Using ODBC and JDBC with Avaya Call Management System

Release 21.0
Issue 3
November 2024

Notices

You may, at your own risk, assemble a MyDocs collection solely for your own internal business purposes, which constitutes a modification to the original published version of the publications. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of publications. You agree to defend, 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, your modifications, additions or deletions to the publications.

A single topic or a collection of topics may come from multiple Avaya publications. All of the content in your collection is subject to the legal notices and disclaimers in the publications from which you assembled the collection. For information on licenses and license types, trademarks, and regulatory statements, see the original publications from which you copied the topics in your collection.

Except where expressly stated by Avaya otherwise, no use should be made of materials provided by Avaya on this site. All content on this site and the publications provided by Avaya including the selection, arrangement and design of the content is owned by Avaya and/or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. Avaya owns all right, title and interest to any modifications, additions or deletions to the content in the Avaya publications.

Notice

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

Documentation disclaimer

“Documentation” means information published in varying media which may include product information, subscription or service descriptions, operating instructions and performance specifications that are generally made available to users of products. Documentation does not include marketing materials. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of Documentation unless such modifications, additions, or deletions were performed by or on the express behalf of Avaya. End user agrees to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End user.

Link disclaimer

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

Warranty

Avaya provides a limited warranty on Avaya hardware and software. Please refer to your agreement with Avaya to establish the terms of the limited warranty. In addition, Avaya’s standard warranty language as well as information regarding support for this product while under warranty is available to Avaya customers and other parties through the Avaya Support website: https://support.avaya.com/helpcenter/getGenericDetails?detailId=C20091120112456651010 under the link “Warranty & Product Lifecycle” or such successor site as designated by Avaya. Please note that if the product(s) was purchased from an authorized Avaya channel partner outside of the United States and Canada, the warranty is provided by said Avaya Channel Partner and not by Avaya.

“**Hosted Service**” means an Avaya hosted service subscription that You acquire from either Avaya or an authorized Avaya Channel Partner (as applicable) and which is described further in Hosted SAS or other service description documentation regarding the applicable hosted service. If You purchase a Hosted Service subscription, the foregoing limited warranty may not apply but You may be entitled to support services in connection with the Hosted Service as described further in your service description documents for the applicable Hosted Service. Contact Avaya or Avaya Channel Partner (as applicable) for more information.

Hosted Service

THE FOLLOWING APPLIES ONLY IF YOU PURCHASE AN AVAYA HOSTED SERVICE SUBSCRIPTION FROM AVAYA OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE), THE TERMS OF USE FOR HOSTED SERVICES ARE AVAILABLE ON THE AVAYA WEBSITE, HTTPS://SUPPORT.AVAYA.COM/LICENSEINFO UNDER THE LINK “Avaya Terms of Use for Hosted Services” OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, AND ARE APPLICABLE TO ANYONE WHO ACCESSES OR USES THE HOSTED SERVICE. BY ACCESSING OR USING THE HOSTED SERVICE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE DOING SO (HEREINAFTER REFERRED TO INTERCHANGEABLY AS “YOU” AND “END USER”), AGREE TO THE TERMS OF USE. IF YOU ARE ACCEPTING THE TERMS OF USE ON BEHALF A COMPANY OR OTHER LEGAL ENTITY, YOU REPRESENT THAT YOU HAVE THE AUTHORITY TO BIND SUCH ENTITY TO THESE TERMS OF USE. IF YOU DO NOT HAVE SUCH AUTHORITY, OR IF YOU DO NOT WISH TO ACCEPT THESE TERMS OF USE, YOU MUST NOT ACCESS OR USE THE HOSTED SERVICE OR AUTHORIZE ANYONE TO ACCESS OR USE THE HOSTED SERVICE.

Licenses

The Global Software License Terms (“Software License Terms”) are available on the following website https://www.avaya.com/en/legal-license-terms/ or any successor site as designated by Avaya. These Software License Terms are applicable to anyone who installs, downloads, and/or uses Software and/or Documentation. By installing, downloading or using the Software, or authorizing others to do so, the end user agrees that the Software License Terms create a binding contract between them and Avaya. In case the end user is accepting these Software License Terms on behalf of a company or other legal entity, the end user represents that it has the authority to bind such entity to these Software License Terms.

Copyright

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

Virtualization

The following applies if the product is deployed on a virtual machine. Each product has its own ordering code and license types. Unless otherwise stated, each Instance of a product must be separately licensed and ordered. For example, if the end user customer or Avaya Channel Partner would like to install two Instances of the same type of products, then two products of that type must be ordered.

Third Party Components

The following applies only if the H.264 (AVC) codec is distributed with the product. THIS PRODUCT IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO (i) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD (“AVC VIDEO”) AND/OR (ii) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE HTTP://WWW.MPEGLA.COM.

