next category.
- If you did not select the **Populate Children** option, continue with Step 20.

20. Double-click the category for which you just applied data access permissions.

The dialog refreshes showing the groups assigned to the category.

21. Select the group to which you want to assign data access permissions. You have to add like views if none are listed.

The dialog refreshes showing the permissions you can assign to the group.

22. Select the permissions you want to assign to the group. Note the following interactions:

- When you select **View**, only view is enabled.
- When you select **Edit**, view and edit are enabled.
- When you select **Add**, view, edit, and add are enabled.
- When you select **Delete**, view, edit, add, and delete are enabled.

23. Repeat Steps 21 and 22 for each group.

24. Select **Back** within the window twice to return to the view level. Repeat Steps 9 through 23 for the next view.

25. When finished adding permissions to a user, select **Close** to leave user administration.

Unlocking user accounts

User accounts are locked when a user fails to log in successfully after a configurable number of attempts. This can happen when accessing the administration interface or when accessing the reporting interface. The limit for maximum failed login attempts is described in [Administering login session properties](#) on page 95.

This section includes the following topics:

- [Unlocking an administration user account](#) on page 59
- [Unlocking a reporting user account](#) on page 59

Unlocking an administration user account

To unlock an administration user account:

1. Log in to the administration interface.
2. Under the **Tasks** tab, select **User Management > Administer Users > Unlock User Account**.

The Unlock User Account dialog is displayed.

3. Select the user accounts you want to unlock. You can unlock more than one user account at a time.
4. Select **Unlock Account**.

The selected accounts are unlocked.

Unlocking a reporting user account

To unlock a reporting user account:

1. Log in to the reporting interface.
2. In the Workspace window, select **Unlock Report User Account**.

The Unlock Report User Account dialog is displayed.

3. Select the user accounts you want to unlock. You can unlock more than one user account at a time.

Managing resources

4. Select **OK**.

The selected accounts are unlocked.

Managing reporting preferences

This section contains procedures related to managing preferences that are exposed when running reports.

This section includes the following topics:

- [Administering threshold definitions](#) on page 61
- [Administering reporting behaviors](#) on page 67
- [Administering service level targets](#) on page 72
- [About reporting names management](#) on page 74
- [Administering agent activity states](#) on page 75
- [Administering agent logout reason codes](#) on page 79
- [Administering reporting keywords](#) on page 81

Administering threshold definitions

The Avaya IQ measurement threshold feature gives report users quick visual cues about the significance of report data, such as changing conditions that might require some kind of response. Threshold definitions for various real-time and historical report measures are associated with one or more queues or routing points.

Threshold definitions associate the measure values displayed in reports with conditional format rules. The background color displayed in a report for a particular measure changes when a threshold definition is assigned to the measure and a report value matches a range of values that is not within the specified range of acceptable values.

For example, a threshold definition can be assigned to the **% Held Contacts** measure so that the background format displayed for values in a report table shows a progressively darker color as the proportion of contacts held by agents exceed the threshold ranges defined for that measure in association with the queue on which is being reported.

For information about these thresholds and threshold reports, see [Threshold definitions](#) on page 38 in *Avaya IQ Standard Reports*.

This section includes the following topics:

- [Threshold definition options](#) on page 62
- [Administering threshold definitions](#) on page 65

Threshold definition options

This section describes the threshold definition administration options.

Measure Type: Measures are grouped into four types:

- Historical
- Sliding Time Window
- Start of Day
- Status

Only certain measures apply to each measure type. See the definition for the **Measure** option.

Measure: All measures that support a threshold have an acceptable target range. This target range is shown in white when defining the threshold. Some measures also have a target value that can be defined within the target range.

Some measures use a bilateral threshold type where low values and high values represent bad conditions and the acceptable target range is somewhere in the middle. The low values are shown in dark blue and light blue and the high values are shown in pink and dark red.

Some measures use an ascending threshold type where the target range starts at zero and increases to some maximum value. The acceptable condition target range is shown in white and the ascending values for bad conditions are shown in pink and dark red.



Important:

After you create a definition, you cannot change the measure that is assigned to the definition.

You can administer definitions for the following threshold measures:

Category	Measure	Measure Type	Curve Type	Target Value
Queue	Average Initiate Duration	Historical	ascending	No
	Average Preview Duration	Historical	ascending	No
	Expected Wait	Status	bilateral	No
Routing Point	% Busies	Sliding Time Window Start of Day	ascending ascending	No
	% Cancels	Sliding Time Window Start of Day	ascending ascending	No

Category	Measure	Measure Type	Curve Type	Target Value
Queue and Routing Point	% Abandons	Historical Sliding Time Window Start of Day	bilateral bilateral bilateral	Yes
	% Conferences	Historical	ascending	No
	% Disconnects from On Hold	Historical	ascending	No
	% Held Contacts	Historical	ascending	No
	% in Service Level	Historical Sliding Time Window Start of Day	bilateral bilateral bilateral	Yes
	% Outflows	Sliding Time Window Start of Day	ascending ascending	No
	% Redirects	Historical	ascending	No
	% Rejects	Historical	ascending	No
	% Transfers	Historical	ascending	No
	Average Abandon Duration	Historical	bilateral	Yes
	Average Active Duration	Historical Sliding Time Window Start of Day	bilateral bilateral bilateral	Yes
	Average Duration to Accept	Sliding Time Window Start of Day	bilateral bilateral	Yes
	Average Hold Duration	Historical	ascending	No
	Average in Focus Hold Duration	Historical	ascending	No
	Average Wait Duration	Historical	bilateral	No
	Average Wrap-up Duration	Historical Sliding Time Window Start of Day	bilateral ascending bilateral	Yes
	Current Maximum Wait Duration	Status	bilateral	No

Category	Measure	Measure Type	Curve Type	Target Value
Behavior	% Long Contacts	Historical	ascending	No
	% Long Holds	Historical	ascending	No
	% Long Wrap-ups	Historical	ascending	No
	% Short Auxiliary State	Historical	ascending	No
	% Short Contacts	Historical	ascending	No
	% Short Wrap-ups	Historical	ascending	No
Other	% Occupancy	Sliding Time Window Start of Day	bilateral bilateral	Yes

Name: Create a distinctive name for the definition. This name is only used by administration to identify the threshold. After you create a definition, you cannot change the name that is assigned to the definition.

Description: Add a description for the definition that identifies the threshold measure and its application. Add any information that will help you manage the specification of the definition.

Resource Type: This option specifies whether the definition is for queues, routing points, or other (other is used when another specific dimension does not apply). Select the resource for which the definition should apply. The **Assign Threshold** option will further specify if you are defining:

- A default definition that will apply to all resources
- A default definition that applies to all queues or all routing points
- A specific definition that will apply to one or more routing points or queues

Thresholds: These options define an acceptable target range, ranges that are outside of your acceptable target range, and a target value if supported for the measure. Depending on the threshold being created, you will specify the bilateral threshold ranges or the ascending threshold ranges.

For a bilateral threshold, you must define four target ranges and a target value if supported for the measure. For example, if you are defining the percent in service level, you might set an acceptable range between 75% and 85%. Enter 75 and 85 in the middle two input fields and enter the target value in the **Target** field. You can then assign your lower or higher out of range values, for example, 65% and 95%. Reports using this threshold definition will show the following colors for data that falls within these ranges:

- Dark blue - 0% to 65%
- Light blue - 65% to 75%
- White - 75% to 85%

- Pink - 85% to 95%
- Dark red - 95% to 100%

For a threshold that uses an ascending threshold type, you must define two target ranges and a target value if supported for the measure. For example, if you are defining average hold duration, you might set an acceptable range of 0 to 60 seconds. No target value is required. Enter 1 minute (60 seconds) in the left input field and enter an upper value that is outside of the acceptable range, but still within reason for the measure. For average hold time, your high end might be 2 minutes. You would enter that value into the right input field. Reports using this threshold definition will show the following colors for data that falls within these ranges:

- White - 0 to 60 seconds
- Pink - 1 to 2 minutes
- Dark red - 2 minutes or more

Assign Threshold: Use this option to define the resources to which the definition will be applied. When creating a default definition, select all resources, all queues, or all routing points. When creating specific definitions, select one or more individual resources for the definition. To display the views, categories, and groups, click on each parent resource to display each child resource. If you select a view, category, or group, all resources under each level are automatically selected. You can then clear and select individual resources if needed.

Note:

When you remove a threshold assignment for a resource, that resource is also removed from all other instances of the resource, whether the user has permission to access all instances of the resource.

Administering threshold definitions

You can add, change, or delete threshold definitions. The change operation has certain conditions where you will need to delete resources assigned to the current definition and then add the resource into a new or existing definition. See these conditions explained in [Changing a threshold definition](#) on page 66.

Adding a threshold definitions

To add a definition:

1. Under the **Enterprise** tab, select **Resources > All Resources > Reporting > Reporting: Thresholds**.

The Resource Management - Thresholds dialog is displayed.

2. Select **New**.

The Threshold Editor is displayed.

3. Under the **Measures** pane, drill down to select the threshold you want to define. See [Threshold definition options](#) on page 62 for a list of the possible measures.
4. Select one of the measures.
The Threshold Editor dialog refreshes with additional options.
5. Assign the rest of the threshold options as described in [Threshold definition options](#) on page 62.
6. When finished assigning options, select **OK**.
A confirmation dialog is displayed.
7. Select **OK** to confirm the message.
The Resource Management - Thresholds dialog is displayed showing the new definition. If the new definition is not shown, select **Refresh** in the resource view. The definition will be displayed.

Changing a threshold definition

To change a threshold definition:

1. Under the **Enterprise** tab, select **Resources > All Resources > Reporting > Reporting: Thresholds**.
The Resource Management - Thresholds dialog is displayed listing the administered threshold definitions.
2. Select one of the existing definitions.
3. Select **Edit**.
The Threshold Editor is displayed showing the options administered for this definition.
4. Change the options as described in [Threshold definition options](#) on page 62.
5. When finished changing the options, select **OK**.
A confirmation dialog is displayed.
6. Select **OK** to confirm the message.

Deleting threshold definitions

To delete one or more existing definitions:

1. Under the **Enterprise** tab, select **Resources > All Resources > Reporting > Reporting: Thresholds**.
The Resource Management - Thresholds dialog is displayed listing the administered threshold definitions.
2. Select one or more of the existing definitions.

3. Select **Delete**.

A confirmation dialog is displayed.

4. Select **OK**.

The selected threshold definition is deleted and a confirmation dialog is displayed.

5. Select **OK** to confirm the message.

The Resource Management - Thresholds dialog is displayed to show that the definition has been deleted. If the definition is not removed, select **Refresh**. The definition should be removed.

Administering reporting behaviors

Avaya IQ provides standard historical reports that supervisors can use to obtain information about various types of agent behaviors. These agent behaviors focus on items that can have a significant impact on cost of service or customer satisfaction. You can administer definitions for the following behavior measures:

Long contact: A count of contacts whose connect duration was greater than the value defined for this measure. The connect duration measurement begins when the agent accepts the contact and ends when the contact disconnects at the agent. Measures can be defined for queues and routing points.

Long hold: A count of contacts that the agent held for a duration that exceeded the value defined for this measure. This measure considers hold time in which the agent focus remained on the held contact and hold time in which the agent focus changed to a different contact. Measures can be defined for queues and routing points.

Long wrap-up: A count of contact wrap-ups whose duration exceeded the value defined for this measure. Measures can be defined for queues and routing points.

Short abandons: A count of abandons whose duration was less than the value defined for this measure. Abandons is a count of contacts that disconnected while waiting for service in routing processes, waiting at the queue or alerting at the agent. This measure is attributed when the contact disconnects. Measures can be defined for queues and routing points.

Short auxiliary state: A count of the number of times the agent went into an Aux. state and remained in that state for a duration that was less than the value defined for this measure. This measure considers all Aux. states. Aux. state durations considered by this measure are attributed when the agent leaves the Aux. State.

An agent may go into wrap-up state or an Aux state briefly and repeatedly in an attempt to affect their position in an idle agent queue. Rapid transitions in and out of Aux states and rapid transitions in and out of wrap-up state when no contact exists are both considered by the Short Aux. measure.

Short contact: A count of contacts whose connect duration was less than the value defined for this measure. The connect duration measurement begins when the agent accepts the contact and ends when the contact disconnects at the agent. Measures can be defined for queues and routing points.

Short outflows: A count of outflows whose duration was less than the value defined for this measure. Outflows is a count of contacts that outflowed from the queue or routing point as a result of a routing process application. Measures can be defined for queues and routing points.

Short trunk seizure: A count of trunk seizures whose duration was less than the value defined for this measure.

Short wrap-up: A count of contact wrap-ups whose duration was less than the value defined for this measure. Measures can be defined for queues and routing points.

Note:

Short abandon and short outflows are valid measures, but are not included in standard reports. If you want reports that show these measures, you need to include them in custom reports. Short trunk seizure is a valid measure, but cannot be displayed in any reports, standard or custom. Avaya recommends that you do not create behavior definitions for short trunk seizure.

For information about these behaviors and behaviors reports, see [Behavior counts and definitions](#) on page 37 and [Agent behavior reports](#) on page 109 in *Avaya IQ Standard Reports*. From the reporting interface see **Workspace > Standard Historical Reports > Agent Behaviors**.

You only need to create behavior definitions for those behaviors on which you want to report. You can create default behavior definitions that apply to all resources or you can create behavior definitions that apply to one or more specific resources. The following example shows a default behavior definition and a specific behavior definition.

- For all queues and routing points, you want to know if any contacts are kept on hold for three minutes or longer. You create a default definition that matches these specifications.
- For the queues where you promise your best customer service, you want to know if any contacts are being kept on hold for more than one minute. You create a specific definition that matches these specifications.

This section includes the following topics:

- [Behavior definition options](#) on page 69
- [Administering behavior definitions](#) on page 70

Behavior definition options

This section describes the behavior definition administration options.

Measure Type: The only possible value for this option is **Behaviors**.

Measure: Select the measure for which you want to create a definition. You can administer time limits for the following behavior measures:

- Long contact
- Long hold
- Long wrap-up
- Short abandons
- Short auxiliary state
- Short contact
- Short outflows
- Short trunk seizure
- Short wrap-up



Important:

Short abandon and short outflows are valid measures, but are not included in standard reports. If you want reports that show these measures, you need to include them in custom reports. Short trunk seizure is a valid measure, but cannot be displayed in any reports, standard or custom.

Name: Create a distinctive name for the definition. Once assigned, you cannot change the name of a definition. You can delete a definition and add a new definition with a new name, but you cannot change the name of an existing definition.

Description: Add a description for the definition. Add any information that will help you manage the specification of the definition.

Resource Type: This option specifies whether the definition is for queues or routing points or both. Select the resource for which the definition should apply. The Short Auxiliary State measure applies to auxiliary states. All other measures apply to either queue or routing point resources.

Behaviors: This option assigns a time value for the behavior. Long behaviors define a measure that exceeds a certain time limit. Short behaviors define a measure that is less than a certain time limit.

Assign Behavior: Use this option to define the resources to which the definition will be applied. If you are creating a default definition, you cannot select a specific resource. The definition will apply to all applicable resources. If you are creating specific definitions, you can select one or more resources for the definition. You can apply a definition to views, categories, groups, or individual resources. To display the views, categories, and groups, click on each parent resource to display each child resource.



Important:

Once you assign a view, category, or a group to a behavior definition, any resources added to the view, category, or a group do not inherit the behavior definition. You must manually apply the definition to the new resource.

Administering behavior definitions

You can add, change, or delete behavior definitions.

To add a definition:

1. Under the **Enterprise** tab, select **Resources > All Resources > Reporting > Reporting: Behaviors**.

The Resource Management - Behaviors dialog is displayed.

2. Select **New**.

The Behavior Editor is displayed.

3. Under the **Measures** pane, expand **Behaviors**.

A list of behaviors is displayed.

4. Select one of the behaviors. See [Behavior definition options](#) on page 69 for a description of the behaviors.

The Behavior Editor dialog refreshes with additional options.

5. Assign the behavior options as described in [Behavior definition options](#) on page 69.

6. When finished assigning options, select **OK**.

A confirmation dialog is displayed.

7. Select **OK** to confirm the message.

The Resource Management - Behaviors dialog is displayed showing the new definition. If the new definition is not shown, select **Refresh**. The definition should be displayed.

To change an existing definition:

1. Under the **Enterprise** tab, select **Resources > All Resources > Reporting > Reporting: Behaviors**.

The Resource Management - Behaviors dialog is displayed listing the administered behavior definitions.

2. Select one of the existing definitions.
3. Select **Edit**.

The Behavior Editor is displayed showing the options administered for this definition.

4. Change the behavior options as described in [Behavior definition options](#) on page 69. When changing an existing definition, you cannot change the name or the measure.
5. When finished changing the editable options, select **OK**.
A confirmation dialog is displayed.
6. Select **OK** to confirm the message.

To delete one or more existing definitions:

1. Under the **Enterprise** tab, select **Resources > All Resources > Reporting > Reporting: Behaviors**.

The Resource Management - Behaviors dialog is displayed listing the administered behavior definitions.

2. Select one or more of the existing definitions.
3. Select **Delete**.

A confirmation dialog is displayed.

4. Select **OK**.
A second confirmation dialog is displayed.
5. Select **Delete** to confirm the message.

The selected behavior definition is deleted and a confirmation dialog is displayed.

6. Select **OK** to continue.

The Resource Management - Behaviors dialog is displayed to show that the definition has been deleted. If the definition is not removed, select **Refresh**. The definition should be removed.

Administering service level targets

A service level target is defined as the percentage of calls you want answered within a certain amount of time. For example, you may want to set a service level target specifying that 80 percent of all calls terminating at a routing point are answered within 30 seconds. Service level target definitions can be created and applied to individual routing points or groups of routing points.

This section includes the following topics:

- [Service level target options](#) on page 72
- [Administering service level target definitions](#) on page 73

Service level target options

This section describes the service level target administration options.

Measure: This is a display only option that defines this measure as Service Level.

Name: Create a distinctive name for the definition. Once assigned, you cannot change the name of a definition.

Description: Add a description for the definition. Add any information that will help you manage the specification of the definition.

Resource Type: This is a display only option that shows that the service level definitions only apply to routing points. Queue service levels are defined on the Communication Manager system and propagated to Avaya IQ.

Service Level: This option assigns the target service level. The target service level defines that a certain percentage of calls will be answered within a certain number of seconds. For example, you may want to set a service level target that 80 percent of all calls terminating at a routing point are answered within 30 seconds.

Assign Service Level: This option defines the resources to which the definition will be applied. If you are creating a default definition, you should select all routing points that are assigned to a Communication Manager system. If you are creating a specific definition, you can drill down into the available routing points and select one or more routing points for the definition. You can apply a definition to views, categories, groups, or individual resources.



Important:

Once you assign a view, category, or a group to a service level definition, any resources added to the view, category, or a group do not inherit the definition. You must manually apply the definition to the new resource.

Administering service level target definitions

You can add, change, or delete service level definitions.

To add a definition:

1. Under the **Enterprise** tab, select **Resources > All Resources > Reporting > Reporting: ServiceLevels**.

The Resource Management - Reporting: ServiceLevels dialog is displayed.

2. Select **New**.

The Service Level Editor is displayed.

3. Assign the service level target options as described in [Service level target options](#) on page 72.

4. When finished assigning options, select **OK**.

A confirmation dialog is displayed.

5. Select **OK** to confirm the message.

The Resource Management - Service Levels dialog is displayed showing the new definition. If the new definition is not shown, select **Refresh** in the resource view dialog. The definition will be displayed.

To change an existing definition:

1. Under the **Enterprise** tab, select **Resources > All Resources > Reporting > Reporting: ServiceLevels**.

The Resource Management - Reporting: ServiceLevels dialog is displayed listing the administered service level definitions.

2. Select one of the existing definitions.

3. Select **Edit**.

The Service Level Editor is displayed showing the options administered for this definition.

4. Change the behavior options as described in [Service level target options](#) on page 72. When changing an existing definition, you cannot change the name.

5. When finished changing the editable options, select **OK**.

A confirmation dialog is displayed.

6. Select **OK** to confirm the message.

To delete one or more existing definitions:

1. Under the **Enterprise** tab, select **Resources > All Resources > Reporting > Reporting: ServiceLevels**.

The Resource Management - Reporting: ServiceLevels dialog is displayed listing the administered behavior definitions.

2. Select one or more of the existing definitions.
3. Select **Delete**.

A confirmation dialog is displayed.

4. Select **Yes**.

A confirmation dialog is displayed.

5. Select **Delete** to confirm the message.

The selected behavior definition is deleted and a confirmation dialog is displayed.

6. Select **OK** to confirm the message.

The Resource Management - Service Levels dialog is displayed to show that the definition has been deleted. If the definition is not removed, select **Refresh**. The definition should be removed.

About reporting names management

Display names can be administered for the following entities:

Communication Manager resources: The following resource names are uploaded to the Avaya IQ system from the Communication Manager system. If an administrator changes these names on the Communication Manager system, those changes are automatically synchronized with the Avaya IQ system. You cannot change these names using Avaya IQ administration.