Service Provider

WITH RESPECT TO CODECS, IF THE AVAYA CHANNEL PARTNER IS HOSTING ANY PRODUCTS THAT USE OR EMBED THE H.264 CODEC OR H.265 CODEC, THE AVAYA CHANNEL PARTNER ACKNOWLEDGES AND AGREES THE AVAYA CHANNEL PARTNER IS RESPONSIBLE FOR ANY AND ALL RELATED FEES AND/OR ROYALTIES. THE H.264 (AVC) CODEC IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO: (i) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD (“AVC VIDEO”) AND/OR (ii) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION FOR H.264 (AVC) AND H

(HEVC) CODECS MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE HTTP://WWW.MPEGLA.COM.

Compliance with Laws

You acknowledge and agree that it is Your responsibility to comply with any applicable laws and regulations, including, but not limited to laws and regulations related to call recording, data privacy, intellectual property, trade secret, fraud, and music performance rights, in the country or territory where the Avaya product is used.

Preventing Toll Fraud

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

Avaya Toll Fraud intervention

If You suspect that You are being victimized by Toll Fraud and You need technical assistance or support, please contact your Avaya Sales Representative.

Security Vulnerabilities

Information about Avaya’s security support policies can be found in the Security Policies and Support section of https://support.avaya.com/security.

Suspected Avaya product security vulnerabilities are handled per the Avaya Product Security Support Flow (https://support.avaya.com/css/P8/documents/100161515).

Trademarks

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

Avaya is a registered trademark of Avaya LLC.

All non-Avaya trademarks are the property of their respective owners.

Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

Downloading Documentation

For the most current versions of Documentation, see the Avaya Support website: https://support.avaya.com, or such successor site as designated by Avaya.

Contact Avaya Support

See the Avaya Support website: https://support.avaya.com for Product or Cloud Service notices and articles, or to report a problem with your Avaya Product or Cloud Service. For a list of support telephone numbers and contact addresses, go to the Avaya Support website: https://support.avaya.com (or such successor site as designated by Avaya), scroll to the bottom of the page, and select Contact Avaya Support.

Contents

Chapter 1: Introduction

Purpose

This document describes how to use Open Database Connectivity (ODBC) and Java Database Connectivity (JDBC) with Avaya Call Management System. It is intended for support personnel and contact center administrators.

Before using this document, ensure that you are familiar with CMS and have a basic understanding of Structured Query Language (SQL) and database logic.

Change history

The following table outlines the key changes in this document for Release 21.x:

Issue	Date	Summary of changes
3	November 2024	• Minor text corrections for topic titles.
2	September 2024	• Revised the procedures about installing and updating the Informix encryption certificate for clarity. • Corrected various commands. For example, references to `cms_ol.kdb` have been changed to `cms_ol.p12` because the `.kdb` format is no longer supported. • Minor rephrasing and formatting fixes in various sections.
1	June 2024	• Revised Informix information and cleaned up outdated IBM references. • Updated ODBC and JDBC software on page 10 with various edits and indicated that you can download client libraries for HCL Informix from https://www.actian.com. • Updated the information about obtaining JDBC and Client SDK files in Installing JDBC on a Windows client on page 19.

Chapter 2: ODBC and JDBC overview

This section provides an overview of how ODBC and JDBC work and interact with CMS.

ODBC background and functionality

ODBC is a client/server feature. The client computers access data through ODBC. The server is the machine where the CMS database is located. The clients must be connected to a network that is fully functional and able to access the server.

ODBC enables access to data at multiple sites, so it is especially useful for call centers with multiple sites. ODBC uses SQL to access data. You can use this data to produce reports.

The ODBC API enables you to access one or many Database Management Systems (DBMSs). You can use queries to access data in the database for use in reports and other outside applications.

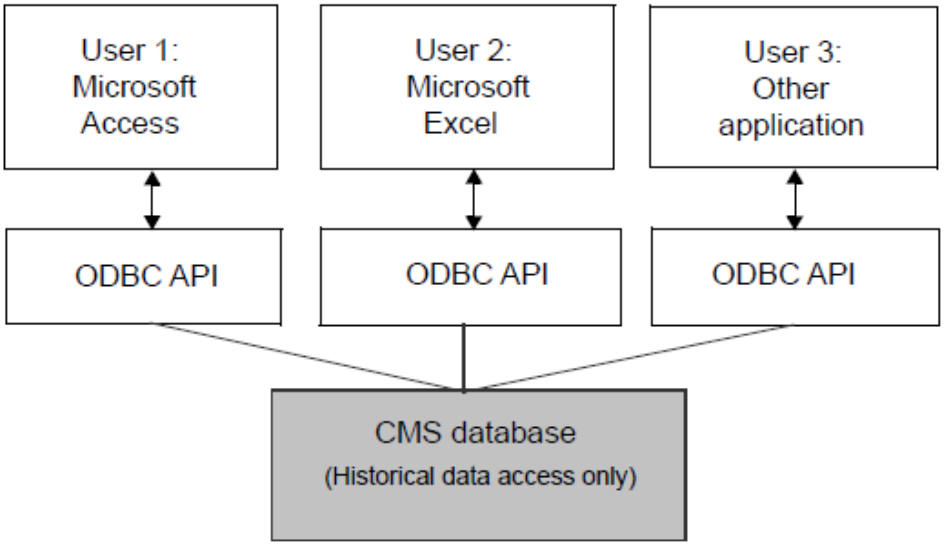
Data access through ODBC

ODBC was developed as a way to access different types of data. A single call center can work with different applications that all access call center data.

ODBC provides a standard method of database access, so you do not need to be concerned with the underlying functionality of network software, naming conventions, and other complexities involved in accessing data through a DBMS. The data must be queried through the embedded SQL query function in the application you are using. Refer to your specific application documentation for information about the application's embedded SQL function.

Data access diagram

The following image illustrates user data access through ODBC:



Important:

Avaya provides support for ODBC connectivity. Avaya does not support third-party client applications such as Microsoft Access or Windows.

SQL for ODBC data

ODBC uses SQL to query and access data. Queries written in SQL can be used to access data with different formats.

SQL is the basis for relational database access. A relational database model is a table that stores data in rows and columns. Relationships between tables are established through data items that match data item values in another table.

SQL queries access the data stored in the relational database tables and extracts it for use in other applications. You can compose an SQL query in the Windows application for which you need the data.

You can also use SQL to construct data calculations, which you can use to see a sum of the data. For example, you can view the total number of calls routed to a particular split or skill.

CMS support of ODBC and JDBC

CMS uses an HCL Informix database management system that supports compatible ODBC and JDBC clients. CMS is delivered with this ODBC and JDBC network connectivity enabled. The ODBC and JDBC clients provide direct access to the Informix database that CMS uses and all the CMS call center data.

ODBC is a specification for a database API. Microsoft ODBC is based on the Call Level Interface specifications from X/Open and the International Standards Organization/International Electromechanical Commission (ISO/IEC). ODBC supports SQL statements with a library of

C functions. An application calls these functions to implement ODBC functionality. ODBC applications enable you to do the following:

- Connect to and disconnect from data sources.
- Retrieve information about data sources.
- Retrieve information about the Informix ODBC driver.
- Set and retrieve Informix ODBC driver options.
- Prepare and send SQL statements.
- Retrieve information about SQL results and process it dynamically.

ODBC enables you to allocate storage for results before or after the results are available. You can determine the results and the action to take without the limitations that predefined data structures impose. ODBC does not require a preprocessor to compile an application program.

The JDBC API is the industry standard for database-independent connectivity between the Java programming language and a wide range of databases, SQL databases, and other tabular data sources such as spreadsheets or flat files. JDBC provides a call-level API for SQL-based database access. JDBC technology enables you to use the Java programming language to take advantage of “Write Once, Run Anywhere” capabilities for applications that require access to enterprise data. With a JDBC technology-enabled driver, you can connect all corporate data even in a heterogeneous environment.

Note:

If you choose to develop an application using ODBC or JDBC, Avaya cannot provide support for that application or for any other third-party software or related mapping.

Related links

ODBC and JDBC software on page 10

ODBC data usage

Data extracted and stored by an ODBC application can be used by ODBC-enabled programs, such as workforce management packages, network routers, and blended inbound outbound applications. You can use an ODBC data application to generate reports using data from multiple call center sites and their databases.

Data queries in ODBC

All queries in ODBC must be composed to ensure continued CMS performance. The query is invoked differently in each Windows application.

For more information about composing database queries, see Performance impact on page 10 and the information about editing queries in *Avaya CMS Supervisor Report Designer*.

ODBC and JDBC software

The HCL Informix ODBC and JDBC have two main components:

- An ODBC and a JDBC client.
- Enabled network connectivity in the HCL Informix IDS database server, which is the CMS server in this instance.

After ODBC and JDBC are installed and administered, the ODBC and JDBC software and its components are transparent to the client applications.

The ODBC and JDBC features enable multiple, synchronous access from clients, users, and applications. ODBC uses Microsoft data source names (DSN) as the link between the ODBC client and the HCL Informix IDS database. JDBC must be configured in the JDBC client software.

You can download client libraries for HCL Informix 14.10 from https://www.actian.com.