- Agents
- Queues (skills)
- Routing points (VDNs)

Reporting text strings: You can administer the following reporting text strings on Avaya IQ:

- Agent Activity States (see [Administering agent activity states](#) on page 75)
- Agent Logout Reasons (see [Administering agent logout reason codes](#) on page 79)
- Keywords (see [Administering reporting keywords](#) on page 81)

The Agent Activity States and Agent Logout Reasons represent agent states tracked by Communication Manager, but the strings are administered only on Avaya IQ and are not shared with the Communication Manager system. Keywords are static strings that can only be changed for Avaya IQ reports.

Resource names: You can administer the following resource names:

- Sources, such as Communication Manager and Proactive Contact systems (administered by Avaya or your BusinessPartner during implementation)
- Users (see [Administering users](#) on page 34)
- Roles (see [Administering roles](#) on page 49)
- Views, categories, and groups (see [Administering reporting groups](#) on page 26)

Administering agent activity states

Agent activity states track all possible states that an agent can encounter while handling a contact. All of the standard predefined agent states are automatically tracked and recorded by the Communication Manager software, and that information is sent to Avaya IQ for reports. In addition to the standard predefined agent states, for which only the occupancy and language display options can be changed, you can create Auxiliary State definitions that will be tracked and reported.



Important:

The agent activity states editor allows you to create strings in thirteen different languages. For Avaya IQ Release 4.1, eight of the thirteen languages are supported, so any translated strings shown in any reports will only work for those eight languages. Support for all thirteen languages is targeted for future versions of Avaya IQ.

This section includes the following topics:

- [Agent activity state options](#) on page 76
- [Administering agent activity state definitions](#) on page 78

Agent activity state options

This section describes the agent activity state administration options.

Source Identifier: This option only applies when adding a new Auxiliary State definition. This option is display-only when editing an Auxiliary State definition or a predefined state definition. The Source Identifier must be an Auxiliary State number between 1 and 99, inclusive. (Auxiliary state 0 is predefined as Auxiliary - Default in Avaya IQ and cannot be assigned.) You should only administer the Auxiliary States that are actually being used on the source Communication Manager systems. The one set of Auxiliary State definitions (1 to 99) must be shared across all Communication Manager sources. You must coordinate the Auxiliary States on the Communication Manager sources so that the definitions are consistent across all Communication Manager systems or partitioned so that each Communication Manager system uses separate groups of Auxiliary States. For example, Auxiliary States 1 through 10 could be used for one Communication Manager system, 11 through 20 on another Communication Manager system, and so on.

Name: Create a distinctive name for the definition that matches the Auxiliary State being added. You cannot change the name of a predefined state. You can change the name of a custom Auxiliary State, which should only be done if you are changing the meaning associated with the Auxiliary State code. For example, if the purpose for code 33 changes from lunch break to team meeting, you should change the name to match the Auxiliary State purpose.

Description: Administer a description for the definition that identifies the state and its application. Add any information that will help you manage the specification of the definition. You cannot change the description of a predefined state. You can change the description of a custom Auxiliary State, which should only be done if you are changing the meaning associated with the Auxiliary State code. For example, if the purpose for code 33 changes from lunch break to team meeting, you should change the description to match the Auxiliary State purpose.



Important:

If you redefine an existing Auxiliary State definition, remember to change any language definitions to match the new state definition.

Occupancy: This option determines if you want the activity state included in occupancy calculations for reports. Occupancy calculations are explained in [Occupancy classifications](#) on page 35 in *Avaya IQ Standard Reports*. The manner in which agent activity states are considered in occupancy calculations is determined by the following administered settings:

- **Occupied** - If you want time that agents spend while in this state to be considered legitimate occupied time for occupancy calculations, select this option.
- **Not occupied** - If you want time that agents spend while in this state to be considered legitimate unoccupied time for occupancy calculations, select this option.
- **Not applicable** - If you do not want time that agents spend while in this state to be considered for any kind of occupancy calculations, select this option.

Note:

All auxiliary state definitions default to **Not applicable**.

An occupied state is considered to be a "working" state, where the not occupied or not applicable states are considered to be "non-working" states.

The following table shows the default occupancy settings for the predefined agent activity states:

Agent activity state	Default occupancy setting
Active	Occupied
Alert	Occupied
Auxiliary - Default	Not applicable
Auxiliary - Login	Not applicable
Auxiliary - System Forced	Not applicable
Hold	Occupied
Idle	Not occupied
Initiate	Occupied
Initiate or Alert	Occupied
In Preview	Occupied
In Wrap-up	Occupied
In Wrap-up No Contact	Not applicable
Logged out	Not applicable
Login	Not applicable
On Hold	Occupied
Unknown	Not applicable

Language Display: These options are available only when you are editing an existing agent activity state. You can administer the following language display options:

- **Name** - This is the actual text that will be displayed on reports for the selected agent activity state. When assigning this string, you can assign a different string for every language, assign the same string to all languages, or assign any combination of the two.
- **Description** - This is a description of the agent activity state language string. This string should be in the same language used for the **Name** option.

Administering agent activity state definitions

You can add or change auxiliary states. You cannot delete predefined or custom Auxiliary States.



Important:

After administering names for Aux. code definitions, the names for the Aux. codes may not be seen in report outputs for up to 30 minutes. This delay occurs because the database materialized views must be updated first before the changes can be seen in reports, and the update only occurs every 30 minutes. Based on this 30 minute update, the most you should have to wait to see the changes in reports is 30 minutes, but it could happen in less than 30 minutes depending on the timing. One exception to this condition is that messages from administration might be delayed if synchronization (pump-up) is currently running. In this exception, it might take as long as the pump-up time plus 30 minutes.

To add an Auxiliary State definition:

1. Under the **Enterprise** tab, select **Resources > All Resources > Reporting > Reporting: AgentActivityStates**.

The Resource Management - Reporting: AgentActivityStates dialog is displayed.

2. Select **New**.

The New Agent Activity State dialog is displayed.

3. Assign the options as described in [Agent activity state options](#) on page 76.

4. When finished assigning options, select **OK**.

The Resource Management - Reporting: AgentActivityStates dialog is displayed showing the new state. If the new state is not shown, select **Refresh**. The definition will be displayed based on sorting order.

To change an existing agent activity state definition:

1. Under the **Enterprise** tab, select **Resources > All Resources > Reporting > Reporting: AgentActivityStates**.

The Resource Management - Reporting: AgentActivityStates dialog is displayed.

2. Select one of the existing definitions.

3. Select **Edit**.

The Edit Agent Activity State dialog is displayed showing the options administered for the selected definition.

4. Change the options as described in [Agent activity state options](#) on page 76. You cannot change the name or description for predefined agent activity state definitions. You can change the name and description for an Auxiliary State definition.

5. When finished changing the editable options, select **OK** or **Apply**.

If you selected **OK**, the Resource Management - Reporting: AgentActivityStates dialog is displayed. If you selected **Apply**, the Edit Agent Activity State dialog remains open so you can make other changes to the definition.

Administering agent logout reason codes

Agent logout reason codes is a feature of the Contact Center software of Communication Manager. These codes are used to identify the reasons why an agent has logged out of the Contact Center system. The logout reason codes help you keep track of agent activity.

There are nine numbered agent logout reason codes, a default agent logout reason code when the agent doesn't enter a code, plus logout reason codes for Abnormal Logout, Implied Logout, and None. With Avaya IQ, you can create a text definition for each of the logout reasons. For consistency, the same definitions must be used by all agents across all of your Communication Manager systems.

The None logout reason code is used when Avaya IQ receives a logout message that contains no understood reason. This would probably not happen for a logout reason code coming from a Communication Manager system, but it may happen with unknown reasons from other data sources.

Agent logout reason codes also support localized display names for all supported languages. Logout reason codes 1 through 9 use the numbers as the default values. The Abnormal Logout, Implied Logout, Logout Default, and None strings are already localized for the supported languages. You can create localized display names for all of the logout reason codes.

Important:

The agent activity states editor allows you to create display names in 13 different languages. For Avaya IQ Release 4.1, English is the only supported language, so any translated display names will not be shown in any reports. Support for all 13 languages is targeted for future versions of Avaya IQ.

This section includes the following topics:

- [Agent logout reasons options](#) on page 79
- [Administering agent logout reasons](#) on page 80

Agent logout reasons options

This section describes the agent logout reasons administration options.

Name: When editing a predefined state, you cannot change the name.

Description: When editing a predefined state, you cannot change the description.

Language Display Name: These options are available only when you are editing an existing agent logout reason. You can administer the following language display options:

- **Language** - These are the languages for which you can assign a display name. You can select one or more languages at one time to assign the same display name to several languages.
- **Language Display Name** - This is the actual text that will be displayed on reports for the select agent logout reason. When assigning this string, you can assign a different string for every language, assign the same string to all languages, or assign any combination that works for your report users.
- **Language Display Description** - This is a description of the agent logout reason language display name. This defines the display name in the different languages.

Administering agent logout reasons

You can change existing agent logout reasons. You cannot add new agent logout reasons or delete predefined logout reasons. Change the options as described in [Agent logout reasons options](#) on page 79.

To change an existing agent logout reason definition:

1. Under the **Enterprise** tab, select **Resources > All Resources > Reporting > Reporting: AgentLogoutReasons**.

The Resource Management - Reporting: AgentLogoutReasons dialog is displayed.

2. Select one of the existing definitions.
3. Select **Edit**.

The Edit Agent Logout Reasons dialog is displayed showing the options administered for the selected definition.

4. In the Language Display Name pane:
 - a. Select one or more languages.
 - b. Assign a language display name.
 - c. Add a description for the language display name.
5. When finished changing the editable options, select **OK** or **Apply**.

If you selected **OK**, the Resource Management - Reporting: AgentLogoutReasons dialog is displayed. If you selected **Apply**, the Edit Agent Logout Reasons dialog remains open so you can make other changes to the definition. After you make all changes to a logout reason, select **OK**.

Administering reporting keywords

Avaya IQ uses a fixed set of keywords that are displayed on reports. Through administration, you can change the display name of these keywords for all supported languages. For example, you can change the **Yes** and **No** indicators shown on reports to **Y** and **N**.

**Important:**

The keywords editor allows you to create display names in 13 different languages. For Avaya IQ Release 4.1, English is the only supported language, so any translated display names will not be shown in any reports. Support for all 13 languages is targeted for future versions of Avaya IQ.

This section includes the following topics:

- [Keywords options](#) on page 81
- [Administering keywords](#) on page 82

Keywords options

This section describes the reporting keywords administration options.

Keyword Definition: You can administer the following keyword options:

- **Group Members** - This is a display-only number of the available keywords associated with the selected group of keywords.
- **Display Name** - These are the display names for each keyword within the selected group of keywords, based on the operating system language of the administration server. You can only select one keyword at a time.
- **Description** - This is a display-only description of the selected keyword.

Language Display Name: You can administer the following language display options:

- **Language** - These are the languages for which you can assign a display name. You can select one or more languages at one time to assign the same display name to several languages.
- **Language Display Name** - This is the actual text that will be displayed on reports for the selected keyword. When assigning this string, you can assign a different string for every language, assign the same string to all languages, or assign any combination that works for your report users.
- **Language Display Description** - This is a description of the keyword in the selected language or languages. This field is blank when selecting more than one language, allowing you to update the description for all the selected languages.

Administering keywords

You can change existing keywords. You cannot add new keywords or delete predefined keywords. Administer the options as described in [Keywords options](#) on page 81.

To change an existing keyword:

1. Under the **Enterprise** tab, select **Resources > All Resources > Reporting > Reporting: Keywords**.

The Resource Management - Reporting: Keywords dialog is displayed.

2. Select one of the existing group of keyword definitions.
3. Select **Edit**.

The Edit Keywords dialog is displayed showing the options administered for the selected group of keywords.

4. In the Keyword Definition pane, select one of the listed keywords.
5. In the Language Display Name pane:
 - a. Select one or more languages.
 - b. Assign a language display name.
 - c. Add a description for the language display name.

6. When finished changing the editable options, select **OK** or **Apply**.

If you selected **OK**, the Resource Management - Reporting: Keywords dialog is displayed. If you selected **Apply**, the Edit Keywords dialog remains open so you can make other changes to the language display names and descriptions of the selected keyword. You can also continue working on other keywords within the selected group of keywords. After you finish making changes to the keywords within the group of keywords, select **OK**.

Managing contact center preferences

This section contains procedures related to administering agent and routing point preferences that affect contact center operation.

This section includes the following topics:

- [Administering multiple agent queue assignments](#) on page 83
- [Administering agent call handling options](#) on page 87
- [Administering routing point options](#) on page 92

Administering multiple agent queue assignments

When agents are first administered on a Communication Manager system, the agents are assigned to queues (skills), and those queues are assigned either a skill level or a reserve level. (Reserve levels are also known as overload level in Avaya Business Advocate.)

As contact center traffic changes during the business day, you might need to change agent queue assignments to accommodate your traffic. Using Avaya IQ administration, you can add, change, or remove queue assignments for agents and you can assign a skill level or reserve level to the queue. These changes made from Avaya IQ are synchronized with the associated Communication Manager system.

This section includes the following topics:

- [Multiple agent queue assignment options](#) on page 83
- [Adding multiple agent queue assignments](#) on page 84
- [Changing multiple agent queue assignments](#) on page 85
- [Removing multiple agent queue assignments](#) on page 86

Multiple agent queue assignment options

Use the following option definitions when assigning queues to agents:

Source: This option is a drop-down list that selects the available Communication Manager systems. When you first open the dialog, the first system is displayed.

Available Agents: This option defines the agents to which you can assign queues. You can assign a queue to as many as 32 agents with one operation. The available agents are based on the system you select and the agents you have permission to edit. You cannot select agents that are identified as none, unidentified, or unmeasured.

You can use **Select All** to select all of your agents, but only if there are 32 or fewer agents that you have permission to edit on your system. If you have more than 32 agents, **Select All** is disabled.

The agent selections are retained when going from one operation to another. For example, if you add a queue to a set of agents, those same agents remain selected for the next operation in case you want to assign another queue to the same set of agents. If you go to a different task in the administration interface, the selection of agents are not retained.

Action Tabs: There are three tabs available to add, change, and remove queue and agent assignments. When you first open the dialog, the **Add** tab is selected.

Add Queue, From Queue, To Queue, Remove Queue: These options define the queues that you can add to agents, change for one or more agents, or remove from agents. The available queues are based on the system you select and the queues that you have permission to read. You must assign a minimum of one queue to each agent and a maximum of 60 queues to each agent, but you can only assign one queue at a time using this procedure. If you attempt to remove the last queue from an agent, the operation will fail. You cannot select queues that are identified as none or unmeasured.

Skill Level: This option defines the skill level or reserve level assigned to the queue. This option only applies when adding a new queue or when changing from an old queue to a new queue. This option is inactive for a remove operation. Skill levels have the following definitions:

- **1 (high) to 16 (low)**
- **Reserve Behind Target**, also known as Reserve Level 1 in Communication Manager and Overload 1 in Avaya Business Advocate. You can only assign this skill level if you are using Business Advocate.
- **Reserve Critical**, also known as Reserve Level 2 in Communication Manager and Overload 2 in Avaya Business Advocate. You can only assign this skill level if you are using Business Advocate.

Adding multiple agent queue assignments

To assign a queue to one or more agents:

1. Under the **Tasks** tab, select **User Management > Administer Multiple Agent Queue Assignments**.

The Multiple Agent Queue Assignment dialog is displayed.

2. Select a system from the **Source** list.

3. Select one or more agents from the Agents pane.
4. Select the **Add** tab.
5. Select one of the available queues from the Queue pane.
6. Select a skill level from the **Skill Level** list.
7. Select **OK** to submit the change immediately or select **Schedule...** to schedule the change for later. For information about scheduling an administrative change, see [Scheduling jobs](#) on page 105.

If you selected **OK** and there were changes, the Status dialog is displayed. This dialog lists all of the agents being changed and the current status of each request. You can sort on any of the columns in the display except the description. If you sort on the status icon, the four types of status are grouped and displayed in sorted order. The status types are **Request is pending**, **Request succeeded**, **Request failed**, and **Unknown**.

8. Select **Refresh** until the status dialog shows that all of the requests were successful. If after 15 seconds a request does not complete successfully, the request is marked unknown. You should resubmit all unknown or failed requests. Requests that report pending agent state change or logouts are successful, but the change will not occur until the agent changes state or logs out.



Important:

Once you close the status dialog, you cannot reopen the status dialog to recheck the status of your requests.

Changing multiple agent queue assignments

To remove one queue and add another queue to one or more agents:

1. Under the **Tasks** tab, select **User Management > Administer Multiple Agent Queue Assignments**.

The Multiple Agent Queue Assignment dialog is displayed.

2. Select a system from the **Source** list.
3. Select one or more agents from the Agents pane.
4. Select the **Change** tab.
5. Select one of the available queues in the From Queue pane that you want to change.
6. Select one of the available queues in the To Queue pane that you want to add. The queue you add here could be the same queue that you selected in the From Queue pane.
7. Select a skill level from the **Skill Level** list. You only have to change the skill level if the From Queue selection is the same as the To Queue selection.

8. Select **OK** to submit the change immediately or select **Schedule...** to schedule the change for later. For information about scheduling an administrative change, see [Scheduling jobs](#) on page 105.

If you selected **OK** and there were changes, the Status dialog is displayed. This dialog lists all of the agents being changed and the current status of each request. You can sort on any of the columns in the display except the description. If you sort on the status icon, the four types of status are grouped and displayed in sorted order. The status types are **Request is pending**, **Request succeeded**, **Request failed**, and **Unknown**.

9. Select **Refresh** until the status dialog shows that all of the requests were successful. If after 15 seconds a request does not complete successfully, the request is marked unknown. You should resubmit all unknown or failed requests. Requests that report pending agent state change or logouts are successful, but the change will not occur until the agent changes state or logs out.



Important:

Once you close the status dialog, you cannot reopen the status dialog to recheck the status of your requests.

Removing multiple agent queue assignments

To remove a queue from one or more agents:

1. Under the **Tasks** tab, select **User Management > Administer Multiple Agent Queue Assignments**.

The Multiple Agent Queue Assignment dialog is displayed.

2. Select a system from the **Source** list.
3. Select one or more agents from the Agents pane.
4. Select the **Remove** tab.
5. Select one of the available queues from the Queue pane.
6. Select **OK** to submit the change immediately or select **Schedule...** to schedule the change for later. For information about scheduling an administrative change, see [Scheduling jobs](#) on page 105.

If you selected **OK** and there were changes, the Status dialog is displayed. This dialog lists all of the agents being changed and the current status of each request. You can sort on any of the columns in the display except the description. If you sort on the status icon, the four types of status are grouped and displayed in sorted order. The status types are **Request is pending**, **Request succeeded**, **Request failed**, and **Unknown**.

7. Select **Refresh** until the status dialog shows that all of the requests were successful. If after 15 seconds a request does not complete successfully, the request is marked unknown. You should resubmit all unknown or failed requests. Requests that report pending agent state change or logouts are successful, but the change will not occur until the agent changes state or logs out.

**Important:**

Once you close the status dialog, you cannot reopen the status dialog to recheck the status of your requests.

Administering agent call handling options

When agents are first administered on a Communication Manager system, the agents are assigned to queues (skills), and those queues are assigned either a skill level or a reserve level. (Reserve levels are also known as overload level in Business Advocate terminology.) These call handling options determine how calls are delivered to agents. Using Avaya IQ administration, you can change these call handling assignments. These changes made from Avaya IQ are synchronized with the associated Communication Manager system.

This section includes the following topics:

- [Agent call handling options](#) on page 87
- [Changing agent call handling options](#) on page 90

Agent call handling options

This section describes the call handling options you can assign to agents. When agents are first administered on a Communication Manager system, the agents are assigned to queues (skills), and those queues are assigned either a skill level or a reserve level. (Reserve levels are also known as overload level in Business Advocate terminology.) These call handling options determine how calls are delivered to agents. Using Avaya IQ administration, you can change these assignments.

See the following topics for more information:

- [Call handling preferences \(General tab\)](#) on page 88
- [Queue assignments \(General tab\)](#) on page 88
- [Selected agents \(Additional Agents\)](#) on page 89

Once you understand the concept of agent call handling options, use the procedure in [Changing agent call handling options](#) on page 90 to apply these options.

Call handling preferences (General tab)

The following options on the **General** tab define how calls are delivered to agents:

Agent skill levels: This option controls call delivery based on the expertise of an agent in one or more queues. Skill level selects a call for an agent based first on highest skill level, then highest priority, and finally on Current Wait Time or Predicted Wait Time.

Percent allocation: This option allows you to assign a percentage of an agent's time to each of the agent's queues to total 100% of the agent's staffed time. Using this method, calls are selected according to the preassigned percentage allocation plan of the agent.

Queues with the greatest need: This option delivers calls based on the needs of the queues assigned to the agent.

Receive direct agent calls first: This option can be selected if **Percent Allocation** is active. This option will allow Direct Agent Calls to arrive at an agent before calls waiting in the queue.

Route calls to meet service objectives: This option can be selected if **Agent skill levels** or **Queues with the greatest need** are active. This option will allow calls to arrive at an agent to meet service objectives.

Queue assignments (General tab)

You can assign as many as 60 queues to an agent. These options are found on the **General** tab. Once you have selected the queues, you can set the following options for each of the queues:

Order of the queues: Queues can be placed in any order. Related queues can be grouped together to help you track the assigned queues. The order of the queues can also determine the Direct Agent Queue assignment if you do not select a specific queue. Since you manually define the order of the queues, you cannot sort on the list of assigned queues.

Skill Level: This option defines the skill level or reserve level assigned to the queue. Skill levels have the following definitions:

- **1** (high) to **16** (low)
- **Reserve Behind Target**, also known as Reserve Level 1 in Communication Manager and Overload 1 in Business Advocate. You can only assign this skill level if you are using Business Advocate.
- **Reserve Critical**, also known as Reserve Level 2 in Communication Manager and Overload 2 in Business Advocate. You can only assign this skill level if you are using Business Advocate.

When a skill changes to a new state, reserve agents are activated or deactivated. Going from normal skills 1 through 16 to Reserve Behind Target causes agents assigned to Reserve Behind Target to be activated (made available) for this skill. Going from Reserve Behind Target to Reserve Critical causes Reserve Critical agents to be made unavailable for this skill. These skill states indicate where the skill's expected wait time is in relation to its target.

Percent allocations: This option allows you to assign a percentage of an agent's time to each of that agent's queues to total 100% of the agent's staffed time. The totals in this column must add up to 100%.

Direct Agent Queue: This option assigns a queue that is used to deliver Direct Agent Calls to the agent. When a direct agent queue is assigned, Direct Agent Calls arrive at an agent before calls waiting in the queue. There are several interactions related to the direct agent queue:

- The direct agent queue cannot be defined as a Reserve Behind Target or Reserve Critical queue. If you change the skill level of the direct agent queue to Reserve Behind Target or Reserve Critical, the system automatically reassigns a queue as the direct agent queue. The queue that the system selects is the first queue in the list of assigned queues that is not a reserve queue. When this happens, a warning icon displays next to the **Direct Agent Queue** field. You can then reassign a different queue as the direct agent queue, or leave the queue assigned by the system.
- If you remove a queue that is assigned as the direct agent queue, the system automatically reassigns a queue as the direct agent queue. The queue that the system selects is the first queue in the list of assigned queues that is not a reserve queue. When this happens, a warning icon displays next to the **Direct Agent Queue** field. You can then reassign a different queue as the direct agent queue, or leave the queue assigned by the system.
- You can select an unmeasured queue as the direct agent queue. Since unmeasured queues do not have names, you must identify the queue by its skill ID shown in parentheses.
- You do not have to assign a direct agent queue. You can select a blank entry from the drop-down list of queues. The system may also blank out this field if there are no queues that are not reserve queues.

Selected agents (Additional Agents)

Once you have set the call handling preferences and the queue assignments, you can apply these options to as many as 50 agents at a time. These options are set on the **Additional Agents** tab. This would be the one agent you selected to start the agent editor, plus up to 49 more agents.

Changing agent call handling options

This section describes how you administer agent call handling options. To understand more about these options, see [Agent call handling options](#) on page 87.

This section includes the following topics:

- [Permissions required to administer agent call handling options](#) on page 90
- [Interactions with unmeasured queues](#) on page 90
- [Planning your call handling options](#) on page 91
- [Using the agent editor](#) on page 91

Permissions required to administer agent call handling options

To administer call handling options, the administrator must have the following permissions:

- To view and add or remove a queue from an agent, the administrator must have at least view permission on the queue. If the administrator does not have permission to view all of the queues assigned to an agent, the administrator cannot effectively administer the agent queues. Any queues that the administrator cannot view are handled the same as unmeasured queues, with the exception that they do have a name. The skill level and percent allocation are static and cannot be changed. The queue cannot be removed.
- If the administrator does not have add or change permission on a queue but does have view permission, the administrator can view the agent information. All input fields and most control buttons are disabled. After viewing the current administration values, the administrator can only cancel out of the dialog.

Interactions with unmeasured queues

Consider the following interactions when administering unmeasured queues:

- An administrator does not have permission to make changes to an unmeasured queue since it is not known to group permission controls. The skill level and percent allocation will be displayed as static text. Changes to unmeasured queues will have to be done on the Communication Manger system. Avaya recommends that all queues should be measured.
- An unmeasured queue does not have a name associated with the queue. The editor displays a blank in the name field.
- An unmeasured queue will not be displayed in the available or assigned queues lists in the Queue Assignments dialog. An administrator cannot add or remove an unmeasured queue to the list. An unmeasured queue does count towards the maximum of 60 queues you can assign to agents.
- An unmeasured queue can be moved up or down in the assigned queue list.

- You can select an unmeasured queue as the direct agent queue. Since unmeasured queues do not have names, you must identify the queue by its skill ID shown in parentheses, for example, (41).

Planning your call handling options

To make call handling changes, you must collect the following information:

- The agent or agents to whom you want to apply the changes.
- The call handling preferences for the queues. This includes skill level, percent allocation, and queues that have the greatest need. You can also assign a Direct Agent Calling queue and options to route calls to meet service objectives.
- The queues you want to assign to the agents. This includes the order of the queues, the skill level assigned to the queues, and the percent allocation for each queue.
- The Direct Agent Calling queue you want to assign, if any.
- Whether you want the change to be immediate or on a scheduled basis.

To learn more about these options, see [Agent call handling options](#) on page 87.

Using the agent editor

To set and assign queue options to one or more agents:

1. Under the **Enterprise** tab, select **Resources > All Resources > SourceName > SourceNameagents**, where **SourceName** is the Communication Manager system.
2. Select an agent from the list of available agents.
3. Select **Edit**.

The Edit Agent dialog is displayed.

4. On the **General** tab, set the call handling preferences as defined in [Call handling preferences \(General tab\)](#) on page 88.
5. Select **Add/Remove...**

The Queue Assignments dialog is displayed.

6. In the Queue Assignments dialog, select the queues you want to add to the agent. Select a queue group from the drop-down list of available queues. You can then search for specific queue members, if needed.

The queues you place in the Assigned Queues pane will be assigned to the agent. Use the shuttle controls to move the queues between the available and assigned panes. You can assign a maximum of 60 queues to an agent. Any unmeasured queues that do not show up in this dialog do count towards the maximum of 60 queues.

7. When finished selecting queues, select **OK**.

The Edit Agent dialog is displayed.

8. Administer the queue assignment options as defined in [Queue assignments \(General tab\)](#) on page 88. Use the **Move Up** and **Move Down** controls to change the order of the queues assigned to the agent. Select one or more queues to move up or down in the list.
9. Using the Additional Agents tab, select which additional agents will be assigned to the same call handling preferences and queues, including the Direct Agent Queue. Select an agent group from the drop-down list of available agent groups. You can then search for specific agents, if needed, and you can sort the agent name and ID columns to help you find specific agents. Use the shuttle controls to move the agents between the Available Agents pane and the Agents to Change pane. You can select a maximum of 49 additional agents.
10. Select **OK** to submit the change immediately or select **Schedule...** to schedule the change for later. For information about scheduling an administrative change, see [Scheduling jobs](#) on page 105.

If you selected **OK** and there were changes, the Agent Status dialog is displayed. This dialog lists all of the agents being changed and the current status of each request. You can sort on any of the columns in the display. If you sort on the status icon, the four types of status are grouped and displayed in sorted order. The status types are error, unknown, pending, and successful.

11. Select **Refresh** until the status dialog shows that all of the requests were successful. If after 15 seconds a request does not complete successfully, the request is marked unknown. You should resubmit all unknown or failed requests. Requests that report pending agent state change or logouts are successful, but the change will not occur until the agent changes state or logs out.



Important:

Once you close the status dialog, you cannot reopen the status dialog to recheck the status of your requests.

Administering routing point options

You can administer two routing point options:

Vector ID: This option assigns a vector to the routing point. You can assign any vector that is administered on the same source as the routing point. Vectors range from 1 to the maximum allowed on the source.

Queue Preferences: This option assigns queue preferences to the routing point. You can assign up to three queues that are administered on the same source as the routing point. You can only assign queues that you have permission to view. You can use queue preferences if you want to quickly give the same treatment to all callers using this routing point. This can be useful to send out-of-hours calls to a single queue that plays a recorded announcement giving the normal hours of operation.

To edit routing point options:

1. Navigate to a routing point group. You can edit routing points from the **All Resources** view or any reporting group view.
2. Select one routing point.
3. Select **Edit**.

The Edit Routing Point dialog is displayed.

Note:

If the routing point has been deleted from the system or if you do not have permissions to edit the routing point, the editor will display in view only mode. You can see the assigned options, but you cannot change any of the options. A deleted routing point will be marked with an asterisk (*).

4. Change the **Vector ID** and **Queue Preferences** options as required.
5. Select **OK** to submit the change request or **Schedule...** to schedule the change request. For information about scheduling an administrative change, see [Scheduling jobs](#) on page 105.

A success, pending, or failure message is displayed. If a failure message is displayed, resubmit the change request. If the request fails again, contact your system administrator to troubleshoot and resolve the problem.

Managing system preferences

This section contains procedures related to the following system preferences:

This section includes the following topics:

- [Administering login session properties](#) on page 95
- [Administering connection properties](#) on page 97
- [Administering SNMP alarming](#) on page 102
- [Administering advanced properties](#) on page 103

Administering login session properties

Path

From the **Tasks** tab, select **System Properties > Administer Login Session Properties**.

Field descriptions

Login Session Properties help you maintain secure access policies for your system. You can set the following properties:

Maximum Failed Login Attempts: This property defines the number of failed login attempts a user can make before they are locked out of the system. Each failed login attempt equals to one failed authentication attempt. The user cannot log back in until the **Lockout Duration** time has passed. The possible values are 1 to 999, with a default value of 3.

Lockout Duration: This property defines the amount of time in minutes a user must wait after being locked out of the system before they can make another login attempt. The possible values are 1 to 99 minutes, with a default value of 10.

Maximum Failed Authentication Attempts: This property defines the number of failed authentication attempts a user can make before an alarm is generated. The possible values are 1 to 999, with a default value of 3.

Session Timeout Duration: This property defines the login session timeout for administration users. The possible values are 1 to 1440 minutes, with a default value of 90 minutes.

Note:

This session timeout option does not control timeout for reporting users. Reporting users have a fixed 90 minute session timeout value.

Initial Password Change: This property enables an automatic password change request the first time a user logs in to administration. Changing this option from **Disable** to **Enable** will not force a password change for all users, only those who have never logged in to administration.

This option only applies to users added under the User Management task who have never before logged in to administration before this option was first enabled. This option does not apply to users integrated using the LDAP feature.

Security Banner Status: This property allows you to enable a security banner that is displayed every time any user logs in to administration. The banner text can be changed to a message that meets your company security needs. Use the following procedures to edit the logon security banner message:

- [Changing the administration logon security banner](#) on page 96

Changing the administration logon security banner



CAUTION:

You must restart the tomcat5 service to make a banner message change. Because restarting the service will end all administrative sessions, you should do this outside of normal business hours.

To change the logon banner message:

1. Edit the following file:

```
$CATALINA_HOME/webapps/CS-OAM/WEB-INF/classes/resources/  
application_Lang.properties
```

The variable *Lang* represents the language version for the property file.

2. Search for the phrase "security_message" in this file. You will see the default text following this phrase. Change the default text to any text you would want to be displayed when a user attempts to log in to administration. Avaya recommends that you make a copy of the original message before you change the default message.
3. After you change the message, save and close the property file.
4. Restart the tomcat5 service using the following command:

```
service tomcat5 restart
```

Related topics

[Unlocking user accounts](#) on page 59

Administering connection properties

This section includes the following topics:

- [Administering database connection properties](#) on page 97
- [Integrating with Active Directory](#) on page 98
- [Administering Communication Manager connections](#) on page 101
- [Administering Proactive Contact connections](#) on page 102
- [Administering Reporting connections](#) on page 102

Administering database connection properties

This section describes how to administer database connection properties. These properties were set during initial installation, configuration, and administration. If you find that you need to change any of the properties, such as the database user and password, use the procedure found in [Changing the database user names or passwords](#) on page 159. You can change database connection properties for the following database users. The identifier shown from the administration interface is shown in parentheses.

- Historical data store user (CCR)
- Content data store user (CCRCSC)
- Historical read-only user (CCRR)
- Real-time data store user (CCRRT)
- Reporting UI data store user (CCRUI)
- Historical read-write user (CCRW)
- System data store user (core)

**CAUTION:**

Verify that the database properties you are changing match the settings on the database. If the settings are changed and do not match the database, reporting data will be lost.

To administer the database connection properties:

1. Under the **Tasks** tab, select **Connection Management > Administer Connections**.
The All Connection Types dialog is displayed.
2. Select **Database Connection**.
The Connection Resources dialog is displayed.

3. Select a database connection name.
4. Select **Edit**.

The Edit Resource dialog is displayed.

5. Change properties as needed. Remember that any property changes made here must also be made on the database.
6. Select **OK**.

If successful, the All Connection Types dialog is displayed. If not successful, read the error message and correct any discrepancies.

Integrating with Active Directory

Avaya IQ can work with Windows Active Directory on Windows 2000 Server and Windows 2003 Server to integrate enterprise users with the Avaya IQ user management system. This allows you to add administrative and reporting users automatically from your enterprise directory without using separate authentication from Avaya IQ. Avaya provisioning can integrate your enterprise directory during initial implementation or you can do the integration yourself using the procedures provided in this section.



CAUTION:

To properly set the search filters and base node to select from, you must have intimate knowledge of your Active Directory setup. Do not attempt this procedure if you do not have that knowledge.

This section includes the following topics:

- [Prerequisites](#) on page 98
- [Administering an LDAP connection](#) on page 98
- [Administering a one-time job for initial synchronization](#) on page 101

Prerequisites

Before you begin to administer an LDAP connection, complete the [Active Directory worksheet for LDAP integration](#) on page 181.

The Active Directory must have the users administered with first and last names. If this is not done, the Base Node setup will not work properly.

Administering an LDAP connection

To administer LDAP options using Avaya IQ administration:

1. Log on to the Avaya IQ administration interface.

2. Under the **Tasks** tab, select **Connection Management > Administer Connections**.
The All Connection Types dialog is displayed.
3. Select **LDAP Connection**.
The Connection Resources dialog is displayed.
4. Select **Add**.
The Add Resource wizard is displayed.
5. Enter data for the following options:
 - **Connection Name** - This is a name for the connection. Take note of this name because it is used later when creating a scheduled job.
 - **Description** - Enter a description for the connection.
6. Select **Next**.
The next LDAP wizard page is displayed.
7. Enter data for the following options:
 - **Enable Connection Options** - Select **true**.
 - **Host name** - Enter the IP address or DNS name of the Windows 2000 or Windows 2003 server where Active Directory is running.
 - **LDAP port** - Enter the communication port to the Active Directory server. The default port for non-SSL connections is 389. The default port for SSL connections is 636.
 - **SSL Enabled** - Select **true** if using SSL on the Active Directory server. Select **false** if not using SSL.
8. Select **Next**.
The next LDAP wizard page is displayed.
9. Enter data for the following options:
 - **Enable SyncEngine Options** - Select **true**.
 - **User Name** - Enter the name of the user who has permission to search on the Active Directory server domain forest. This enterprise LDAP user must have the Active Directory object permissions of read all user information and search. This can be done by the ADS Delegate Control Wizard.
 - **User Password and User Password confirmation** - Enter and confirm the user password.
 - **Base node to pull from** - Enter the location on Active Directory from where you want to synchronize users. This should be the starting point within the ADS tree, the DC, and one level down. For example, `OU=SV Users,DC=horde,DC=avaya,DC=com`.
 - **Search Filter** - Enter a search filter to further streamline which users will be synchronized from the Active Directory. This is the actual direction to the particular group of Avaya IQ administration and report users, going from the lowest part of the

ADS tree (CN group of Avaya IQ users) to the top of the ADS tree. For example, `memberof=CN=iquser,OU=SV Users,DC=horde,DC=avaya,DC=com`. The search filter must conform with RFC 2254.

Contact the customer IT department for the ADS string. You can also use a tool named **ADSEdit** to get the proper ADS string. This tool is available in Resource Kit Win2k and Win2003. The search conforms to RFC2254 to use either **memberof**, **givenname**, or **objectclass**.

- **JDBC Name** - Enter **core**.
 - For all other JDBC options, do not enter any values.
 - For all DSE options, do not enter any values or change default values.
 - For the **Abort on first error**, **Sync all**, **Job Script**, **Sync Direction**, **Out Template**, **In Template**, and **Rules File** options, use the default values.
 - **Execution Time** - Enter the time of day when you want the LDAP scheduler job to run.
 - **Execution Frequency** - Select **Daily** so that synchronizations run every day. After the first synchronization, which synchronizes a complete set of enterprise directory data, subsequent updates only synchronize changes from the enterprise directory.
10. Select **Next**.
- The next LDAP wizard page is displayed.
11. Enter data for the following options:
- Set the **Enable Security Options** to **true** or **false**. If **false**, no other options on this page must be administered.
 - If the security options are enabled, set **Javax.net.ssl.truststore** to `$CSBASE/usermgmt/security/.truststore`.
 - Enter the appropriate password in the **javax.net.ssl.truststorepassword**, and **javax.net.ssl.truststorepassword confirmation** fields.
12. Select **Next**.
- The next LDAP wizard page is displayed.
13. Enter data for the following options:
- Set the **Enable Authentication Options** to **true** or **false**. If **false**, no other options on this page must be administered.
 - If the authentication options are enabled, administer the **User DN suffix** and **User DN prefix** options.
14. Select **Next**.
- The Finish Up dialog is displayed.
15. Select **Finish**.
- The LDAP options are added to the host. After the LDAP job has been scheduled and run for the first time, enterprise users will be synchronized into Avaya IQ.

16. After users are synchronized into Avaya IQ, you must assign the users to roles and assign permissions for the users, if needed. See the following information:
 - [About user roles](#) on page 38
 - [Administering roles](#) on page 49
 - [About data access permissions](#) on page 42
 - [Administering permissions for a user](#) on page 56

Administering a one-time job for initial synchronization

You must create a job to synchronize with the Active Directory for the first time.

To administer a one-time job to initially synchronize the enterprise directory:

1. Under the **Tasks** tab, select **Utility > Administer Scheduled Jobs**.
The View Scheduled Jobs dialog is displayed.
2. Select **Add**.
The Create Scheduled Job dialog is displayed.
3. Administer the following options:
 - **Job Type** - Select Enterprise Synchronization.
 - **Name** - Enter a name for the one-time job.
 - **Job Parameters** - Enter the Connection Name you used when you administered the LDAP options.
 - **Frequency** - Select One Time and Now to execute immediately.
4. Select **OK**.

Administering Communication Manager connections

Links to your Communication Manager sources were originally done during implementation of your deployment. This information is documented in [Creating and associating sources](#) on page 94 in *Avaya IQ Implementation*. If you need to add new Communication Manager sources, contact Avaya or your BusinessPartner.

Administering Proactive Contact connections

Links to your Proactive Contact sources were originally done during implementation of your deployment. This information is documented in [Creating and associating sources](#) on page 94 in *Avaya IQ Implementation*. If you need to add new Proactive Contact sources, contact Avaya or your BusinessPartner.

Administering Reporting connections

The reporting connections are created during installation and no options can be changed.

Administering SNMP alarming

Avaya IQ provides the ability to send alarms to your Network Management System (NMS). The capability is provided by a Simple Network Management Protocol (SNMP) feature. You or your BusinessPartner can administer this feature.

When SNMP is administered, you will get CPU and disk-space traps. Follow your local procedures to fix these problems. If you suspect that Avaya IQ is the source of problem and that adding disks, memory, tuning, and so on will not help, contact Avaya services for assistance.

To administer SNMP when using an NMS:

1. Log in as root on the Administration or All Functions host.
2. Enter:

```
cd $CCR_HOME/bin
```

3. Enter:

```
./iqsnmp.sh deploy
```

This command installs the SNMP components. The command determines what components are required based on the host type, and only installs those components. The command also determines minimum required RPMs to make SNMP work properly, so you may see messages requiring you to install additional RPMs. If you get this message, install the RPMs and run the deployment command again.

4. Enter:

```
iqsnmp.sh add -i ID -d NMS -a IP_Address -p Port -n Name
```

This command adds a SNMP Trap Receiver definition so that alarms are reported to the NMS. The options are defined as follows:

- *ID* is any unique ID within the **SNMPTrapReceiver** table. Start with the number 1 and increment the ID number as you add more trap definitions.
- *IP_Address* is the IP address of the NMS.
- *Port* is the listener port of the NMS (default is 162).
- *Name* is a unique community or security name identification of the trap. The community name identifies where the alarm came from. The security name is important if the NMS uses a security protocol.

After you add the trap, you can view, update, and delete the trap definition using the **select**, **update**, and **delete** options.

5. Repeat this procedure on all remaining application hosts in a multiple host configuration.

Administering advanced properties

Avaya IQ exposes many internal properties with the administration interface. For Release 4.1, Avaya recommends that you do not attempt to edit any of the advanced properties unless directed by Avaya services personnel.