ODBC and JDBC features

The HCL Informix database server provides the ODBC and JDBC communication and connectivity that enable external data access to the CMS database. There are ODBC and JDBC clients available for Windows and other operating systems. This document covers the Windows clients. Windows 10 and 11 are supported.

All historical CMS database tables, dictionary tables, and customer-provided tables can be accessed by ODBC or JDBC clients through standard ODBC or JDBC enabled software applications.

All standard Structured Query Language (SQL) queries generated by user applications are supported by ODBC and JDBC, as limited by permissions. Table-level read-only permissions restrict access to certain database tables.

Language

Avaya tests ODBC and JDBC in English only for use with CMS. HCL Informix ODBC and JDBC support other double-byte languages, but if you use a language other than English, Avaya does not provide ODBC or JDBC support for that language.

Supported number of logins

Order the required number of ODBC and JDBC licenses to support the maximum number of simultaneous connections required. Access is enforced by the license file.

Performance impact

The number, size, and types of queries received by the CMS can impact performance. The recommendations for composing queries in the CMS custom report editor also apply to ODBC queries.

Some of the activities that can impact CMS performance are:

Tables: Use the exact table and database item names when querying the database. You can maximize the performance of the system by running queries that access large tables or that perform table joins during a period of low agent activity and low real-time report activity.

Accessing large tables, such as the split/skill or agent tables, or joining tables in queries can have a negative impact on CMS performance.

Calculations: Review calculations before sending them to the database. This ensures that the correct operation is performed. Arithmetic operations are performed with the rules of operator precedence, in order from left to right.

Queries: Prioritize resource intensive queries the same way you prioritize reports during high business activity. Running complex or multiple queries on the database impact system performance similar to running multiple reports.

Number of simultaneous database accesses: Minimize the number of database connects and disconnects from an application, and spread your ODBC activities throughout the day.

Synonyms: Download the synonyms to your client application or database and then perform the join at the client.

CMS maintenance: Be aware that during off-peak hours, CMS runs it's own activities, such as archiving and making backups. This can use a significant amount of resources and time when working with a large database.

Table permissions, security and port allocation

ODBC users log into the CMS server with password protection. Users have SQL access to Informix tables, as limited by the table permissions.

All historical and dictionary database tables have read-only access permission. The customer-created tables (any table name that begins with "c_") on the host have read and write permissions. No other tables are accessible through ODBC.The ports will be defined on the CMS server in the `/opt/Informix/etc/sqlhosts` file.

If you want to limit the CMS logins which have ODBC access, that procedure is described in detail in Providing secure access to the CMS database.

Important:

If your network uses a firewall, it is common for unused ports to be locked. ODBC uses network ports 50000 and 50001. If these ports are locked, you will not be able to connect to the CMS database with ODBC.

Informix User definition

In the case of direct connections through JDBC and ODBC, a license will be required for each individual user directly connecting through JDBC or ODBC. There will not be an additional license required for the individual's machine or device through which such access is made.

It is your responsibility to ensure you acquire the appropriate number of licenses for the anticipated use of the CMS, and to properly determine how many direct connections to the database will be required.

You are only licensed and allowed to make direct connections to the database up to the number of licenses you acquired.

If additional licenses are required, you are obligated to acquire them before making connection to the database.

CMS and ODBC interoperability

When using ODBC with CMS, you must keep the following in mind:

Dictionary names: Clients can access CMS Dictionary names. You must map the synonym to the report from the client.

Permissions: Applications that access Informix externally, such as database access scripts, might not work if the table permission script tries to access a table to which permission is denied.

Field display: The time and date data you receive from the database might not be formatted. Generally, times can be shown in seconds or in 24-hour clock format. You need to review data for formatting when you import it into your software application. The data returned from your SQL queries will be formatted in the manner described in your database interface specifications. See your software's documentation for further information on formatting data.

Switch features and capabilities: Some switch features and capabilities have an impact on CMS open database items.

For more information on these features and capabilities, see the appropriate database items and calculations document for your CMS release.

CMS database logic structure

CMS historical tables store information in one record per row format. This formatting affects the way data can be accessed through ODBC. When accessing data in the historical tables, you might need to sum the information to retrieve complete data.

Example

A record will be created for each split/skill that an agent is logged into in the agent tables. If an agent is logged into four splits/skills, there will be four records for that agent.

Similarly, if an agent starts the day with four splits/skills, and is added to a fifth split/skill before the end of the day, the agent's fifth record will be generated only from the point at which the additional split/skill was added. The other four records will reflect the total logon time.

Agent tables

If an agent logs off and logs on more than once in a specified interval, another complete set of records is created for that agent for each logon in the agent tables.

Example

If an agent logs into four split/skills, logs out, and then logs back on during a set interval, there will be two sets of four records for that agent, one set per logon.

VDN tables

The VDN tables store one record per vector on which a VDN terminates.

Therefore, if the terminating vector for a specific VDN changes in a set interval, there are two records for that VDN - one per terminating vector.

This logic also applies to the Vector, Trunk, Trunk Group, and Split/Skill tables. If information is required from these tables, a sum Structured Query Language (SQL) query can be necessary to access complete data from each table.

Circular structure tables

The Exceptions, Call Record, and Agent Trace tables are circular files. These tables populate continuously, until the table capacity plus ten percent has been reached. At that point, the oldest ten percent of the records are deleted.

Example

If an agent trace table has a capacity of 100 rows, and the total rows populated equals 110, the oldest ten rows will automatically be deleted.

Therefore, the data in that table will change continuously as the table is updated.

Chapter 3: ODBC software configuration

Installing ODBC on a Windows client

The HCL Informix ODBC software can be installed on your Windows desktop computer or on your network for each client to access.

Note:

The Windows interface is customizable. You might notice some user interface differences based on your system configuration.

Requirements

Before installing the HCL Informix ODBC driver software on your computer, verify that:

- The client network software is installed.
- Your computer is communicating with the CMS server over the network.

  Use your desktop TCP/IP products Packet Internet Groper (PING) utility (for example, ping hostname) to ensure that Communication between your computer and the CMS server is functional.

- **Caution:**

  Do not proceed if basic communications between your computer and the server cannot be established.

  The desktop computer is running Windows.

Installing ODBC on Windows

Procedure

1. CSDK client zip file from the CMS server to your Windows system using the following steps:
   a. Use your choice of transfer application to connect to the CMS server, such as WinSCP.

b. Navigate to a Windows folder where you want to copy the files. You can choose any folder.

c. Navigate to the following CMS server directory: `/storage/cms_dvd/CSDK`

d. Copy the Client SDK zip file to a Windows folder.

2. Open Windows Explorer.
3. Navigate to the folder where you copied the zip file.
4. Double-click the CSDK zip file.
5. Unzip the files to the folder of your choice.
6. In Windows Explorer, navigate to the folder where you unzipped the files.
7. Double-click the `installclientsdk.exe` file.
8. Click **Next**.

   The installation program displays the Licensing Agreement page.
9. Enter the appropriate response for the licensing question.
10. Click **Next**.
11. Choose a location for the Client-SDK installation. You can use the default location or choose a specific location.
12. Click **Next**.
13. Keep the default install option of **Set: Typical**
14. Click **Next**.
15. Click **Install**.
16. When promted to install driver package, click **No**.
17. Click **Next**.

    The installation program displays the Installation Complete screen.
18. Click **Done**.
19. Continue with Configuring an ODBC data source on page 15.

Configuring an ODBC data source

About this task

When setting up the ODBC driver, configure the database to access a specific server.

When the ODBC driver is configured, it is accessible to ODBC-enabled applications on your computer. With ODBC, you can send queries to the CMS database from applications such as Microsoft Access. The query is used to access data and extract it for use in other applications.

Procedure

1. From Control Panel, navigate to **Set up ODBC Data sources (32-bit)** or **Set up ODBC Data sources (64-bit)** as appropriate for your version of Windows.

   The ODBC Data Source Administrator window is displayed.

2. Click one of the following tabs:

   - **System DSN**: Select this option if you want the data source to be available to all users. You need administrative privileges to create a system DSN.
   - **User DSN**: Select this option if you want the data source to be available to the current user. This setting is useful for providing access to a specific user. Do not administer data sources on a per-user login ID basis.
   - **File DSN**: Select this option if you want the data source to be stored in a file rather than the registry. This file will have a DSN extension.

3. Click **Add**.

   The Create New Data Source window displays a list of data source drivers.

4. Select the Informix ODBC driver.

5. Do the following if you are using the File DSN tab:

   a. After selecting the driver, click **Next**.

   b. Browse to or type the name of the file data source.

   c. Click **Next**.

   d. Click **Finish**.

      The HCL Informix ODBC Driver Setup window is displayed.

6. Do the following if you are using the User DSN or System DSN tab:

   a. After selecting the driver, click **Finish** to proceed with the setup.

   b. In the **Data Source Name** field, enter a name for the server or database you are connecting to.

      An example entry for this field is `cms_net` or `cms_<hostname>`, where `<hostname>` is the CMS hostname.

   c. In the **Description** field, enter a description for the data source you are connecting to.

   d. Click **Connection** tab.

   e. In the **Server Name** field, enter the CMS server name.