Scheduling jobs

This section describes how to use the job scheduler and includes the following topics:

- [Scheduler job options](#) on page 105
- [Creating an on-demand scheduled job](#) on page 107
- [Creating scheduled jobs using a resource editor](#) on page 107
- [Viewing the status and history of scheduled jobs](#) on page 108
- [Editing a scheduled job](#) on page 109
- [Disabling, enabling, and deleting scheduled jobs](#) on page 110
- [Managing scheduled jobs](#) on page 111



Important:

Users must be authorized to access the scheduler based on their role. They must also have authorization to access the administrative task they will schedule.

Scheduler job options

This section describes the scheduler job options. Depending on the type of job you are scheduling, you may only see a subset of these options.

Job Type: This is the type of scheduled job. In this release of the product, you can schedule the following types of jobs:

- Enterprise directory synchronization
- Administration scheduled jobs when using the resource editors
- System scheduled jobs created when Avaya IQ was installed

For this release, the only job available when creating a new job directly from the scheduling interface is for enterprise directory synchronization.

Category: This is a display-only option that describes the type of job being scheduled.

Name: This is the name you assign to the job. The job name can be up to 60 characters long. For repeat jobs, create a name you will recognize later when monitoring your job status. Do not reuse the same job name for two different jobs. Create a new name for every job.

Job Parameters: This option details the changes being made within the job. Depending on the operation, this option requires input or is display-only.

- When creating a new job from the View Scheduled Jobs dialog, you must enter the Connection Name of the LDAP integration dialogs.
- When creating a scheduled job from a resource editor, this is a display-only option that shows the changes being made with your scheduled job. Verify that you made all the changes you wanted. If you need to go back and make more changes for this scheduled job, select Cancel to return to the resource editor.

Frequency: This option lets you specify how often you want to run the job. The available options include:

- One time - You can run the job immediately or set a time to run the job once. This is the only option for on-demand jobs.
- Hourly - You can set the amount of time between hourly jobs. The time period between jobs can be set in both hours and minutes.
- Daily - You can set the number of days between jobs.
- Weekly - You can set the number of weeks between jobs and which days of the week you want the job to run. For example, you can set the job to run every week on Monday and Friday, which gives you more flexibility when scheduling the job.
- Monthly - You can set the number of months between jobs, the day of the month you want the job to execute, or a relative day in the month that you want the job to execute. For example, you can set the job to run the 15th of every month or you can set the job to run the last Friday of every month.
- Yearly - You can set a specific date for the job to run or you can select a relative date for the job to run. For example, you can select January 15 to run the job or you can select the last Wednesday in January to run the job.

When setting the time of day, you can select either A.M., P.M., or a 24-hour clock. When using A.M. or P.M., you may only enter hours 1 through 12. When using the 24-hour clock, you can enter hours 0 through 23.

Range of Recurrence: This option lets you set the recurrence of your scheduled jobs, except for on-demand jobs, which occur only one time. The available options include:

- Start date - You must set the start date and time for the first occurrence of the job.
- End date - You must select an end date option. You can set the job to have no end date, to end after so many occurrences, or to end by a specific date and time.

Creating an on-demand scheduled job

To create a new on-demand scheduled job:

1. Under the **Tasks** tab, select **Utility > Administer Scheduled Jobs**.
The View Scheduled Jobs dialog is displayed.
2. Select **Add**.
The Create Scheduled Job dialog is displayed.
3. Set the schedule options as described in [Scheduler job options](#) on page 105.
4. When all options are defined, select **OK**.
A confirmation message is displayed.
5. Select **OK**.
The View Scheduled Jobs dialog is displayed.

Creating scheduled jobs using a resource editor

You can use the scheduler to change agent call handling preferences, multiple agent queue assignments, and routing point assignments. For example, if you want to change the queue assignments for an agent every day at noon and then change back at 5 p.m., you can create two separate jobs that make the change on a daily basis. The resources for which you can schedule changes include the following:

- [Administering multiple agent queue assignments](#) on page 83
- [Administering agent call handling options](#) on page 87
- [Administering routing point options](#) on page 92



Important:

Once you schedule a job using a resource editor, you cannot change the parameters of the job. You can only disable and delete the job. You can then create a new scheduled job to replace the old job.

To schedule a job when using a resource editor:

1. Make the changes you want to schedule using the resource editor.
2. Select **Schedule...**.
The Schedule Administration Job dialog is displayed.
3. Set the schedule options as described in [Scheduler job options](#) on page 105.

4. When all options are defined, select **OK**.

A confirmation message is displayed stating that the administration change was either successfully scheduled or that the scheduling failed.

5. Select **Close**.

The resource editor dialog is displayed.

6. Continue with other editor changes or select **Cancel** to leave the editor.

Viewing the status and history of scheduled jobs

You should monitor your scheduled jobs regularly to make sure that jobs are running properly.

To view scheduled jobs:

1. Under the **Tasks** tab, select **Utility > Administer Scheduled Jobs**.

The View Scheduled Jobs dialog is displayed.

2. Use the search function to limit the number of jobs displayed to only those you want to see. You can search based on status and category. To show all jobs after a search, select **Clear Results**.

3. Check the status of the jobs. This dialog provides the following information:

- **Name** - The name assigned to the job. Next to the name, the job is identified as **System Scheduled** or **Administration Scheduled**.
- **Frequency** - The assigned frequency for the job.
- **Last Run** - When the job was last run. If there is no date and time in this column, the job has yet to run for the first time.
- **Status** - The current status of the job. The following is a list of possible states:
 - **Failed** - The last run failed. Check the job parameters and try again. The failure may also be caused when the user was not authorized to make the administration change.
 - **Partial Failure** - The last run had problems during execution and only partially succeeded. Check the job parameters and try again.
 - **Pending Execution** - The job is scheduled to run in the future.
 - **Running** - The job is currently running.
 - **Success** - The last run completed successfully.
 - **Unknown** - The status of the job is unknown. Refresh the display to get a current status.
- **Scheduled by** - Who scheduled the job.

4. Select one of the scheduled jobs.
The status of the job is displayed at the bottom of the dialog.
5. Select **History**.
The Job History dialog is displayed.
6. You can enter a number to show that many recent jobs or you can enter a range of dates to see the history of a job.
7. Select **Show history**.
The history of the job as specified in the criteria is displayed.
8. When finished viewing the history, select **Close**.
The View Scheduled Jobs dialog is displayed.

Editing a scheduled job

To edit an active scheduled job:

1. Under the **Tasks** tab, select **Utility > Administer Scheduled Jobs**.
The View Scheduled Jobs dialog is displayed.
2. Select one of the scheduled jobs. The job must be active.
The status of the job is displayed at the bottom of the dialog.
3. Select **Edit**.
The Edit System Scheduled Job dialog is displayed.
4. Change the time properties of the scheduled job as described in [Scheduler job options](#) on page 105. Only the scheduled frequency and range of recurrence of the job can be changed. If you need to change any other parameters of the job, you should delete the job and recreate the job with the new parameters.
5. When the time options are changed, select **OK**.
The View Scheduled Jobs dialog is displayed.

Disabling, enabling, and deleting scheduled jobs

To disable or enable a job:

1. Under the **Tasks** tab, select **Utility > Administer Scheduled Jobs**.
The View Scheduled Jobs dialog is displayed.
2. Select one of the scheduled jobs.
The status of the job is displayed at the bottom of the dialog.
3. Select **Disable** if the job is currently enabled, or select **Enable** if the job is currently disabled.
A confirmation dialog is displayed.
4. Select **OK**.
The job is disabled or enabled.

To delete a job:

1. Under the **Tasks** tab, select **Utility > Administer Scheduled Jobs**.
The View Scheduled Jobs dialog is displayed.
2. Select one of the scheduled jobs.
The status of the job is displayed at the bottom of the dialog.
3. If the job is currently enabled, you must disable the job before it can be deleted. Select **Disable**.
A confirmation dialog is displayed.
4. Select **OK**.
The job is disabled.
5. Select the scheduled job again.
The status of the job is displayed at the bottom of the dialog.
6. Select **Delete**.
A confirmation dialog is displayed.
7. Select **OK**.
The job is deleted.

Managing scheduled jobs

This section contains tips on how you can more efficiently manage scheduled jobs.

If you have a routine job that you need to run often but not on any particular schedule, you can do the following:

1. Create the job with a daily frequency.
2. Run it the first time.
3. After the job completes, go to the View Scheduled Jobs dialog and disable the job.
4. When you need to run the job again, enable the job and it will run at the time originally specified when you created a job.
5. After the job runs, disable the job.

Routine maintenance

This section describes routine and occasional maintenance procedures you should perform for Avaya IQ. This section includes the following topics:

- [Monitoring logs and alarms](#) on page 114
- [Backup strategies](#) on page 114
- [Backing up Avaya IQ data](#) on page 116
- [Backing up the operating system](#) on page 117
- [Backing up the database](#) on page 117
- [Cleaning up user accounts](#) on page 146
- [About licensing](#) on page 146
- [Acquiring and installing license files](#) on page 148
- [Maintaining license files](#) on page 150
- [Installing updates](#) on page 151
- [Editing properties](#) on page 152
- [Changing the reporting email server](#) on page 152
- [Changing the reporting host used for aggregation](#) on page 154
- [Adjusting parameters for communication with Proactive Contact cron jobs](#) on page 155
- [Loading date and time zone data](#) on page 156
- [Verifying date, time, and NTP status](#) on page 159
- [Changing the database user names or passwords](#) on page 159
- [Database management](#) on page 164
- [Data removal](#) on page 164
- [Database schema and metadata sanity check](#) on page 165
- [Reinitializing user service](#) on page 166
- [Editing the service configuration](#) on page 166
- [Managing distributors](#) on page 166
- [Managing trusted certificates](#) on page 166

Monitoring logs and alarms

Avaya has the following recommendations for how frequently you should monitor your log and alarm files:

- Conduct a risk analysis based on the nature of your business. You should consider how critical the application is to your business, and the type of data contained in the log and alarm files.
- Consider the damage or repercussions that could occur if particular types of events went undetected.
- Determine if weekly, daily or continuous monitoring of an event must be performed.
- Create your own policy based on your analysis. You might require different monitoring intervals for different events.
- Check the admin access log.
- Check the security access log.

For detailed information about how to monitor logs and alarms, see *Avaya IQ Alarms and Logs*.

Backup strategies

Backing up your data reduces the risk of losing data due to hardware failures, human errors, application failures, and security breaches, such as hackers or viruses. Maintaining quality backups is economical and minimizes costs for your contact center operation. Your contact center will have additional costs if your data must be recovered and your backups are not available or are of poor quality. You might experience these costs as system down time, data loss, or unnecessary financial expense. You must back up your data if your data is crucial to the successful operation of your contact center.



CAUTION:

Even if you back up your data on a regular basis, you may still lose some administrative data between the time of the last backup and when your system fails. If you follow the recommended backup strategies, these potential losses will be minimized.

Avaya recommends that you:

Determine how critical the data is to your business.

- What data do you need to back up?
- What damage or repercussions would occur if the data was lost?

- How quickly would the system need to be operational if the system became inoperative?
- How frequently is the data in your database updated?
- How long can your application be down while you are recovering your database?
- How big is your database?
- What will you use to back up your data? Disk or tape?
- Is it necessary to rotate your backup media?
- How frequently should you backup your data?

Create your own data backup policy.

- Use the tools provided and supported by your software vendors.
- Follow any recommendations provided by your software vendors.
- Determine when daily, weekly, or monthly backups must be performed.
- Determine when an incremental or full backup must be performed.
- Determine if you will create backups after all administrative changes.
- Determine how long you will retain a backup.

Verify that your backups are of good quality.

- Use a reliable backup system.

Store your backups in a safe location.

- Keep your backups secured in your equipment room.

To do your backups, use the procedures in the following sections:

- [Backing up Avaya IQ data](#) on page 116
- [Backing up the operating system](#) on page 117
- [Backing up the database](#) on page 117

Backing up Avaya IQ data

Routinely backing up Avaya IQ data is critical to the smooth operation of your contact center. Should one of your application hosts fail, having a backup of the Avaya IQ data will help speed recovery of the system.



Important:

You should create a routine backup schedule and follow this schedule for all application hosts in the deployment.

Procedures for restoring these backup files for a recovery are documented in *Avaya IQ Troubleshooting*. Avaya or BusinessPartner personnel will be involved for any recovery procedure of this type.

Avaya recommends that you back up Avaya IQ data after the initial implementation, after a major set of administrative changes, and after any third-party configuration data is changed. At a minimum, you should do a backup no less than once a week. You can administer the backup to run on a scheduled basis, but you must manually copy the data to media on a regular basis. You must determine what type of media you will use for the backup.

Backups of the Avaya IQ data require about 10 GB of temporary free space. Before you begin this procedure, find a directory that has this amount of free space.

To back up Avaya IQ data:

1. Log on to your application host as root.
2. Enter:

```
mkdir /<DIR>/backup
```

<DIR> must be a directory that has at least 10 GB of free space.

3. Enter:

```
cd /<DIR>/backup
```

4. Enter the following commands to back up the Avaya IQ files:

```
tar -cvzf etc_<host_date>.tgz /etc
```

```
tar -cvzf var_<host_date>.tgz /var
```

```
tar -cvzf Avaya_<host_date>.tgz /opt/Avaya
```

```
tar -cvzf coreservices_<host_date>.tgz /opt/coreservices
```

```
tar -cvzf oracle_<host_date>.tgz $ORACLE_HOME
```

This will create the backup files in the specified backup directory. Enter the host name and date to help keep track of the backup files.

5. To verify that the commands ran successfully, enter the following command:

```
ls
```

6. To view the contents of each backup tar file, enter:

```
tar -tvzf <filename>.tgz
```

7. Transfer all of the backup files to your backup media. This can be disk or tape.
8. Store the backup media in a safe location that can be found quickly for recovery.
9. After the backup files have been transferred to your backup media, enter:

```
rm -rf /<DIR>/backup
```

This removes the temporary backup location.

10. Repeat this procedure for every application host in your deployment.

Backing up the operating system

The OS used with application and database hosts should be backed up on a routine basis on backup media of your choice. You should follow the backup procedures documented by your OS vendor. When restoring your OS from a backup, you should follow the restore procedures documented by your OS vendor.

Backing up the database

Routinely backing up the database is critical to the smooth operation of your contact center. Should your database host fail, having a backup of the database will help speed recovery of the system. You should create a routine backup schedule and follow this schedule for the database host. The size of your warehouse, the desired duration of performing a backup, and the ease of recovery plays a big part when determining your backup strategy.

Important:

Avaya recommends that you use RMAN to do Oracle backups. RMAN has been tested and was found to successfully back up the database and the backups were used to successfully restore the database.

You can administer the backup to run on a scheduled basis and write the backed up data to media. You must determine what type of media you will use for the backup. A backup of the database can be very large.

You should follow the procedures documented by your database vendor when backing up the database and restoring your database from a backup. Additional steps required to restore the database can be found in *Avaya IQ Troubleshooting*. Avaya or BusinessPartner personnel may be involved with database recovery.

This section includes the following topics:

- [Sample backup scenarios](#) on page 118
- [General backup procedures](#) on page 120
- [Oracle files required to perform backup procedures](#) on page 121
- [RMAN setup and configuration](#) on page 122
- [RMAN configuration for control files](#) on page 131
- [Full backup of database and archive logs \(first on-line backup\)](#) on page 134
- [Full backup of database and archive logs with archive log purge](#) on page 136
- [RMAN incremental differential backup](#) on page 136
- [RMAN incremental cumulative backup](#) on page 137
- [RMAN tablespace backup](#) on page 137
- [Creating a cron job to schedule your full backup](#) on page 138
- [Verifying backup sets](#) on page 140

Sample backup scenarios

Oracle provides several levels of backup for your database. To plan the best scenario for your situation, you must first understand the different levels of backups.

Full backup: A non-incremental RMAN backup. Note that "full" does not refer to how much of the database is backed up, but to the fact that the backup is not incremental. Consequently, you can make a full backup of one data file. If your database is small, a full backup may not take that long and you could do a full backup every day. If you have a large database, a full backup is something you can only do at low traffic periods and not on a daily basis.

Archive log backup: The mode of the database in which Oracle copies filled online redo logs to disk. Oracle automatically performs the this archiving unless you change the operation to manual. An archive log backup is typically done on an hourly basis to back up small amounts of data in between other daily backups.

Incremental backup: An RMAN backup in which only modified blocks are backed up. Incremental backups are classified by level. An incremental level 0 backup performs the same function as a full backup in that they both back up all blocks that have ever been used. The difference is that a full backup will not affect blocks backed up by subsequent incremental backups, whereas an incremental backup will affect blocks backed up by subsequent incremental backups.

Incremental backups at level 1 back up only blocks that have changed since previous incremental backups. Blocks that have not changed are not backed up. An incremental backup can be either a differential incremental backup or a cumulative incremental backup. A cumulative incremental backup backs up all blocks changed since the last level 1 incremental backup. A differential incremental backup backs up all blocks changed since the last level 0 or level 1 incremental backup.

Based on how these backups operate, the following are two sample scenarios that may work for you depending on the size of your database and performance of your database host.

For any scenario you set up, remember to keep old backups until you are sure they are not needed. Verify sanity of all backups using the Oracle tools.

Scenario #1

This is the minimum backup strategy that can be implemented. This is not recommended by Avaya because if a failure occurs, all transactions committed after the last full backup are lost.

- Perform a full backup weekly, and before and after configuration changes made to the database.

Scenario #2

This scenario may work well for small databases where you can complete a full backup overnight during low traffic periods.

- Perform full backups daily
- Perform archive log backups hourly

Scenario #3

This scenario fits within a full week of scheduled backups. A full backup is only done once a week and the daily backups are repeated every week.

- Perform full backup on Day 1
- Perform backup of archive logs hourly
- Perform differential incremental backup on Day 2
- Perform differential incremental backup on Day 3
- Perform cumulative incremental backup on Day 4
- Perform differential incremental backup on Day 5
- Perform differential incremental backup on Day 6
- Perform differential incremental backup on Day 7

This scenario may work well for medium to large databases where you cannot do full backups every night, but incremental backups can be done for several days in between full backups. You will still want to do backups during low traffic periods.

Scenario #4

This scenario fits within a full week of scheduled backups, but only certain tablespaces are backed up each day. A full backup is only done once a week. You should repeat this scenario every week.

- Perform full backup on Day 1
- Perform backup of archive logs hourly
- Perform differential incremental backup of non-historical tablespaces and historical tablespaces 1 and 2 on Day 2
- Perform differential incremental backup of non-historical tablespaces and historical tablespaces 3 and 4 on Day 3
- Perform differential incremental backup of non-historical tablespaces and historical tablespaces 5 and 6 on Day 4
- Perform differential incremental backup of non-historical tablespaces and historical tablespaces 7 and 8 on Day 5
- Perform differential incremental backup of non-historical tablespaces and historical tablespaces 9 and 10 on Day 6
- Perform differential incremental backup of non-historical tablespaces and any other historical tablespaces on Day 7

This scenario may work well for very large databases where you cannot do full backups every night, but incremental backups can be done for several days in between full backups. You will still want to do backups during low traffic periods.

General backup procedures

Depending on the type of backup you are doing, you will follow one of the following backup procedures:

- Cold and offline backups
- Online backups

Cold and offline backups are supported by Oracle, but not viewed as an optimal solution for Avaya IQ as there is a service impact. If a user decides to implement these types of backups, please refer to the Oracle documentation.

An online backup of the database means that the database is backed up without shutting down any databases or Oracle. The benefit is that there is no service interruption and users can continue using Avaya IQ. To do an online backup of a database when in ARCHIVELOG mode:

1. Back up all database datafiles.
2. Force an online redo logs switch with ALTER SYSTEM SWITCH LOGFILE.
3. Back up the archived redo logs.

4. Create a backup of the control file.

Oracle files required to perform backup procedures

Backup, restore, and recovery involves various oracle files that comprise a database. The following describes the files that make up an Oracle database.

Oracle requires the following files for its operation:

- **Datafiles:** Contains logical units (called blocks) that comprise the database. The SYSTEM tablespace data file, which holds the data dictionary and other system-owned database objects. The datafiles are located under the database storage location

Data files can be backed up by RMAN.

- **Online Redo Logs:** Contains transaction information for transaction rollback and for instance recovery in case of a database crash. Since these files hold critical information, it is wise to maintain two or more identical copies of these files on independent disks (multiplexing). Each set of copies is known as a redo log group. Note that online logs should NEVER be backed up in a hot backup. If you do back them up, there is a danger that you may overwrite your current (valid) logs with the backed up ones which are out of date and therefore invalid.
- **Control File:** Contains the physical structure of the database (location of all files), current database state, and information regarding backups taken by RMAN. Control files are being critical to database operation.

Control files can be optionally backed up by RMAN.

- **Archived Redo Logs:** Archived copies of online redo logs created after a switch occurs from one online log to the next one in the group. Archiving ensures that a complete transaction history is maintained. Once an online log is archived, it can be overwritten without any loss of transaction history. Archive logs are required for online backups.