      Enter `cms_<hostname>` if you know the CMS hostname. Otherwise, you can enter `cms_net`. Note that you cannot connect to multiple CMS systems simultaneously using *cms_net* because the **Server Name** field requires a unique value across all DSNs. If you try to create another DSN using *cms_net* and provide a different hostname, it will change all DSNs with the same server name to use the new hostname.

f. Enter the hostname or IP address.

g. In the **Service** field, enter the port number for your database host machine.

   Use port 50000 for *cms_net* and port 50001 for *cms_<hostname>*.

h. In the **Protocol** list, select **olsocssl** if ODBC TLS/SSL is configured on the CMS server.

   Otherwise, select **olsoctcp**.

i. Leave the **Options** field blank.

j. Enter `cms` in the **Database Name** field.

k. Enter the CMS user ID and password.

7. Click the **Environment** tab.
8. Select the check box to the right of **Use Server Database Locale**.

   Note that you might need to change the **Client Locale** setting to `en_US.UTF8` if the connection is not successful.
9. Click the **Connection** tab.
10. Click **Apply**.
11. Click **Apply & Test Connection** and ensure that the connection is successful.
12. Click **OK** as needed until the windows are closed.

    The ODBC driver software is installed on your computer.

Removing a data source

Procedure

1. From Control Panel, navigate to **Set up ODBC Data sources (32-bit)** or **Set up ODBC Data sources (64-bit)** as appropriate for your version of Windows.

   The ODBC Data Source Administrator window is displayed.
2. Click the **System DSN** tab.
3. Select the appropriate ODBC data source.
4. Click **Remove** and follow the prompts.

Configuring ODBC tracing options

About this task

You can specify how the ODBC driver traces ODBC function calls. If tracing is activated, the system generates a file that contains the actual ODBC function calls.

Procedure

1. From Control Panel, navigate to **Set up ODBC Data sources (32-bit)** or **Set up ODBC Data sources (64-bit)** as appropriate for your version of Windows.

   The ODBC Data Source Administrator window is displayed.
2. Click the **Tracing** tab.
3. Choose one of the following options:
   - Click **Start Tracing Now** to trace ODBC calls or observe ODBC activity.
   - Click **Stop Tracing Now** to stop tracing when the ODBC session is completed.
   - In the Log File Path area, click **Browse** to select or change the file to which the Informix driver writes tracing information. The default log file is `\SQL.LOG`.

     Important:

     Do not change the default entry in the Custom Trace DLL area.

Viewing installed ODBC data source drivers

About this task

You can view additional information about installed drivers. If you cannot see a driver on the Drivers tab, you must reinstall it.

Procedure

1. From Control Panel, navigate to **Set up ODBC Data sources (32-bit)** or **Set up ODBC Data sources (64-bit)** as appropriate for your version of Windows.

   The ODBC Data Source Administrator window is displayed.
2. Click the **Drivers** tab.
3. Select the driver from the list.

   If the driver you are looking for is not on the list, it was not installed properly.
4. Click the **About** tab to view additional information for the selected driver.

Chapter 4: JDBC software configuration

Installing JDBC on Windows

This section contains the following information:

- Requirements
- Installing JDBC on a Windows client

Note:

The Windows interface is completely customizable. You might notice some user interface differences based on your system configuration.

Requirements

Before installing the HCL Informix JDBC driver software on your computer, verify that:

- The client network software is installed.
- Your computer is communicating with the CMS server over the network.

  Use your desktop TCP/IP products Packet Internet Groper (PING) utility (for example, ping hostname) to ensure that the communication between your computer and the CMS server is functional.

- **Caution:**

  Do not proceed if basic communications between your computer and the server cannot be established.

- Determine `%CLASSPATH%` for Java applications.

Installing JDBC on a Windows client

About this task

When you install JDBC, you must copy both a CSDK zip file and a CSDK tar file, unzip and untar the files, and install both executable files.

Before you begin

Download Client SDK and JDBC libraries for HCL Informix 14.10 from https://www.actian.com.

Procedure

1. After downloading the JDBC zip file, copy it to a folder on your Windows 64-bit system.
2. From Windows Explorer, navigate to the folder where you copied the .zip file.
3. Double-click the JDBC .zip file.
4. Unzip the files to the folder of your choice.
5. In Windows Explorer, navigate to the folder where you unzipped the files.
6. Double-click the `installclientsdk.exe` file.

   The installation program displays the Introduction page.
7. Click **Next**.

   The installation program displays the Software License Agreement page.
8. Select **I accept the terms of the license agreement** and click **Next**.

   The installation program displays the Installation Location page.
9. Accept the default location and click **Next**.

   The installation program displays the Choose Client SDK Features to Install page.
10. Accept the defaults and click **Next**.

    The installation program displays the Installation Summary page.
11. Click **Install**.