Note that online logs are archived only when the database operates in ARCHIVELOG mode. The default operation mode is NOARCHIVELOG where online redo logs are not archived before being overwritten.

Archive logs can be optionally backed up by RMAN.

- **Server Parameter File (also known as Stored parameter file):** Contains initialization parameters that are used to configure the Oracle instance on startup. This file is located in `$ORACLE_HOME/dbf`.

The server parameter file can be optionally backed up by RMAN.

- Password File: Stores credentials of users who are allowed to log on to Oracle as privileged (sysdba) users without having to supply an Oracle password. Users with sysdba privileges are allowed to perform database startup, shutdown and backups (among other administrative operations). Please check the Oracle Administrator's guide for details on sysdba and sysoper privileges. The password file is located at `$ORACLE_HOME/dbs`.
This file is not backed up by RMAN, and must be backed up via OS commands, i.e. tar.
- Networking Files: `tnsnames.ora`, `listener.ora` and `sqlnet.ora` are Oracle network configuration files. They are generally maintained in `$ORACLE_HOME/network/admin`.
These files are not backed up by RMAN, and must be backed up via OS commands, i.e. tar.
- Additional Files: All database creation scripts in the backup directory should be backed up. This may help in determining the correct database file directory structure for disaster recovery. However, this is not absolutely necessary as file locations can be retrieved from the backup control file.

RMAN setup and configuration

This section describes at a high level how to set up and configure Oracle's RMAN tool. For details on how to set up and configure RMAN, see Oracle database documentation.

The Avaya IQ backup strategy assumes that you know how to use the following Oracle tools and techniques:

- RMAN
- Flash Recovery Area (FRA)

The FRA is not required, but recommended for Oracle 10g, and consolidates all recovery files in one place, including: RMAN backups, redo logs, control file backups, and other flashback logs.

According to Oracle, FRA can automatically manage all the backup and recovery files with no DBA interventions.

- Recovery Catalog for RMAN

A Recovery Catalog is not required for RMAN, but is recommended by Oracle to store RMAN scripts, storage of backup information, storage of default channel configuration, and so on.

Avaya IQ backup testing was done using a disk drive as the backup media. It is recommended that customers use disk or tape as backup media.

This section includes the following topics:

- [Configuring RMAN and FRA](#) on page 123
- [Configuring an RMAN catalog](#) on page 126

Configuring RMAN and FRA

To set up and configure RMAN in the target database:

1. Back up critical Oracle files. Regular backups should be made of the Oracle Home directory. Here is an example procedure to backup the critical Oracle files. Find a storage location on the server to store the backup files (~600MB). Some critical Oracle files are needed for disaster recovery.

```
<su to the oracle user on the system>
[root@robdb /]# su - oracle
[root@robdb oracle]# tar cvzf Oracle_home_<host_date>.tgz $ORACLE_HOME
[oracle@robdb ~]$ ls -l
total 580284
-rw-r--r--  1 oracle oinstall 593602472 Sep  5 04:48 Oracle_home_robicq.tgz
```

2. Put the database in ARCHIVELOG mode.

```
<su to the oracle user on the system>
# su - oracle
$

<launch sqlplus to perform database changed>
$ sqlplus sys/<password>@ccr as sysdba;
SQL> shutdown immediate;
Database closed.
Database dismounted.
ORACLE instance shut down.

$ sqlplus / as sysdba;

SQL*Plus: Release 10.2.0.2.0 - Production on Wed Jun 20 18:55:23 2007

Copyright (c) 1982, 2005, Oracle. All Rights Reserved.

Connected to an idle instance.

SQL> startup mount
ORACLE instance started.

Total System Global Area 2147483648 bytes
Fixed Size 1261860 bytes
Variable Size 520097500 bytes
Database Buffers 1610612736 bytes
Redo Buffers 15511552 bytes
Database mounted.
SQL> alter database archivelog;

Database altered.

SQL> alter database open; (A10)

Database altered.
```

3. Configuring the size and destination of the Flash Recovery Area are the two critical steps in configuring an FRA. Do not put the destination on the same disk as Oracle. Oracle recommends that another disk be used by the Flash Recovery Area.

Note:

Make the flash recovery area large enough to hold the number of desired backups times the size of the database, that is, 3 daily full backup times 100 GB would require a minimum of 310 GB for a flash recovery area. The example sets the flash recovery area to 20 GB.

```
<connect to sqlplus to perform maintenance>
$ sqlplus / as sysdba;
```

```
SQL*Plus: Release 10.2.0.2.0 - Production on Wed Jun 20 18:55:23 2007
```

```
Copyright (c) 1982, 2005, Oracle. All Rights Reserved.
```

```
Connected to an idle instance.
```

```
<defines size of the flash recovery area>
SQL> alter system set db_recovery_file_dest_size=20G scope=both;
```

```
System altered.
```

```
<set the location for the flash recovery area - preferably a separate disk from
tablespaces>
```

```
SQL> alter system set db_recovery_file_dest='/u01/app/oracle/flash_recovery_area;
```

```
System altered.
```

```
<view the flash recovery directory created on disk>
[oracle@robdb flash_recovery_area]$ ls -l /u01/app/oracle/flash_recovery_area
total 8
drwxr-x---  4 oracle oinstall 4096 Aug 29 22:21 AVAYAIQ
[oracle@robdb AVAYAIQ]$ ls -l /u01/app/oracle/flash_recovery_area/AVAYAIQ/
total 16
drwxr-x---  5 oracle oinstall 4096 Aug 30 00:19 archivelog
drwxr-x---  3 oracle oinstall 4096 Aug 29 22:21 backupset
```

4. Create an RMAN user (rman_user) with sysdba privileges. The RMAN user is used to manage backups, restores, and recovery. Any user name can be used. For this example we create a user call RMAN_USER.

<assumes that you are still connected from the previous steps. You must disconnect to create the user.>

```
SQL> disconnect
```

Disconnected from Oracle Database 10g Enterprise Edition Release 10.2.0.2.0 -
Production

With the Partitioning and Data Mining options

```
SQL> connect sys/AvayaIQ07@AVAYAIQ as sysdba;
```

Connected.

```
SQL> alter database open;
```

Database altered.

```
SQL> create user "RMAN_USER" profile "DEFAULT" identified by password
      2 default tablespace "USERS" ACCOUNT UNLOCK;
```

User created.

```
SQL> GRANT SYSDBA to "RMAN_USER";
```

Grant succeeded.

```
SQL> GRANT "CONNECT" to "RMAN_USER";
```

Grant succeeded.

Configuring an RMAN catalog

RMAN backup information can be stored in the RMAN catalog (a separate database) or in the target database's control files. Using an RMAN catalog is a safer alternative to control files and will make all recovery scenarios simpler. Otherwise, the correct backup files have to be determined by the DBA during a recovery scenario. Using an RMAN catalog also adds another level of availability to the database in case the control files of the target database also need to be recovered.

In the Recovery Catalog Repository (or database instance RMANREP), do the following procedures:

1. Create a database for the RMAN backup catalog. For improved recovery, a separate database will be built. Keeping a separate database for backup information will enable recovery of the Avaya IQ database when the IQ database is corrupted, control files are missing, or other catastrophic issues.

The following is an example of creating a new RMAN database. It is not the only method of creating a backup catalog database. This method will work from the command line when there is no GUI interface available.

```
<this example assumes that you are creating the database as a root user, i.e. sudo
/ su commands are used>
[root@rodbdb ~]# sudo su - oracle -c "dbca -silent -createDatabase -templateName
avayaiq_db_template.dbt -gdbName rmanrep -sid rmanrep -sysPassword password
-systemPassword password -emConfiguration LOCAL -dbsnmpPassword password
-sysmanPassword password -datafileDestination /u01/app/oracle/oradata
-recoveryAreaDestination /u01/app/oracle/flash_recovery_area -storageType FS
-characterSet AL32UTF8 -nationalCharacterSet UTF8 -registerWithDirService false
-listeners listener -memoryPercentage 20 -databaseType DATA_WAREHOUSING
-sampleSchema false -oratabLocation /etc/oratab -continueOnNonFatalErrors false"
Creating and starting Oracle instance
1% complete
4% complete
Creating database files
5% complete
9% complete
Creating data dictionary views
10% complete
11% complete
13% complete
14% complete
15% complete
16% complete
19% complete
20% complete
21% complete
22% complete
23% complete
```

Adding Oracle JVM
24% complete
30% complete
37% complete
44% complete
46% complete
Adding Oracle Data Mining
47% complete
48% complete
50% complete
Adding Oracle Text
51% complete
52% complete
54% complete
55% complete
Adding Oracle XML DB
56% complete
57% complete
58% complete
59% complete
63% complete
64% complete
Adding Oracle Intermedia
65% complete
77% complete
Adding Oracle Spatial
78% complete
79% complete
80% complete
81% complete
86% complete
Completing Database Creation
88% complete
89% complete
91% complete
95% complete
99% complete
100% complete
Look at the log file "/u01/app/oracle/product/10.2.0/Db_1/cfgtoollogs/dbca/
rmanrep/rmanrep0.log" for further details.

2. Create a tablespace for the catalog.

```
< In Recovery Catalog Repository / Database Instance (rmanrep)>
[oracle@rodbdb bin]$ sqlplus sys/password@rmanrep as sysdba
```

```
SQL*Plus: Release 10.2.0.2.0 - Production on Tue Sep 4 01:58:31 2007
```

```
Copyright (c) 1982, 2005, Oracle. All Rights Reserved.
```

```
Connected to:
```

```
Oracle Database 10g Enterprise Edition Release 10.2.0.2.0 - Production
With the Partitioning and Data Mining options
```

```
SQL> CREATE SMALLFILE TABLESPACE "CATALOG_TBS" DATAFILE '/u01/app/oracle/oradata/
rmanrep/CATALOG_01' SIZE 15M LOGGING EXTENT MANAGEMENT LOCAL SEGMENT SPACE
MANAGEMENT AUTO;
```

```
Tablespace created.
```

3. Create an RMAN catalog user (rcat_user) to connect to the recovery catalog.

```
<Continuing from sqlplus login above>
```

```
SQL> create user "RCAT_USER" PROFILE "DEFAULT" IDENTIFIED BY "password"
  2  QUOTA UNLIMITED ON "CATALOG_TBS"
  3  DEFAULT TABLESPACE "CATALOG_TBS" ACCOUNT UNLOCK;
```

```
User created.
```

```
SQL> GRANT SYSDBA TO "RCAT_USER";
```

```
Grant succeeded.
```

```
SQL> GRANT "RECOVERY_CATALOG_OWNER" TO "RCAT_USER";
```

```
Grant succeeded.
```

```
SQL> GRANT "RESOURCE" TO "RCAT_USER";
```

```
Grant succeeded.
```

```
SQL> GRANT "CONNECT" TO "RCAT_USER";
```

```
Grant succeeded.
```

```
SQL> GRANT CREATE TYPE TO "RCAT_USER";
```

```
Grant succeeded.
```

```
ALTER USER "RCAT_USER" DEFAULT ROLE ALL;
```

```
User altered.
```

```
SQL> quit
```

4. Create the recovery catalog.

```
<Continuing from table space creation above>
[oracle@robdb rmanrep]$ rman catalog rcat_user/password@rmanrep

Recovery Manager: Release 10.2.0.2.0 - Production on Tue Aug 28 20:42:59 2007

Copyright (c) 1982, 2005, Oracle. All rights reserved.

connected to recovery catalog database

RMAN> create catalog tablespace catalog_tbs;

recovery catalog created

RMAN> quit

Recovery Manager complete.
```

5. Set the catalog database to restart after the database host reboots. By default, databases are not set to automatically restart after a reboot. You can change this setting by modifying the `oratab` file located in `/etc`.

```
<edit the oratab file in /etc; below is the unmodified file>
# This file is used by ORACLE utilities. It is created by root.sh
# and updated by the Database Configuration Assistant when creating
# a database.

# A colon, ':', is used as the field terminator. A new line terminates
# the entry. Lines beginning with a pound sign, '#', are comments.
#
# Entries are of the form:
#   $ORACLE_SID:$ORACLE_HOME:<N|Y>:
#
# The first and second fields are the system identifier and home
# directory of the database respectively. The third field indicates
# to the dbstart utility that the database should, "Y", or should not,
# "N", be brought up at system boot time.
#
# Multiple entries with the same $ORACLE_SID are not allowed.
#
#
AVAYAIQ:/u01/app/oracle/product/10.2.0/Db_1:Y
rmancat:/u01/app/oracle/product/10.2.0/Db_1:N

<change the rmancat (catalog database) setting to Y >
rmancat:/u01/app/oracle/product/10.2.0/Db_1:Y
```

6. Register the target database with the recovery catalog.

```
[oracle@rodbdb bin]$ rman target=rman_user/password@avayaiq catalog=rcat_user/
password@rmanrep
```

```
Recovery Manager: Release 10.2.0.2.0 - Production on Tue Sep 4 02:36:58 2007
```

```
Copyright (c) 1982, 2005, Oracle. All rights reserved.
```

```
connected to target database: AVAYAIQ (DBID=353319860)
connected to recovery catalog database
```

```
RMAN> register database;
```

```
database registered in recovery catalog
starting full resync of recovery catalog
full resync complete
```

7. Verify database registration with the recovery catalog.

```
RMAN> report schema;
```

```
Report of database schema
```

```
List of Permanent Datafiles
=====
```

File	Size(MB)	Tablespace	RB segs	Datafile Name
1	460	SYSTEM	YES	/u01/app/oracle/oradata/avayaiq/system01.dbf
2	925	UNDOTBS1	YES	/u01/app/oracle/oradata/avayaiq/undotbs01.dbf
3	260	SYS_AUX	NO	/u01/app/oracle/oradata/avayaiq/sysaux01.dbf
4	5	USERS	NO	/u01/app/oracle/oradata/avayaiq/users01.dbf
5	4096	AVAYAIQ	NO	/u01/app/oracle/oradata/avayaiq/avayaiq
6	4096	AVAYAIQDIM	NO	/u01/app/oracle/oradata/avayaiq/avayaiqdim
7	4096	AVAYAIQFACT1	NO	/u01/app/oracle/oradata/avayaiq/avayaiqfact1
8	4096	AVAYAIQFACT2	NO	/u01/app/oracle/oradata/avayaiq/avayaiqfact2
9	4096	AVAYAIQFACT3	NO	/u01/app/oracle/oradata/avayaiq/avayaiqfact3
10	4096	AVAYAIQRPT	NO	/u01/app/oracle/oradata/avayaiq/avayaiqrpt
11	4096	AVAYAIQSDS	NO	/u01/app/oracle/oradata/avayaiq/avayaiqsds
12	4096	AVAYAIQRT	NO	/u01/app/oracle/oradata/avayaiq/avayaiqrt
13	4096	AVAYAIQRCL	NO	/u01/app/oracle/oradata/avayaiq/avayaiqrcl
14	15	CATALOG_TBS	NO	/u01/app/oracle/oradata/rmanrep/CATALOG_01

```
List of Temporary Files
```

```
=====
```

File	Size(MB)	Tablespace	Maxsize(MB)	Tempfile Name
1	20	TEMP	5000	/u01/app/oracle/oradata/avayaiq/temp01.dbf

Avaya recommends that you use tape for production systems. To configure tape media, please refer to RMAN and to your third party media backup manager vendor documentation.

--- RMAN configuration for control files

This section includes the following topics:

- [Display RMAN configuration](#) on page 131
- [RMAN auto-backup location and file format for control files](#) on page 132
- [RMAN backup of control file naming convention](#) on page 132
- [Validation of RMAN backup of control file naming convention](#) on page 133

Display RMAN configuration

Displaying RMAN configuration is useful in understanding vital information for recovery. Here is an example of the RMAN configuration.

```
[oracle@robdb 2007_09_04]$ rman target=rman_user/password@avayaiq
catalog=rcat_user/password@rmanrep
```

```
Recovery Manager: Release 10.2.0.2.0 - Production on Tue Sep 4 20:28:48 2007
```

```
Copyright (c) 1982, 2005, Oracle. All rights reserved.
```

```
connected to target database: AVAYAIQ (DBID=353319860)
connected to recovery catalog database
```

```
RMAN> show all;
```

```
RMAN configuration parameters are:
```

```
CONFIGURE RETENTION POLICY TO REDUNDANCY 1; # default
CONFIGURE BACKUP OPTIMIZATION OFF; # default
CONFIGURE DEFAULT DEVICE TYPE TO DISK; # default
CONFIGURE CONTROLFILE AUTOBACKUP ON;
CONFIGURE CONTROLFILE AUTOBACKUP FORMAT FOR DEVICE TYPE DISK TO '%F'; # default
CONFIGURE DEVICE TYPE DISK PARALLELISM 1 BACKUP TYPE TO BACKUPSET; # default
CONFIGURE DATAFILE BACKUP COPIES FOR DEVICE TYPE DISK TO 1; # default
CONFIGURE ARCHIVELOG BACKUP COPIES FOR DEVICE TYPE DISK TO 1; # default
CONFIGURE MAXSETSIZE TO UNLIMITED; # default
CONFIGURE ENCRYPTION FOR DATABASE OFF; # default
CONFIGURE ENCRYPTION ALGORITHM 'AES128'; # default
CONFIGURE ARCHIVELOG DELETION POLICY TO NONE; # default
CONFIGURE SNAPSHOT CONTROLFILE NAME TO '/u01/app/oracle/product/10.2.0/Db_1/dbs/
snapcf_avayaiq.f'; # default
```

RMAN auto-backup location and file format for control files

This is a crucial step in helping ensure the DBID is preserved for full database and disaster recovery situations. Completing the RMAN autobackup configuration will result in the DBID being stored as part of the filename for the control files. Note that you must specify a backup location which is typically where the other backup files are being stored. Here is an example for changing the configuration.

```
[oracle@robdb dbs]$ rman target=rman_user/password@avayaiq catalog=rcat_user/
password@rmanrep
```

```
Recovery Manager: Release 10.2.0.2.0 - Production on Tue Sep 4 23:15:36 2007
```

```
Copyright (c) 1982, 2005, Oracle. All rights reserved.
```

```
connected to target database: AVAYAIQ (DBID=353319860)
connected to recovery catalog database
```

```
RMAN> configure controlfile autobackup on;
new RMAN configuration parameters:
CONFIGURE CONTROLFILE AUTOBACKUP ON;
new RMAN configuration parameters are successfully stored
starting full resync of recovery catalog
full resync complete
```

```
RMAN> configure controlfile autobackup format for device type disk to '/u01/app/
oracle/flash_recovery_area/AVAYAIQ/autobackup/controlfile_%F';
```

```
old RMAN configuration parameters:
CONFIGURE CONTROLFILE AUTOBACKUP FORMAT FOR DEVICE TYPE DISK TO 'controlfile%F';
new RMAN configuration parameters:
CONFIGURE CONTROLFILE AUTOBACKUP FORMAT FOR DEVICE TYPE DISK TO '/u01/app/oracle/
flash_recovery_area/AVAYAIQ/autobackup/controlfile_%F';
new RMAN configuration parameters are successfully stored
starting full resync of recovery catalog
full resync complete
```

RMAN backup of control file naming convention

After completing a database backup, control files will also be automatically backed up to the location specified in the previous steps. The first number string is the DBID and the second number string is the date.

```
controlfile_c-353319860-20070904-06
```

Validation of RMAN backup of control file naming convention

The control files location and file name format can be validated by completing a backup of the current control file.

```
[oracle@robdb dbs]$ mkdir /u01/app/oracle/flash_recovery_area/AVAYAIQ/autobackup/
[oracle@robdb dbs]$ cd /u01/app/oracle/flash_recovery_area/AVAYAIQ/
[oracle@robdb autobackup]$ chmod 750 autobackup
[oracle@robdb autobackup]$ chown oracle:oinstall autobackup
[oracle@robdb autobackup]$ rman target=rman_user/password@avayaig
catalog=rcat_user/password@rmanrep
```

Recovery Manager: Release 10.2.0.2.0 - Production on Tue Sep 4 23:15:36 2007

Copyright (c) 1982, 2005, Oracle. All rights reserved.

connected to target database: AVAYAIQ (DBID=353319860)
connected to recovery catalog database

```
RMAN> backup current controlfile;
```

```
Starting backup at 04-SEP-07
allocated channel: ORA_DISK_1
channel ORA_DISK_1: sid=1040 devtype=DISK
channel ORA_DISK_1: starting full datafile backupset
channel ORA_DISK_1: specifying datafile(s) in backupset
including current control file in backupset
channel ORA_DISK_1: starting piece 1 at 04-SEP-07
channel ORA_DISK_1: finished piece 1 at 04-SEP-07
piece handle=/u01/app/oracle/flash_recovery_area/AVAYAIQ/backupset/2007_09_04/
ol_mf_ncnnf_TAG20070904T232644_3fwhjnwmm_.bkp tag=TAG20070904T232644 comment=NONE
channel ORA_DISK_1: backup set complete, elapsed time: 00:00:01
Finished backup at 04-SEP-07
```

```
Starting Control File and SPFILE Autobackup at 04-SEP-07
piece handle=/u01/app/oracle/flash_recovery_area/AVAYAIQ/autobackup/
controlfile_c-353319860-20070904-06 comment=NONE
Finished Control File and SPFILE Autobackup at 04-SEP-07
```

```
RMAN> exit
```

Recovery Manager complete.

```
[oracle@robdb autobackup]$ ls -l
total 7136
-rw-r----- 1 oracle oinstall 7274496 Sep  4 23:26
controlfile_c-353319860-20070904-06
```

Full backup of database and archive logs (first on-line backup)

The benefits of this type of backup include:

- The backup is done online. Avaya IQ does not have to be stopped.
- The backup can be scheduled using an RMAN script and a cron job or an Oracle scheduler job.
- The backup is easy to do using RMAN.