    The installation program installs the software and displays the Installation Complete page.
12. Copy the JDBC tar file to a folder on your Windows system.
13. Navigate to the folder where you copied the tar file.
14. Double-click the `.tar` file and untar the files to the folder of your choice.
15. In Windows Explorer, navigate to the folder where you untarred the files.
16. Double-click the `setup.jar` file.

    The installation program displays the Welcome page.
17. Click **Next**.
18. Enter the appropriate response for the licensing question.
19. Click **Next**.
20. Choose a location to install the JDBC software. You can use the default location or choose a specific location.
21. Click **Next**.

The page displayed shows where the HCL Informix JDBC Driver will be installed and the size of the driver.

22. Click **Next**.

    The installation process starts. When finished, the installation status is displayed.

23. Click **Finish**.

Chapter 5: Providing secure access to the CMS database

The CMS database has **open access** permissions as a standard feature. That is, any CMS login connecting to the CMS server using ODBC/JDBC has permissions to view CMS data tables.

Note:

CMS does not allow you to control which tables the CMS login has access to, or which ACD data the CMS login can view.

To limit the users that can access the CMS database using ODBC/JDBC follow the steps listed in this section. The users for whom you set permissions must adhere to the following requirements:

- All CMS login IDs to which you choose to provide CMS database access must be members of the dbaccess group.
- You must execute the dbaccess option under the cmsadm menu, which makes the proper Informix permission changes to the CMS database.

Your secure access permissions are preserved for you in the `cmsadm` backup and in the CMS Maintenance backup. The permissions are migrated during a CMS upgrade and can be restored in the event of a loss of your CMS server data.

Preparing to set secure database access

Procedure

1. Review all CMS logins and determine which users need ODBC and JDBC access.

   You can view user permissions information in CMS Supervisor or by running the `cms` command.

2. Make a note of which CMS logins need to be in the dbaccess group.

   You can run `cat /etc/group | grep dbaccess` to determine which users are already in the dbaccess group. For example, if the *odbcusr1* and *odbcusr2* are already in the group, a result such as the following is displayed:

   ```
   dbaccess::1002:odbcusr1,odbcusr2
   ```

Adding members to the dbaccess group

Procedure

1. Each CMS login which receives ODBC/JDBC access must be a member of the UNIX dbaccess group.

   Note:

   The root, CMS, and cmssvc users will have full default permissions to ODBC/ JDBC.

2. To put CMS logins into the dbaccess group, enter: `usermod -G dbaccess cmslogin` where cms login is the user id of the specific CMS login to be placed in the group. You must execute the usermod command once for each CMS login to which you want to provide CMS database access.

   Caution:

   Enter a capital **G** while typing the command. Entering a lower case g will change the users default group, which can cause access issues to CMS.

Example

```
usermod -G dbaccess odbcusr1
usermod -G dbaccess odbcusr2
```

Setting secure access permissions in the CMS database

About this task

Use this procedure to perform DB access permission changes. After the changes are completed, users with access to the dbaccess group can run ODBC and JDBC clients and access the CMS database.

Procedure

1. Log in as root and run the `cmsadm` command.
2. Enter the number associated with the **`dbaccess`** option. The system displays the following message:

   A message such as the following is displayed:

   ```
   Begin CMS DB Access Permissions changes grant resource to "public";
   Your CMS database currently has public access permissions to all resources.
   Do you wish to revoke this access and only grant access to specific CMS
   users? [y,n,?]
   ```

3. Enter `y` to proceed with changing database permissions.

   The output displays `grant connect to <cmslogin>` for each CMS login ID in the dbaccess group.

Next steps

To preserve your changes, run a CMSADM backup followed by a Maintenance Backup immediately.

Removing ODBC access permissions for a specific user ID

Procedure

1. If you wish to remove any CMS login IDs from those designated to have ODBC/JDBC access permission, you must first remove them from the dbaccess group.

   Note:

   You must execute usermod command once for each CMS login you are removing from the group.The usermod command will not remove the user from its default group cms.

   For example, if you wish to remove the CMS login ID odbcusr1 from the dbaccess group: usermod -G ""

   ```
   odbcusr1
   ```

   .

   Caution:

   Enter a capital **G** while typing the command. Entering a lower case g will change the users default group, which can cause access issues to CMS.

   This command will remove the user from all the custom groups along with dbaccess.

2. Enter: `cmsadm`.

   The system displays the Avaya Call Management System menu.

3. Enter the number associated with the dbaccess option. The system reads the UNIX group information and resets the access permissions for only those members still in the dbaccess group.