During execution of the first on-line backup process, the archive log files are backed up and a full backup of the database (all tablespaces and data files). You can see the location where the backup files are stored. Additionally, the current control files and SPFILE are stored as part of backup set.

```
[oracle@rodbdb rmanrep]$ rman target=rman_user/password@avayaiq catalog=rcat_user/
password@rmanrep
```

```
Recovery Manager: Release 10.2.0.2.0 - Production on Wed Aug 29 22:21:28 2007
```

```
Copyright (c) 1982, 2005, Oracle. All rights reserved.
```

```
connected to target database: AVAYAIQ (DBID=353319860)
connected to recovery catalog database
```

```
<backup database and archive log>
RMAN> backup database plus archivelog;
```

```
Starting backup at 29-AUG-07
current log archived
allocated channel: ORA_DISK_1
channel ORA_DISK_1: sid=1084 devtype=DISK
channel ORA_DISK_1: starting archive log backupset
channel ORA_DISK_1: specifying archive log(s) in backup set
input archive log thread=1 sequence=383 recid=1 stamp=631819605
input archive log thread=1 sequence=384 recid=2 stamp=631828846
input archive log thread=1 sequence=385 recid=3 stamp=631836006
input archive log thread=1 sequence=386 recid=4 stamp=631841192
input archive log thread=1 sequence=387 recid=5 stamp=631857698
input archive log thread=1 sequence=388 recid=6 stamp=631864632
input archive log thread=1 sequence=389 recid=7 stamp=631864633
input archive log thread=1 sequence=390 recid=8 stamp=631864638
input archive log thread=1 sequence=391 recid=9 stamp=631864640
input archive log thread=1 sequence=392 recid=10 stamp=631864641
input archive log thread=1 sequence=393 recid=11 stamp=631864643
input archive log thread=1 sequence=394 recid=12 stamp=631864644
input archive log thread=1 sequence=395 recid=13 stamp=631864646
input archive log thread=1 sequence=396 recid=14 stamp=631876887
```

```

input archive log thread=1 sequence=397 recid=15 stamp=631893181
input archive log thread=1 sequence=398 recid=16 stamp=631904513
input archive log thread=1 sequence=399 recid=17 stamp=631914562
input archive log thread=1 sequence=400 recid=18 stamp=631923600
input archive log thread=1 sequence=401 recid=19 stamp=631923713
channel ORA_DISK_1: starting piece 1 at 29-AUG-07
channel ORA_DISK_1: finished piece 1 at 29-AUG-07
piece handle=/u01/app/oracle/flash_recovery_area/AVAYAIQ/backupset/2007_08_29/
o1_mf_anno TAG20070829T222154_3fdkh44s_.bkp tag=TAG20070829T222154 comment=NONE
channel ORA_DISK_1: backup set complete, elapsed time: 00:00:09
Finished backup at 29-AUG-07
Starting backup at 29-AUG-07
using channel ORA_DISK_1
channel ORA_DISK_1: starting full datafile backupset
channel ORA_DISK_1: specifying datafile(s) in backupset
input datafile fno=00005 name=/u01/app/oracle/oradata/avayaiq/avayaiq
input datafile fno=00006 name=/u01/app/oracle/oradata/avayaiq/avayaiqdim
input datafile fno=00007 name=/u01/app/oracle/oradata/avayaiq/avayaiqfact1
input datafile fno=00008 name=/u01/app/oracle/oradata/avayaiq/avayaiqfact2
input datafile fno=00009 name=/u01/app/oracle/oradata/avayaiq/avayaiqfact3
input datafile fno=00010 name=/u01/app/oracle/oradata/avayaiq/avayaiqrpt
input datafile fno=00011 name=/u01/app/oracle/oradata/avayaiq/avayaiqsds
input datafile fno=00012 name=/u01/app/oracle/oradata/avayaiq/avayaiqrt
input datafile fno=00013 name=/u01/app/oracle/oradata/avayaiq/avayaiqrcl
input datafile fno=00002 name=/u01/app/oracle/oradata/avayaiq/undotbs01.dbf
input datafile fno=00001 name=/u01/app/oracle/oradata/avayaiq/system01.dbf
input datafile fno=00003 name=/u01/app/oracle/oradata/avayaiq/sysaux01.dbf
input datafile fno=00014 name=/u01/app/oracle/oradata/rmanrep/CATALOG_01
input datafile fno=00004 name=/u01/app/oracle/oradata/avayaiq/users01.dbf
channel ORA_DISK_1: starting piece 1 at 29-AUG-07
channel ORA_DISK_1: finished piece 1 at 29-AUG-07
piece handle=/u01/app/oracle/flash_recovery_area/AVAYAIQ/backupset/2007_08_29/
o1_mf_nnndf_TAG20070829T222203_3fdkhd23_.bkp tag=TAG20070829T222203 comment=NONE
channel ORA_DISK_1: backup set complete, elapsed time: 00:01:05
channel ORA_DISK_1: starting full datafile backupset
channel ORA_DISK_1: specifying datafile(s) in backupset
including current control file in backupset
including current SPFILE in backupset
channel ORA_DISK_1: starting piece 1 at 29-AUG-07
channel ORA_DISK_1: finished piece 1 at 29-AUG-07
piece handle=/u01/app/oracle/flash_recovery_area/AVAYAIQ/backupset/2007_08_29/
o1_mf_ncsnf_TAG20070829T222203_3fdkfxn_.bkp tag=TAG20070829T222203 comment=NONE
channel ORA_DISK_1: backup set complete, elapsed time: 00:00:02
Finished backup at 29-AUG-07

```

```
Starting backup at 29-AUG-07
current log archived
using channel ORA_DISK_1
channel ORA_DISK_1: starting archive log backupset
channel ORA_DISK_1: specifying archive log(s) in backup set
input archive log thread=1 sequence=402 recid=20 stamp=631923790
channel ORA_DISK_1: starting piece 1 at 29-AUG-07
channel ORA_DISK_1: finished piece 1 at 29-AUG-07
piece handle=/u01/app/oracle/flash_recovery_area/AVAYAIQ/backupset/2007_08_29/
o1_mf_annnn_TAG20070829T222311_3fdkkjrz_.bkp tag=TAG20070829T222311 comment=NONE
channel ORA_DISK_1: backup set complete, elapsed time: 00:00:02
Finished backup at 29-AUG-07
```

```
RMAN> exit
```

Recovery Manager complete.

Full backup of database and archive logs with archive log purge

The following command will perform a full backup of the database and archive log files. After the backup is complete, RMAN will delete the archive logs that have been backed up. Additionally, the current control files and SPFILE are stored as part of the backup set.

```
[oracle@rodbdb rmanrep]$ rman target=rman_user/password@avayaiq catalog=rcat_user/
password@rmanrep
```

```
Recovery Manager: Release 10.2.0.2.0 - Production on Wed Aug 29 22:21:28 2007
```

```
Copyright (c) 1982, 2005, Oracle. All rights reserved.
```

```
connected to target database: AVAYAIQ (DBID=353319860)
connected to recovery catalog database
```

```
<backup database and archive log and remove backed-up archive logs>
BACKUP DATABASE PLUS ARCHIVELOG delete INPUT;
```

RMAN incremental differential backup

Incremental backups are useful for backing up just the database blocks that have changed since the last incremental backup. With this approach each incremental backup is short in duration and you will never have to backup more than the previous incremental redo logs for recovery. However, recovery can take a long time as each incremental backup has to be restored. The following are benefits of using this option:

- Less backup media is used compared to full backups.
- Faster backup time.

- Less overall traffic load over the network compared to full backups.

To do an incremental differential backup:

1. Do a base incremental backup on day 1.

```
RMAN> backup incremental level=0 database;
```

2. Perform differential backups the remainder of your backup period, typically every day of the week.

```
RMAN> backup incremental level=1 database;
```

With this approach each incremental backup is short in duration and you will never have to do more than one day's worth of redo logs for recovery. However, recovery can take a long time if a system failure occurs just before your next full backup. If this occurs, you will have to apply your last full backup and then all incremental backups.

RMAN incremental cumulative backup

Another form of an incremental backup, the cumulative backup, accumulates all the changes that have occurred for all backup levels lower than the cumulative level specified. Restoring the database will be faster, but backup times are increased.

To do an incremental cumulative backup:

1. Do a base incremental backup on day 1.

```
RMAN> backup incremental level=0 database
```

2. Perform cumulative backups at regular intervals during your backup week. For example, you may do differential backups for two days followed by a cumulative backup on the third day.

```
RMAN> backup incremental level=1 cumulative database;
```

RMAN tablespace backup

To do an RMAN backup of the tablespaces, run commands as shown in the following example:

```
backup tablespace
backup tablespace HISTORICAL_TABLESPACE1 plus archivelog;
. . .
backup tablespace HISTORICAL_TABLESPACE10 plus archivelog;
```

Creating a cron job to schedule your full backup

After configuring RMAN and running successful backup scenarios manually, schedule a full online backup using the `cron` command. Consult your OS administrator and DBA for details on building scripts.

To create a cron job to schedule a backup:

1. Enter:

```
crontab -e
```

The `crontab` file is opened.

2. Enter commands to run scheduled backup jobs, similar to the following example:

```
# IQ Cron for Performing an Incremental Online Backup daily 23:59 (11:59pm), Monday
- Friday
59 11 * * 7 /tmp/full_online_dbbackup.sh 1> /tmp/full_backup_rman.$$log 2>&1
# IQ Cron for Performing an Full Online Backup daily 23:59 (11:59pm), Monday -
Friday
59 11 * * 1-5 /tmp/incremental_dbbackup.sh 1> /tmp/incremental_backup_rman.$$log
2>&1
```

This will run the cron job to execute the `full_online_dbbackup.sh` script at 59 minutes past the hour on Sunday, and an incremental backup Monday through Friday. However, if you want to override to specify different start times, different log locations, and so on, use `crontab -e` and modify accordingly. Use `man cron` for more information on options.

The following is an example of a full online backup script:

```
#!/bin/sh

export ORACLE_HOME=/u01/app/oracle/product/10.2.0/Db_1
export ORACLE_SID=avayaiaq

echo "$ORACLE_HOME/bin/rman target=rman_user/password catalog=rcat_user/
password@rmanrep @/tmp/backup.cmd"
$ORACLE_HOME/bin/rman target=rman_user/password catalog=rcat_user/password@rmanrep
@/tmp/backup.cmd
```

The following is an example of an incremental online backup script:

```
#!/bin/sh

export ORACLE_HOME=/u01/app/oracle/product/10.2.0/Db_1
export ORACLE_SID=avayaiq

echo "$ORACLE_HOME/bin/rman target=rman_user/password catalog=rcat_user/
password@rmanrep @/tmp/differential_backup.cmd"
$ORACLE_HOME/bin/rman target=rman_user/password catalog=rcat_user/password@rmanrep
@/tmp/differential_backup.cmd
```

Verifying backup sets

RMAN provides various options to validate backups and restores. You can list backup sets, validate backup sets, verify backup sets have been created in the specified location, and check the backup to see if it can be restored.

This section includes the following topics:

- [List backup set](#) on page 140
- [Validate backup set](#) on page 143
- [Verify backup sets have been created in the specified location](#) on page 144
- [Testing the backups for restores](#) on page 145

List backup set

This section shows an example of how you can list the backup set. This example assumes that that you have exported the SID. For example, enter the command:

```
export ORACLE_SID=<SID>

$ rman target=rman_user/<password> catalog=rcat_user/<password>

Recovery Manager: Release 10.2.0.2.0 - Production on Wed Aug 29 22:28:30 2007

Copyright (c) 1982, 2005, Oracle. All rights reserved.

connected to target database: AVAYAIQ (DBID=353319860)
connected to recovery catalog database

RMAN> list backupset;
List of Backup Sets
=====

BS Key   Size          Device Type Elapsed Time Completion Time
-----
360      753.59M      DISK        00:00:08      29-AUG-07
BP Key: 363   Status: AVAILABLE Compressed: NO   Tag: TAG20070829T222154
Piece Name: /u01/app/oracle/flash_recovery_area/AVAYAIQ/backupset/
2007_08_29/o1_mf_annnn_TAG20070829T222154_3fdkh44s_.bkp
```

List of Archived Logs in backup set 360

Thrd	Seq	Low SCN	Low Time	Next SCN	Next Time
1	383	13392436	28-AUG-07	13423437	28-AUG-07
1	384	13423437	28-AUG-07	13441384	28-AUG-07
1	385	13441384	28-AUG-07	13459680	28-AUG-07
1	386	13459680	28-AUG-07	13473296	28-AUG-07
1	387	13473296	28-AUG-07	13502826	29-AUG-07
1	388	13502826	29-AUG-07	13518597	29-AUG-07
1	389	13518597	29-AUG-07	13527114	29-AUG-07
1	390	13527114	29-AUG-07	13535672	29-AUG-07
1	391	13535672	29-AUG-07	13544196	29-AUG-07
1	392	13544196	29-AUG-07	13552713	29-AUG-07
1	393	13552713	29-AUG-07	13561201	29-AUG-07
1	394	13561201	29-AUG-07	13570008	29-AUG-07
1	395	13570008	29-AUG-07	13578528	29-AUG-07
1	396	13578528	29-AUG-07	13602449	29-AUG-07
1	397	13602449	29-AUG-07	13630767	29-AUG-07
1	398	13630767	29-AUG-07	13671715	29-AUG-07
1	399	13671715	29-AUG-07	13715594	29-AUG-07
1	400	13715594	29-AUG-07	13753676	29-AUG-07
1	401	13753676	29-AUG-07	13755414	29-AUG-07

BS Key	Type	LV	Size	Device	Type	Elapsed Time	Completion Time
361	Full		2.30G	DISK		00:01:03	29-AUG-07
BP Key: 364 Status: AVAILABLE Compressed: NO Tag: TAG20070829T222203							
Piece Name: /u01/app/oracle/flash_recovery_area/AVAYAIQ/backupset/							
2007_08_29/o1_mf_nnndf_TAG20070829T222203_3fdkhd23_.bkp							
List of Datafiles in backup set 361							

File	LV	Type	Ckp	SCN	Ckp Time	Name
1		Full	13755435		29-AUG-07	/u01/app/oracle/oradata/avayaiq/system01.dbf
2		Full	13755435		29-AUG-07	/u01/app/oracle/oradata/avayaiq/undotbs01.dbf
3		Full	13755435		29-AUG-07	/u01/app/oracle/oradata/avayaiq/sysaux01.dbf
4		Full	13755435		29-AUG-07	/u01/app/oracle/oradata/avayaiq/users01.dbf
5		Full	13755435		29-AUG-07	/u01/app/oracle/oradata/avayaiq/avayaiq
6		Full	13755435		29-AUG-07	/u01/app/oracle/oradata/avayaiq/avayaiqdim
7		Full	13755435		29-AUG-07	/u01/app/oracle/oradata/avayaiq/avayaiqfact1
8		Full	13755435		29-AUG-07	/u01/app/oracle/oradata/avayaiq/avayaiqfact2
9		Full	13755435		29-AUG-07	/u01/app/oracle/oradata/avayaiq/avayaiqfact3
10		Full	13755435		29-AUG-07	/u01/app/oracle/oradata/avayaiq/avayaiqrpt
11		Full	13755435		29-AUG-07	/u01/app/oracle/oradata/avayaiq/avayaiqsds
12		Full	13755435		29-AUG-07	/u01/app/oracle/oradata/avayaiq/avayaiqrt
13		Full	13755435		29-AUG-07	/u01/app/oracle/oradata/avayaiq/avayaiqrcl
14		Full	13755435		29-AUG-07	/u01/app/oracle/oradata/rmanrep/CATALOG_01

Routine maintenance

```
BS Key  Type LV Size      Device Type Elapsed Time Completion Time
-----
362     Full   6.80M      DISK        00:00:02      29-AUG-07
        BP Key: 365   Status: AVAILABLE Compressed: NO   Tag: TAG20070829T222203
        Piece Name: /u01/app/oracle/flash_recovery_area/AVAYAIQ/backupset/
2007_08_29/o1_mf_ncsnf_TAG20070829T222203_3fdkkfxn_.bkp
        Control File Included: Ckp SCN: 13755470      Ckp time: 29-AUG-07
        SPFILE Included: Modification time: 29-AUG-07
```

```
BS Key  Size      Device Type Elapsed Time Completion Time
-----
406     177.00K    DISK        00:00:01      29-AUG-07
        BP Key: 409   Status: AVAILABLE Compressed: NO   Tag: TAG20070829T222311
        Piece Name: /u01/app/oracle/flash_recovery_area/AVAYAIQ/backupset/
2007_08_29/o1_mf_annnn_TAG20070829T222311_3fdkkjrz_.bkp
```

List of Archived Logs in backup set 406

Thrd	Seq	Low SCN	Low Time	Next SCN	Next Time
1	402	13755414	29-AUG-07	13755473	29-AUG-07

RMAN> exit

Recovery Manager complete.

Validate backup set

This section shows an example of how you can validate the backup set for a subsequent restore. This example assumes that you have exported the SID (that is, from the command line, enter the command:

```
export ORACLE_SID=<SID>

$ rman target=rman_user/<password> catalog=rcat_user/<password>

Recovery Manager: Release 10.2.0.2.0 - Production on Wed Aug 29 22:31:33 2007

Copyright (c) 1982, 2005, Oracle. All rights reserved.

connected to target database: AVAYAIQ (DBID=353319860)
connected to recovery catalog database

RMAN> validate backupset 360;

allocated channel: ORA_DISK_1
channel ORA_DISK_1: sid=1051 devtype=DISK
channel ORA_DISK_1: starting validation of archive log backupset
channel ORA_DISK_1: reading from backup piece /u01/app/oracle/flash_recovery_area/
AVAYAIQ/backupset/2007_08_29/o1_mf_annnn_TAG20070829T222154_3fdkh44s_.bkp
channel ORA_DISK_1: restored backup piece 1
piece handle=/u01/app/oracle/flash_recovery_area/AVAYAIQ/backupset/2007_08_29/
o1_mf_annnn_TAG20070829T222154_3fdkh44s_.bkp tag=TAG20070829T222154
channel ORA_DISK_1: validation complete, elapsed time: 00:00:27

RMAN> exit

Recovery Manager complete.
```

Verify backup sets have been created in the specified location

This section shows an example of how you can verify that backup sets have been created in the specified location. This example assumes that you have exported the SID. For example, enter the command:

```
export ORACLE_SID=<SID>

$ ls -l /u01/app/oracle/flash_recovery_area/AVAYAIQ/backupset/2007_08_29
total 3190720
-rw-r----- 1 oracle oinstall 790194176 Aug 29 22:22
o1_mf_annnn_TAG20070829T222154_3fdkh44s_.bkp
-rw-r----- 1 oracle oinstall 181760 Aug 29 22:23
o1_mf_annnn_TAG20070829T222311_3fdkkjrz_.bkp
-rw-r----- 1 oracle oinstall 7143424 Aug 29 22:23
o1_mf_ncsnf_TAG20070829T222203_3fdkfxn_.bkp
-rw-r----- 1 oracle oinstall 2466545664 Aug 29 22:23
o1_mf_nnndf_TAG20070829T222203_3fdkhd23_.bkp

$ rman target=rman_user/<password> catalog=rcat_user/<password>

Recovery Manager: Release 10.2.0.2.0 - Production on Wed Aug 29 22:31:33 2007

Copyright (c) 1982, 2005, Oracle. All rights reserved.

connected to target database: AVAYAIQ (DBID=353319860)
connected to recovery catalog database

o RMAN>restore database validate

allocated channel: ORA_DISK_1
channel ORA_DISK_1: sid=1051 devtype=DISK
channel ORA_DISK_1: starting validation of archive log backupset
channel ORA_DISK_1: reading from backup piece /u01/app/oracle/flash_recovery_area/
AVAYAIQ/backupset/2007_08_29/o1_mf_annnn_TAG20070829T222154_3fdkh44s_.bkp
channel ORA_DISK_1: restored backup piece 1
piece handle=/u01/app/oracle/flash_recovery_area/AVAYAIQ/backupset/2007_08_29/
o1_mf_annnn_TAG20070829T222154_3fdkh44s_.bkp tag=TAG20070829T222154
channel ORA_DISK_1: validation complete, elapsed time: 00:00:27

RMAN> exit

Recovery Manager complete.
```

Testing the backups for restores

This section shows two examples of how you can test the database backup for a subsequent restore. This example assumes that you have exported the SID. For example, enter the command:

```
export ORACLE_SID=<SID>
```

```
Starting restore at 29-AUG-07
allocated channel: ORA_DISK_1
channel ORA_DISK_1: sid=1043 devtype=DISK

channel ORA_DISK_1: starting validation of datafile backupset
channel ORA_DISK_1: reading from backup piece /u01/app/oracle/flash_recovery_area/
AVAYAIQ/backupset/2007_08_29/o1_mf_nnndf_TAG20070829T222203_3fdkhd23_.bkp
channel ORA_DISK_1: restored backup piece 1
piece handle=/u01/app/oracle/flash_recovery_area/AVAYAIQ/backupset/2007_08_29/
o1_mf_nnndf_TAG20070829T222203_3fdkhd23_.bkp tag=TAG20070829T222203
channel ORA_DISK_1: validation complete, elapsed time: 00:00:56
Finished restore at 29-AUG-07

RMAN> exit
```

Recovery Manager complete.

```
$ rman target=rman_user/<password> catalog=rcat_user/<password>
```

Recovery Manager: Release 10.2.0.2.0 - Production on Wed Aug 29 22:31:33 2007

Copyright (c) 1982, 2005, Oracle. All rights reserved.

```
connected to target database: AVAYAIQ (DBID=353319860)
connected to recovery catalog database
```

```
RMAN> restore database check logical validate;
```

```
Starting restore at 29-AUG-07
using channel ORA_DISK_1
```

```
channel ORA_DISK_1: starting validation of datafile backupset
channel ORA_DISK_1: reading from backup piece /u01/app/oracle/flash_recovery_area/
AVAYAIQ/backupset/2007_08_29/o1_mf_nnndf_TAG20070829T222203_3fdkhd23_.bkp
channel ORA_DISK_1: restored backup piece 1
piece handle=/u01/app/oracle/flash_recovery_area/AVAYAIQ/backupset/2007_08_29/
o1_mf_nnndf_TAG20070829T222203_3fdkhd23_.bkp tag=TAG20070829T222203
channel ORA_DISK_1: validation complete, elapsed time: 00:00:45
Finished restore at 29-AUG-07
```

```
RMAN> exit
```

Recovery Manager complete.

Cleaning up user accounts

Before users are removed from Avaya IQ (either from User Management or the Enterprise Directory), you must first clean up the user's account. If this is not done, a user's scheduled reports or scheduled administration jobs could use up a lot of system processing time and waste storage space.

To clean up user accounts:

1. Prior to deleting the user from the enterprise directory or from the Common User Service directory (via User Management administration), change the user's password.
2. Log in to reporting as the user using the new password.
3. Clean up the user's **My Folders** directories, including any scheduled report jobs. If there are custom reports (report definitions) of value, copy these to the **Custom Reports** folder and then to your own **My Folders** directory. Delete all of the user's scheduled jobs.
4. Log in to administration as the user using the new password.
5. Clean up any scheduled jobs created by the user. Make sure the scheduled job is not needed by any other users or the system.
6. Once the user's jobs and folders are cleaned up, the user can be deleted from the enterprise directory or from the Common User Service directory. See [Deleting users](#) on page 37 in *Avaya IQ Administration*.

About licensing

Licensing ensures that customers are permitted to use only the product functionality for which they have paid and are licensed. License files for Avaya IQ are generated and acquired using the Avaya Remote Feature Activation (RFA) process and installed using the Web License Manager (WebLM) tool. See [Acquiring and installing license files](#) on page 148.

The features licensed for Avaya IQ include:

- Number of concurrent agents
- Number of concurrent report users
- Number of concurrent Report Designer users (custom report creators)
- Number of Communication Manager data sources
- Number of Proactive Contact data sources
- Historical data export package
- Real-time data export packages

- Data import

Licensing is enforced in the following manner:

- On initial start-up, the system checks for the existence of a valid license file. During normal operation, whenever a licensed feature is accessed or an attempt is made to acquire a licensed resource, license management verifies that a license is available.
- If no valid license file exists, the installed product name does not match the licensed name, the license has expired, or the product version is older than the version specified in the license file, a CRITICAL alarm is raised and all subsequent license requests are denied.
- If an expected licensed feature is not found in the license file, the license request is denied.
- During normal operation, if a feature that uses licensing subsequently determines that the license server is unavailable, a 30 day grace period is initiated and a MINOR alarm is raised daily as long as the grace period is in effect. If the grace period is in effect and the condition that caused the grace period to start is resolved, the grace period alarm is cleared, and no further alarms are raised until a new alarmable condition is encountered.
- When the license file expiration date falls within 30 days of the current date, a MINOR alarm is raised daily to warn that the license file will expire soon.
- When the grace period expires, a CRITICAL alarm is raised and all data source connections (Communication Manager and Proactive Contact) are stopped.
- When the license file expires, a CRITICAL alarm is raised and all data source connections (Communication Manager and Proactive Contact) are stopped.
- Data source licenses are allocated only when you associate a data source with a host. You can create as many data sources as you want, but a license is only counted when the association is made.
- When an agent state changes from logged out to logged in, a license for that agent is acquired. When an agent's state changes from logged in to logged out, the license for that agent is released. When the link to a data source goes down, licenses are released. Unused licenses are released every 5 minutes.
- If a license cannot be acquired for an agent after three consecutive requests every 5 minutes, a MINOR alarm is generated. However, the agent will be recognized as being logged in and data will be tracked for that agent.
- If no valid license file is available, attempts to add a data source (Communication Manager or Proactive Contact) will fail and display an error to the user. Administration to add a site and a host is permitted.
- Prior to establishing a connection to a Communication Manager or Proactive Contact data source, a request is made to acquire a license. If the license cannot be acquired, a MAJOR alarm is raised but the connection is established anyway. However, if license renewal fails, the connection is stopped.

- When a data export API session is created, the license for the data export feature will be queried. If the feature is on, the operation will be permitted. If the feature is off, an error will be returned to the API user indicating that the feature has not been purchased.

Acquiring and installing license files

Installing a license file consists of two distinct procedures:

- [Acquiring a license file](#) on page 148
- [Installing a license file](#) on page 149

Acquiring a license file

Licensing ensures that customers are permitted to use only the product functionality for which they have paid and are licensed. License files for Avaya IQ are generated and acquired using the Avaya Remote Feature Activation (RFA) process and installed using the Web License Manager (WebLM) tool.

To acquire a license file, an Avaya or BusinessPartner representative uses the RFA feature. The Avaya employee or BusinessPartner must be certified to use the RFA feature. For information about RFA training, certification, and how to acquire a license file, see the following documents:

- Remote Feature Activation (RFA) User Guide
- Getting Started with Remote Feature Activation (RFA)

These documents can be found on the Avaya support site:

<http://support.avaya.com>

To acquire a license file, you must provide the following information to the Avaya or BusinessPartner representative:

- Host ID (MAC address or HWaddr) of the host where the All Functions or Administration host function will be installed. This host is where WebLM will be installed, and it is the only host where the license file is installed. You can use the Linux `ifconfig` command to display the Host ID.
- SAP order number
- BusinessPartner Tier I and Tier II information, if applicable
- Customer contact information

Download the license file to a PC that will be used to access the WebLM tool. The PC must have Web access to the host designated as the All Functions host or the Administration host.

Installing a license file

To install a license file on a host that has been administered or is expected to be administered with the All Functions or Administration host function:

1. From the PC where you have the license file, open a Web browser and enter:

`https://administration_host:8443/WebLM/`

where *administration_host* is the name of the host administered with All Functions or Administration. The WebLM login dialog is displayed.

2. Log in with the **admin** login ID and password.

Note:

The initial password is **weblmadmin**. The first time you access WebLM, you must change the initial password before you continue.

3. Select **Login**.

The Install License dialog is displayed.

4. Select **Browse** to locate the license file.

The Choose File dialog is displayed.

5. Browse through the filesystem on the PC to select the license file.

6. When the license file is displayed, select **Install** to install the license file.

7. After the license is installed, you must stop and restart the Tomcat services. Enter the following commands:

```
cd /opt/coreservices/lifecycle/bin
./lc ls
```

The list of services are displayed. Look for the AdminTomcat service as shown in the following example.

```
. . .
. . .
0789d6d511539d260111539d49910007 : AdminTomcat : STARTED
. . .
. . .
```

8. For the AdminTomcat service, enter:

```
./lc stop UUID
./lc start UUID
```

where *UUID* is the 32 character string shown in the display for the AdminTomcat service. Repeat this step for every service that is not started.

Maintaining license files

To maintain your license file, you may need to do any of the following procedures.

- [Checking status of a license](#) on page 150
- [Replacing a license file](#) on page 150

Checking status of a license

You can check the status of a license. The status includes the expiration date, the quantity of licensed features, the quantity of features currently acquired on the system, and the peak usage for measured features. For example, if you are licensed for 400 agents, the license status will show the current number of agents that have acquired a license.

To check the status of a license:

1. Open a Web browser and enter:
`https://administration_host:8443/WebLM/`
where `administration_host` is the name of the host administered with All Functions or Administration. The WebLM login dialog is displayed.
2. Log in with the `admin` login ID and password.
The Install License dialog is displayed.
3. Under **Licensed Features**, select **Avaya IQ**.
The status of the licensed features is displayed.
4. To display the peak usage for measured features, select **View Peak Usage**.
The peak usage for the measured features is displayed.

Replacing a license file

To replace a license file on the All Functions or Administration host:

1. Acquire a new license file. Follow the procedures in [Acquiring a license file](#) on page 148.
2. From the PC where you have the license file, open a Web browser and enter:

`https://administration_host:8443/WebLM/`

where `administration_host` is the name of the host administered with All Functions or Administration. The WebLM login dialog is displayed.

3. Log in with the **admin** login ID and password.
The Install License dialog is displayed.
4. Select **Uninstall License**.
The Uninstall License dialog lists the licenses installed on this system.
5. Select the installed license from the list and select **Uninstall**.
6. Select **Install License**.
The Install License dialog is displayed.
7. Select **Browse** to locate the new license file.
The Choose File dialog is displayed.
8. Browse through the filesystem on the PC to select the license file.
9. When the license file is displayed, select **Install** to install the license file.
10. After the license is installed, you must stop and restart the Tomcat services. Enter the following commands:


```
cd /opt/coreservices/lifecycle/bin
./lc ls
```

The list of services are displayed. Look for the AdminTomcat service as shown in the following example.

```
. . .
. . .
0789d6d511539d260111539d49910007 : AdminTomcat : STARTED
. . .
. . .
```

11. For the AdminTomcat service, enter:


```
./lc stop UUID
./lc start UUID
```

where *UUID* is the 32 character string shown in the display for the AdminTomcat service. Repeat this step for every service that is not started.

Installing updates

You should regularly check for product updates, security updates, and security advisories at the Avaya support Web site:

<http://support.avaya.com/download>

Install any required updates to the installed version of the software. Installation instructions are provided with every update. Before you install an update, you should back up your system as described in the following sections:

- [Backup strategies](#) on page 114
- [Backing up Avaya IQ data](#) on page 116
- [Backing up the operating system](#) on page 117
- [Backing up the database](#) on page 117

Editing properties

All processing elements within Avaya IQ have many editable property values. These property values control all facets of how the processing elements communicate with other elements. Most of the properties should never require changes. Any properties that do require changes are documented in specific procedures within the Implementation and Administration topics. Any other property editing should be done by qualified Avaya or BusinessPartner personnel.

Changing the reporting email server

When your system was installed, an email server was administered to email reports to users. If your email server or user changes, you can reassign a different email server or user.



CAUTION:

Change your email options during low or no traffic periods. To make this change, you have to stop and restart an Avaya IQ process for the change to take effect.

To change the email options:

1. Log in to the administration interface.
2. Under the **Enterprise** tab, select **Sites > HostSites > HostName**, where **HostSites** is the name of your sites and **HostName** is the name of your All Functions or Reporting hosts.
The Subsystem/Process dialog is displayed.
3. Expand the **Real Time Report Execution** subsystem.
The **Reporting JBoss** container is displayed.
4. Select the **Reporting JBoss** container.
The **Reporting JBoss** container dialog is displayed.
5. Select the **PE Real Time Report Service** process.

6. Select **Edit**.

The Edit Container dialog is displayed.

7. Scroll down to the email server and user options.

8. Change the server and user options as shown in the following description:

- **Email Server Name** - This is the name of the customer's SMTP email server. This server is used to deliver reports saved to email for report users. During host administration on an All Functions or Reporting host, you must define an email account from which Avaya IQ reports are mailed to Avaya IQ report users. This email account should be created (or can already exist) on a customer email server that supports SMTP mail service. The name of the account is not important, but the customer may want to create a special account so that report users can recognize that email from that account will be Avaya IQ reports. This email account cannot be created on an Avaya IQ host because Avaya IQ hosts do not support SMTP operation.
- **Email Port** - This is the SMTP port number used to communicate with the email server. The default value is 25. Change this value if your email server uses a different SMTP port.
- **Email User Name** - This is a non-privileged user on the SMTP email server. An email user is only required if the SMTP server requires authentication in order to send email.
- **Email User Password** - This is the password for the email user. You must reenter the password to verify that you entered the password correctly, but no checks are made to confirm that the user and password are valid for the email server.

9. Select **OK**.

The Reporting JBoss container dialog is displayed.

10. Log in to the OS with your root login and password.

11. Enter:

```
/opt/coreservices/lifecycle/bin/lc ls
```

The list of services are displayed. This example shows the Reporting JBoss container.

```
List of services :
```

```
.
.
0789d6d511239d31011123bb8c100103 : ReportingJBoss : STARTED
0789d6d511239d31011123bb902c0107 : PERealTimeReportService : STARTED
.
.
```

12. Enter:

```
./lc stop UUID  
./lc start UUID
```

where *UUID* is the 32 character string shown in the display for the Reporting JBoss container.

13. Repeat Step 11 to verify that the Reporting JBoss container restarts. You might have to wait a few minutes for the container to restart.
14. Repeat this procedure for all Reporting hosts.
15. Run a test report and verify that the new email service is working.

Changing the reporting host used for aggregation

If your configuration uses two reporting hosts, aggregation runs on only one of those hosts. When your system was installed, the first reporting host that was administered is automatically assigned as the host to run aggregation. If you want to change which host runs aggregation, use the procedure shown in this section. The only reason to change the aggregation host is if one host is out of service or the host is being replaced.



CAUTION:

Change your aggregation host during low or no traffic periods. To make this change, you have to stop and restart Avaya IQ for the change to take effect.

To change the aggregation host:

1. Log in to the administration interface.
2. Under the **Enterprise** tab, select **Sites > HostSites > HostName**, where **HostSites** is the name of your sites and **HostName** is the name of your All Functions or Reporting hosts.
The Subsystem/Process dialog is displayed.
3. Expand the **Historical Data Consolidation** subsystem.
The related processing elements are displayed.
4. Highlight the **PE Aggregation** processing element.
5. Select **Edit**.
The Edit Processing Element dialog is displayed.
6. Scroll down to the aggregation IP address and port options.
7. Change the IP address of the new Reporting host where you want to run aggregation. Do not change the default port number of 9300.

8. Select **OK**.

The Subsystem/Process dialog is displayed.

9. Log in to the OS with your root login and password.

10. Enter:

```
/opt/coreservices/lifecycle/bin/lc ls
```

The list of services are displayed. This example shows the aggregation processing element.

```
List of services :  
  
.  
0789d6d517eba29c0117ebe7c0d5008a : PEAggregation : STARTED  
.
```

11. Enter:

```
./lc stop UUID
```

```
./lc start UUID
```

where *UUID* is the 32 character string shown in the display for the aggregation processing element.

12. Repeat Step 10 to verify that the processing element restarts. You might have to wait a few minutes for the processing element to restart.

Adjusting parameters for communication with Proactive Contact cron jobs

If you change Proactive Contact maintenance cron jobs or decrease the wait recovery time for cron jobs from the default of 67 minutes to a different value, the PCAdapter processing element parameters on Avaya IQ may need adjustments to better communicate with the Proactive Contact jobs. If this situation occurs, use the procedure in this section to adjust the processing element parameters. These changes are made using the administration interface.

To adjust the PCAdapter parameters for Proactive Contact cron jobs:

1. Under the **Enterprise** tab, select **Sites >SiteName > HostName**.
2. Expand the **Data Collection** subsystem.
3. Highlight the **PE PC Adapter** associated with the Proactive Contact system where the cron jobs were changed.

4. Locate the **Maximum Bad Callbacks** option (the default is 100). This value is the counter for number of bad callbacks. If a connection is lost, the bad callback counter is incremented up to the maximum value (every 40 seconds). If the maximum value is reached, then the PCAdapter will go into a Restart state. You can set this value to 20 to decrease the wait time for recovery.

If you modify the **Maximum Bad Callbacks** option to a value less than 100, it is recommended that you modify the delay time for login. To do this, you will edit the **StateMachineConfig.xml** file located in `/opt/Avaya/CCR/data/eventmgt/XML`. The file and directory will be located on the application host where PCAdapter is running.

1. Enter:

```
cd /opt/Avaya/CCR/data/eventmgt/XML
```

2. Enter:

```
vi StateMachineConfig.xml
```

3. Search for **State Key="Logging In"**.

4. Within this state definition, change the following values:

```
<ActionRetryCount>10</ActionRetryCount> to <ActionRetryCount>60</ActionRetryCount>
```

```
<DelayBetweenRetriesInMSeconds>20000</DelayBetweenRetriesInMSeconds> to  
<DelayBetweenRetriesInMSeconds>120000</DelayBetweenRetriesInMSeconds>
```

This change will ensure that the Proactive Contact system has time to initialize its own services before the PCAdapter attempts to log in.

Loading date and time zone data

To properly display report data, you must add date and time zone data to your configuration. This data must be loaded on an All Functions host in a Dual Host deployment or on an Administration host in a multiple host deployment. Loading date and time zone data populates the date time values into the historical and real-time databases.

If your contact is centrally located, that is, all of your agents are in one location, you should only load a single time zone that represents that location. If your contact center is distributed, that is, your agents are spread across several locations, you should load time zone for each of your locations where you have agents.

The command used to load this data is named `dtzcli`. This command loads date and time zone data for any available time zone. By default, the command loads 3 months of time zone data for the historical schema and 4 hours of time zone data for the real-time schema. During implementation, the UTC time zone is loaded with 10 days of data for the historical schema and one hour of data for the real-time schema. This gives you enough time zone data to run test reports during implementation.

Since there are more than 500 time zones for which you can load data, you should only load the time zones for which you want reports. For example, if your users require reports for U.S. Eastern time, U.S. Pacific time, and Central European time, you only need to load data for those time zones. If in the future you need to add more date and time zone data, you can always load additional time zones.

Note:

The start times set by the `dtzcli` command have nothing to do with the start times for reports.

This section includes the following topics:

- [Date and time zone command options](#) on page 157
- [Using the date and time zone command](#) on page 158

Date and time zone command options

The date and time zone command has the following options:

List available time zones: This option provides a listing of all available time zone definitions. You will notice that one location may have more than one time zone definition. For example, if you need to report on agents located in Chicago, Illinois, USA, you can load any of the following time zones:

- America/Chicago
- Etc/GMT-6
- US/Central

Select the time zone that best matches the name of the reporting location. In this example, it would be most logical to use the time zone definition named America/Chicago.

List administered time zones: This option lists the time zones that are currently loaded on the system. If a time zone is currently loaded and active, do not attempt to reload the time zone.

Add a new time zone: This option allows you to add new time zone data. To add new time zone data, you need the following information:

- Time zone ID

This is the time zone ID as displayed when you use the `?` option. You must enter the time zone ID exactly as it is shown in the list of available time zone IDs.

- Time zone prompt

This is the time zone prompt as you want it to display in report input pages and on reports. Avaya recommends that you select a prompt name that report users will easily understand.

- Historical schema and range of dates

This determines if you load time zone data for the historical schema and how much data will be loaded. You can change the amount of data by specifying a different range of dates.

- Real-time schema

This determines if you load time zone data for the real-time schema.

Activate a time zone: This option allows you to activate a time zone that is currently deactivated. Time zone data is automatically extended for all active time zones.

Deactivate a time zone: This option allows you to deactivate a time zone. If you are not running any reports for a time zone, you can save space in the database by deactivating a time zone.

Extend time zone data forward: This option allows you to extend the time zone data for 3-5 months for the historical schema and 4 hours for the real-time schema. This option extends the time zone data for all administered time zones. Before you use this option, stop any scheduled time zone extension programs by editing the `crontab` file (`crontab -e`) and comment out the time zone programs. Remember to change the `crontab` file back after extending the time zone data.

Extend time zone data backward: This option allows you to extend the time zone data for the historical schema to a specific date in the past. This option extends the time zone data for all administered time zones. Before you use this option, stop any scheduled time zone extension programs by editing the `crontab` file (`crontab -e`) and comment out the time zone programs. Remember to change the `crontab` file back after extending the time zone data.

Quit: This option takes you out of the command.

Using the date and time zone command

To load date and time zone data:

1. Log on to the OS as root.
2. Maximize the size of your terminal window. Because the list of available time zones are displayed in three columns, you can sometimes miss the display of all time zones unless you use a large terminal window.
3. Enter:

```
cd /opt/Avaya/CCR/bin
```

4. Enter:

```
./dtzcli.sh
```

A list of command options is displayed.
5. Select an option from the list.
6. Answer the prompts based on the option descriptions in [Date and time zone command options](#) on page 157.
7. Repeat this procedure for all time zones you need to load.

Verifying date, time, and NTP status

You should verify that the date and time are synchronized on all hosts in the deployment. Verify that NTP is operating correctly on all hosts and sources in the deployment.

Changing the database user names or passwords

Avaya IQ communicates to the database with user names and passwords created when the database was installed and when Avaya IQ was installed. The database user names and passwords were created on the database and that information was configured on Avaya IQ. If the database user names or passwords are changed on the Avaya IQ host, they must be changed on the database host. Conversely, if the database user names or passwords are changed on the database host, you must update the user names or passwords on the Avaya IQ host. This section has procedures you must use to remedy the following conditions when the user names or passwords are mismatched:

- The password for the SDS (core) database user was changed manually or expired on the database host. When this happens, the administration interface cannot properly communicate with the database, and you cannot fix any other expired database passwords.
- The remaining database user names or passwords are changed manually on the Avaya IQ host or changed manually on the database host. When this happens, you must update the user names or passwords on the associated Avaya IQ or database host.

Use the following procedures to remedy both of these conditions:

- [Changing the SDS password on Avaya IQ](#) on page 160
- [Changing a user name or password on Avaya IQ](#) on page 161



Important:

Avaya recommends that you not change database user names. If you must change a user name, have an experienced DBA make the change.



CAUTION:

When you change the database user or password, there will be a period of time when Avaya IQ cannot communicate with the database. Coordinate the timing of the change so that you make the change on one host and then on the other host.

Changing the SDS password on Avaya IQ

To update the SDS (core) database user's password on Avaya IQ after the password has expired or was first changed on the database host:

1. Log on to the OS on your All Functions or Administration host.
2. Use the following commands to recreate the database user that existed when the system was first installed:

```
service wdinit stop
```

```
cd $CCR_HOME/data/install
```

```
./runBootstrapDB.sh -dbUser UserName -dbPassword Password
```

The variable *UserName* is the SDS (core) connection name and *Password* is the user's password.

3. Use the following SQL commands to delete the existing SDS (core) database service connection pool:

```
delete from sdproperty where propcntnrid in (select propcntnrid
      from sdpropcntnr where entitytype = 'SDResource' and entityname =
      'core');
```

```
delete from sdpropcntnr where entitytype = 'SDResource' and
      entityname = 'core';
```

```
delete from sdresource where name = 'core';
```

4. Use the following commands to recreate the SDS (core) database service connection pool:

```
cd $CCR_HOME/data/install

./runDBResource.sh -resName core -dbProduct Oracle
                  -dbConnectionString DB_Connection_String -dbUser DB_user
                  -dbPassword DB_password -dbSchemaName DB_Schema_Name
                  -dbSchemaOwner DB_Schema_Owner -dbPoolSize 32
```

For example:

```
./runDBResource.sh -resName core -dbProduct Oracle
                  -dbConnectionString jdbc:oracle:thin:@dill.dr.avaya.com:1521:ccr
                  -dbUser ccrsds -dbPassword xxxxx -dbSchemaName ccrsds
                  -dbSchemaOwner ccrsds -dbPoolSize 32
```

The output of this command can be found in `$CCR_HOME/install_logs/config.log`.

5. Use the following command to restart the system:


```
service wdmnit start
```
6. Verify that the Tomcat process is running:


```
ps -ef | grep tomcat
```
7. If you need to change any other database user names or passwords, use the procedure in [Changing a user name or password on Avaya IQ](#) on page 161.

Changing a user name or password on Avaya IQ

Important:

Do not use this procedure if the SDS (core) database user name or password has first changed on the database host. Use the procedure found in [Changing the SDS password on Avaya IQ](#) on page 160.

To change a non-SDS (core) database user or password on an Avaya IQ host first and then on the database host:

1. Log on to the OS on your All Functions or Administration host.
2. Test the database connection using the following procedure before making any changes:
 - a. Enter:


```
sqlplus IQ_Connection_Name/
        IQ_Connection_Name_DB_Pwd@DB_User_Machine
```

 Example: `sqlplus iq/password@dbhost`
 - b. To exit SQL Plus, enter:


```
exit
```

3. Log in to the administration interface of Avaya IQ.
4. Under the **Tasks** tab, select **Connection Management > Administer Connections**.
The All Connection Types dialog is displayed.
5. Select **Database Connection**.

The Connection Resources dialog is displayed. The list of database names displayed in this dialog correspond as shown in the following table:

Avaya IQ OAM Connection name	Oracle database user name	Database name
CCR	CCR	RPT_HIST_OWNER_USR
CCRCSC	CCRRPT	RPT_CONTENT_USR
CCRR	CCR	RPT_HIST_RO_USR
CCRRT	CCRRT	RPT_RT_USR
CCRUI	CCRRCL	RPT_UI_USR
CCRW	CCR	RPT_HIST_RW_USR
core	CCRSDS	RPT_SDS_USR

Note:

In some installations, the same database user was associated with the CCR, CCRR, and CCRW connection names. If the password changed on the database host for any one of these database users, you must change the password for all three connection names CCR, CCRR, and CCRW on the Avaya IQ host.

6. Highlight one of the connection names.
7. Select **Edit**.
The Edit Resource dialog is displayed.
8. Scroll down in the dialog and find the **User Name** and **User Password** fields. Change these options as needed.
9. Select **Apply**.
10. Select **OK**.

The Connection Resources dialog is displayed.

Note:

If the password for SDS (core) is being changed on the Avaya IQ first, you must immediately log out of administration, shut down the All Functions or Administration host immediately, and run an Oracle script. To do this, enter the following commands:

```
service wdinit stop
cd $CCR_HOME/data/install
./runBootstrapDB.sh -dbUser UserName -dbPassword Password
```

The variable *UserName* is the core connection name and *Password* is the user's password.

11. Log on to the OS on your All Functions or Administration host.
12. Use the following command to shut down the host, if not already shut down:


```
service wdinit stop
```

If you have a multiple host configuration, shut down all hosts in the configuration using this same command. Verify that all hosts are shut down.
13. Log in to your database host and change the database password for the user changed in the previous steps. Use the table above to find the Oracle database user associated with the Avaya IQ user just changed. If the account is locked, log in as sysdba and unlock the account.
14. Log on to the OS on your All Functions or Administration host.
15. Use the following command to restart the host:


```
service wdinit start
```

If you have a multiple host configuration, restart all hosts in the configuration using this same command. Verify that all hosts are restarted.
16. When Avaya IQ has restarted on all hosts, confirm that the system can communicate with the database. Test the database connection using the following procedure:
 - a. Enter:


```
sqlplus IQ_Connection_Name/
IQ_Connection_Name_DB_Pwd@DB_User_Machine
```

Example: `sqlplus iq/password@dbhost`
 - b. To exit SQL Plus, enter:


```
exit
```
17. Repeat this procedure for any other non-SDS (core) database user names or passwords that require changes.

Database management

Avaya IQ buffers events from data sources if there is a problem with the system. For example, if the database is currently unavailable, the system should be able to buffer for a short time given the buffer configuration administrated during install. During such outages, buffering will continue until maximum capacity. Typically a "Threshold exceeded" notification log message is given prior to reaching buffer capacity. This message is available in the log file of the host system for the Data Processing Container or available through the Log Viewer. In addition, once capacity is reached, an Alarm is generated indicating "Persistence store has reached its limit." This message will also be available in the Log Viewer and the Alarm Manager. To prevent loss of events from data sources, your DBA needs to investigate ways to make the disk I/O operate faster.

- Use the management tools provided by your database software provider.
- Follow the recommendations provided by your database software provider.
- Monitor your tablespace usage to ensure that you have enough space.

Avaya IQ buffers events from data sources if there is a problem with the system. For example, if the database is currently unavailable, the system should be able to buffer for a short time given the buffer configuration administrated during install. During such outages, buffering will continue until maximum capacity. Typically a "Threshold exceeded" notification log message is given prior to reaching buffer capacity. This message is available in the log file of the host system for the Data Processing Container or available through the Log Viewer. In addition, once capacity is reached, an Alarm is generated indicating "Persistence store has reached its limit." This message will also be available in the Log Viewer and the Alarm Manager. To prevent loss of events from data sources, your DBA needs to investigate ways to make the disk I/O operate faster.

Data removal

The Avaya IQ data model is based on standard data warehouse design principles. Administered entities, such as agents, queue groups or routing point groups, are stored in dimension tables. Measurements on those entities, such as contact counts, time durations, and so forth, are stored in fact tables. Fact tables generally store significantly more data than the dimension tables. Data removal is designed to remove data only from the database fact tables.

On a regular basis, you should remove unneeded fact table data from your database. The `fact_data_purge` command does this for you. You can remove old data from all fact tables at the same time or you can remove data from individual fact tables one at a time.

The `fact_data_purge` command deletes data for the date you enter and any data older than that date. For example, if you enter 11/12/2005 in the command, all fact table data for November 12, 2005, and earlier will be removed.



CAUTION:

Only remove data for which you no longer wish to run reports. Do not remove data you need for reports.

To remove data from all fact tables:

1. Connect to the database so you can run database commands.

2. Enter:

```
/opt/Avaya/CCR/bin/fact_data_purge.sh MM/DD/YYYY
```

where **MM** is the two-digit month, **DD** is the two-digit day, and **YYYY** is the four-digit year of the date.

3. The data is deleted from all fact tables.

To remove data from a single fact table:

1. Connect to the database so you can run database commands.

2. Enter:

```
/opt/Avaya/CCR/bin/fact_data_purge.sh MM/DD/YYYY fact_table
```

where **MM** is the two-digit month, **DD** is the two-digit day, **YYYY** is the four-digit year of the date, and **fact_table** is the individual fact table.

3. The data is deleted from the specified fact table.

Database schema and metadata sanity check

To verify consistency between the database schema information of the historical report tables and the metadata records, a sanity check is done automatically every day. If an inconsistency is found, an alarm is raised, and the inconsistency is logged in the Scheduler container log files located at:

```
/var/log/Avaya/CCR/SCHED_UUID/
```

The **UUID** variable represents a dynamically generated container UUID directory. The name preceding the UUID identifies the container function. In this case it is the Scheduler container.

The following is an example of a Scheduler container UUID directory:

```
SCHED_0789038d09d500320109d50323b70003
```

Depending on the error, you may need assistance from Avaya. For inconsistencies such as dropped tables, your database administrator can add those tables back into the database. For errors in the metadata, you must contact Avaya for assistance.

Reinitializing user service

To reinitialize user service:

1. Under the **Tasks** tab, select **System Configuration > Manage Administrative Data > Reinitialize User Service**.
2. Select **Reinitialize**.

Editing the service configuration

For Avaya IQ Release 4.1, this feature is not being used.

Managing distributors

For Avaya IQ Release 4.1, this feature is not being used.

Managing trusted certificates

Avaya IQ allows you to add, import, export, and delete security certificates. Certificates are used to help guarantee users that they are accessing a valid site and that their communications with the site will be treated securely. For example, certificates can be installed on each Administration and Reporting host to provide a valid certificate for all administration and reporting users.

This section includes the following topics:

- [Listing server certificates](#) on page 167
- [Viewing pending certificates](#) on page 169
- [Default server certificate settings](#) on page 170
- [Listing trusted certificates](#) on page 170
- [JKS synchronization](#) on page 172

Listing server certificates

To list server certificates:

1. Under the **Tasks** tab, select **Security > Administer Server Certificates**.
The Server Certificates dialog is displayed. The server certificates are listed in this dialog.
2. From this dialog, you can do any of the following procedures:
 - [Viewing server certificates](#) on page 167
 - [Adding server certificates](#) on page 167
 - [Importing server certificates](#) on page 168
 - [Exporting server certificates](#) on page 168
 - [Deleting server certificates](#) on page 169

Viewing server certificates

To view server certificates:

1. Under the **Tasks** tab, select **Security > Administer Server Certificates**.
The Server Certificates dialog is displayed.
2. Select the host for which you want to view the server certificates.
3. Select **Switch To**.
The certificates for the host are displayed.
4. Select the certificate you want to view.
5. Select **View**.
The Server Certificate Details dialog is displayed.
6. Select **Close**.
The Server Certificates dialog is displayed.

Adding server certificates

To add a server certificate:

1. Under the **Tasks** tab, select **Security > Administer Server Certificates**.
The Server Certificates dialog is displayed.
2. Select the host for which you want to add a server certificate.

3. Select **Switch To**.
The certificates for the host are displayed.
4. Select **Add**.
The Add Server Certificate dialog is displayed.
5. Complete the data fields required to create the server certificate.
6. Select **Apply**.
The Server Certificates dialog is displayed showing the new certificate.

Importing server certificates

To import a server certificate:

1. Under the **Tasks** tab, select **Security > Administer Server Certificates**.
The Server Certificates dialog is displayed.
2. Select the host for which you want to import a server certificate.
3. Select **Switch To**.
The certificates for the host are displayed.
4. Select **Import**.
The Server Certificate Import dialog is displayed.
5. Enter a name into the **Certificate Alias** field.
6. Select **Establish Chain of Trust** if applicable.
7. Paste the content of the server certificate into the **Certificate PEM** data field.
8. Select **Apply**.
The Server Certificates dialog is displayed showing the new certificate.

Exporting server certificates

To export a server certificate:

1. Under the **Tasks** tab, select **Security > Administer Server Certificates**.
The Server Certificates dialog is displayed.
2. Select the host for which you want to export a server certificate.
3. Select **Switch To**.
The certificates for the host are displayed.

4. Select **Export**.
The Server Certificate Export dialog is displayed.
5. Copy the content of the **Certificate PEM** data field to a text editor so you can save the certificate to another system.
6. Select **Close**.

Deleting server certificates

To delete a server certificate:

1. Under the **Tasks** tab, select **Security > Administer Server Certificates**.
The Server Certificates dialog is displayed.
2. Select the host for which you want to delete a server certificate.
3. Select **Switch To**.
The certificates for the host are displayed.
4. Select **Delete**.
A confirmation dialog is displayed.
5. Select **OK**.
The Server Certificates dialog is displayed showing that the selected certificate was deleted.

Viewing pending certificates

To view pending certificates:

1. Under the **Tasks** tab, select **Security > Administer Server Certificates > View Pending Certificates**.
The Pending Certificate Requests dialog is displayed.
2. Select the host for which you want to view the pending certificates.
3. Select **Switch To**.
The pending certificates for the host are displayed.
4. Select the certificate you want to enroll or delete.
5. Select **Manual Enroll**, **Auto Enroll**, or **Delete**.
The Pending Certificates dialog is displayed.

6. Select **Close**.

The Pending Certificate Requests dialog is displayed.

Default server certificate settings

To create default server certificate settings:

1. Under the **Tasks** tab, select **Security > Administer Server Certificates > Administer Certificate Defaults**.

The Server Certificate Default Settings dialog is displayed.

2. Enter default certificate settings.
3. Select **Apply**.

The Server Certificates dialog is displayed.

Listing trusted certificates

To list trusted certificates:

1. Under the **Tasks** tab, select **Security > Trusted Certificates**.

The Trusted Certificates dialog is displayed. The trusted certificates are listed in this dialog.

2. From this dialog, you can do any of the following procedures:

- [Viewing trusted certificates](#) on page 170
- [Importing trusted certificates](#) on page 171
- [Exporting trusted certificates](#) on page 171
- [Deleting trusted certificates](#) on page 172

Viewing trusted certificates

To view trusted certificates:

1. Under the **Tasks** tab, select **Security > Trusted Certificates**.

The Trusted Certificates dialog is displayed.

2. Select the host for which you want to view the trusted certificates.
3. Select **Switch To**.

The certificates for the host are displayed.

4. Select the certificate you want to view.
5. Select **View**.
The Trusted Certificate Details dialog is displayed.
6. Select **Close**.
The Trusted Certificates dialog is displayed.

Importing trusted certificates

To import a trusted certificate:

1. Under the **Tasks** tab, select **Security > Trusted Certificates**.
The Trusted Certificates dialog is displayed.
2. Select the host for which you want to import a trusted certificate.
3. Select **Switch To**.
The certificates for the host are displayed.
4. Select **Import**.
The Trusted Certificate Import dialog is displayed.
5. Enter a name into the **Certificate Alias** field.
6. Paste the content of the trusted certificate into the **Certificate PEM** data field.
7. Select **Apply**.
The Trusted Certificates dialog is displayed showing the new certificate.

Exporting trusted certificates

To export a trusted certificate:

1. Under the **Tasks** tab, select **Security > Trusted Certificates**.
The Trusted Certificates dialog is displayed.
2. Select the host for which you want to export a trusted certificate.
3. Select **Switch To**.
The certificates for the host are displayed.
4. Select **Export**.
The Trusted Certificate Export dialog is displayed.

5. Copy the content of the **Certificate PEM** data field to a text editor so you can save the certificate to another system.
6. Select **Close**.

The Trusted Certificates dialog is displayed showing the new certificate.

Deleting trusted certificates

To delete a trusted certificate:

1. Under the **Tasks** tab, select **Security > Trusted Certificates**.
The Trusted Certificates dialog is displayed.
2. Select the host for which you want to delete a trusted certificate.
3. Select **Switch To**.

The certificates for the host are displayed.

4. Select **Delete**.

A confirmation dialog is displayed.

5. Select **OK**.

The Trusted Certificates dialog is displayed showing that the selected certificate was deleted.

JKS synchronization

To synchronize trusted and server certificates:

1. Under the **Tasks** tab, select **Security > Synchronize JKS**.
The JKS Synchronization dialog is displayed.
2. Do not change the name displayed in the **Host** field.
3. Select the trusted certificate and server certificate you want to synchronize.
4. If you want to remove extra entries that will not be synchronized, select the **Remove Extra** option.
5. Select **Synchronize JKS**.

A success or failure message is displayed.

Appendix A: Administration worksheets

This section contains worksheets used help gather administration data.

This section includes the following worksheets:

- [Reporting group worksheets](#) on page 175
- [Active Directory worksheet for LDAP integration](#) on page 181

Reporting group worksheets

Use the following worksheets to help you set up your reporting groups. Make as many copies of these worksheets as you need to set up all of your groups. Each of the worksheets contain sample data.

This section includes the following worksheets:

[Creating reporting groups](#) on page 177: Select an administered view, list your first category, and list all of the groups you need under that category. Repeat this process for all categories under that view. If you need reporting groups for another view, repeat this process.

[Choosing group members](#) on page 179: For your first category, list the group members for that category. Repeat this process for all categories.

Creating reporting groups

[illegible]

Choosing group members

[illegible]

Active Directory worksheet for LDAP integration

Use the following worksheet to collect information about your Active Directory server so you can synchronize your enterprise directory with Avaya IQ. Have your Active Directory IT personnel work with Avaya or BusinessPartner provisioning to define all of the options shown in this worksheet. Two critical items are the Base Node and Search Filter. These options determine exactly which users will be synchronized from your Active Directory into the Avaya IQ directory.

Note:

Not all options are shown in this worksheet.

Option	Your value
Active Directory IP address or DNS name	
Port number (default is 389; SSL default is 636)	
Active Directory user name	
Active Directory user name password	
LDAP base node name	
Search filter	
Execution Frequency	
User DN suffix (optional)	
User DN prefix (optional)	

Index

A

Active Directory	98
administration features	9
administration road map	10
advanced properties	103
agent activity states	75
agent call handling options	87
agent logout reason codes	79
agents	22
alarming	102
alarms	114

B

backing up Avaya IQ	116
backing up the database	117
backing up the OS	117
backup strategies	114
behaviors	67

C

certificates	14 , 166
connection properties	97
contact center preferences	83

D

data access permissions	42
data removal	164
database connection properties	97
database management	164
database schema check	165
database user and password maintenance	159
directory integration	98
duplicate logon sessions	16

E

edit service configuration	166
editing properties	152
email server maintenance	152
Enterprise Directory	98
enterprise directory integration	98
enterprise tab	17

J

jobs	105
----------------	---------------------

L

LDAP integration	98
licensing	146
logging on	13
login session properties	95
logs	114

M

maintenance	113
manage distributors	166
manage trusted certificates	166
metadata sanity check	165
monitoring the system	114
multiple administration sessions	
administration conflicts	16
multiple agent queue assignments	83

O

operations permissions	39
----------------------------------	--------------------

P

password management	18
pop-up blocker settings	13
Proactive Contact maintenance	155

Q

queues	22
------------------	--------------------

R

reinitialize user service	166
reporting behaviors	67
reporting group administration	26
reporting groups	23
reporting keywords	81
reporting names management	74
reporting preferences	61

Index

role administration	49
role permissions	51
role planning.	47
routing point options	92
routing points	22

S

scheduling jobs	105
security	11
service level targets	72
SNMP.	102
software updates	151
system monitoring	114
system preferences	95

T

tasks tab	17
thresholds	61
time zone data.	156

U

unlocking user accounts	59
updates	151
user administration.	34
user permissions.	56
user roles	38
users	22
users with disabilities.	19

W

worksheets	173
----------------------	---------------------