   For example, if you have removed odbcusr1 from the dbaccess group but left odbcusr2 in the group, then:

   ```
   Begin CMS DB Access Permissions changes
   Please wait while connect permissions are granted for requested users
   grant connect to “Odbcusr2”;
   Changes to CMS DB Access Permissions finished.
   ```

4. To preserve your changes, run a `cmsadm` backup followed by a Maintenance Backup immediately.

Returning the CMS database to public permissions

Procedure

1. To get the list of all ODBC users, enter: `grep dbaccess /etc/group`.
2. You must first remove all users from the dbacess group. Run the `usermod` command for each CMS login that is currently in the dbaccess group.

   Caution:

   Enter a capital **G** while typing the command. Entering a lower case g will changethe users default group, which can cause access issues to CMS.

   For example, if the users odbcusr1 and odbcusr2 are the entire set of CMS login IDs with secure access permissions.`usermod -G "" odbcusr1` and `usermod -G "" odbcusr2`
3. Enter: `cmsadm`

   The system displays the Avaya Call Management System Administration menu.
4. Enter the number associated with the dbaccess option.

```
Begin CMS DB Access Permissions changes
No CMS user ids are in UNIX group dbaccess.
If you proceed, the CMS database is set to public permissions access for all
resources.
Do you really want to do this? [y,n,?]
```

5. Enter: y

```
Please wait while CMS Informix Database permissions are set to public.
grant resource to public;
revoke connect from cms;
revoke connect from cmssvc;
Grant resource to public on CMS database.
Changes to CMS DB Access Permissions finished.
```

   Run a `cmsadm` backup followed by a Maintenance Backup to preserve your changes.

Chapter 6: Encrypting the ODBC and JDBC connections

CMS supports an option to configure the CMS network ports 50000 and 50001 for Informix TLS and SSL encryption. These CMS network ports can also be used for ODBC and JDBC connections. The TLS/SSL encryption requires you to install a PKCS 12 certificate.

After Informix encryption is enabled, the only operational impact is encrypted network connections for ports 50000 and 50001. All other CMS interfaces to Informix are not impacted.

About the Informix TLS and SSL encryption utility

Informix encryption attributes are provisioned during CMS installation. Use the `ids_tls_configure` utility to activate and manage encryption.

This utility enables you to do the following:

- Enable Informix network encryption.

  To enable Informix network encryption, you must provide a CA certificate. The certificate will be integrated into the Informix encryption configuration.

- Update the Informix network encryption certificate.

  When a new CA certificate is required, the utility updates the certificate in the existing Informix encryption configuration.

- Disable the Informix network encryption.

  The Informix encrypted network connections can be disabled. This will revert existing Informix network connections back to plain TCP/IP (non-TLS) mode.

- Display the Informix encryption state.
- View the Informix encryption certificate details.

Managing certificates for Informix TLS and SSL encryption

To configure TLS/SSL encryption, you must provide a commercially-signed certificate that is valid for the CMS server and the network where CMS resides. A specific alias must be added to the

certificate for Informix stability with TLS/SSL configured. The certificate is verified when you run the `ids_tls_configure` command.

Note the following requirements for the CA certificate:

- You are responsible for ensuring your certificate is valid. The certificate must be valid for the CMS server and the network where CMS resides.
- If you are converting a certificate to the PKCS 12 format, add the alias `cms_net_encrypt` to your certificate or certificate chain. Specific procedures for adding or converting an alias are not provided due to variations in certificate and certificate chain structures. Industry certificate management utilities, such as Keytool and OpenSSL, enable you to add or convert the alias value.
- If you have the Java Key Store (JKS) certificate for the CMS Web Client certificate (`cmsweb.jks`), a PKCS 12 certificate can be exported from the `cmsweb.jks` certificate as described in Exporting a PKCS 12 certificate from the cmsweb.jks certificate on page 27.

Note the full path and the password for the certificate. You will need the path and password to enable Informix TLS/SSL encryption or to update the encryption certificate.

To verify that the alias is in the certificate, run the following command:

```
keytool -list -v -keystore <Example.p12> -storepass
<CertificatePassword> | grep Alias
```

Exporting a PKCS 12 certificate from the cmsweb.jks certificate

About this task

This procedure is an example of how you can export a PKCS 12 certificate from the `cmsweb.jks` certificate. Note the full path and the password for the certificate. You will need this path and password to enable TLS/SSL encryption or to update the TLS/SSL encryption certificate.

Before you begin

Generate and install the `cmsweb.jks` certificate. For more information about Web Client certificates, see *Maintaining and Troubleshooting Avaya Call Management System*.

Procedure

1. Log in to the CMS server with root privileges.
2. Choose a location on your CMS server to store the certificate.
3. Run the following command:

```
keytool -J-Dkeystore.pkcs12.legacy
-importkeystore -srckeystore /opt/cmsweb/cert/cmsweb.jks
-destkeystore cmsweb.p12 -deststoretype PKCS12 -srcstoretype
JKS -srcstorepass <SOURCE_PASSWORD> -srcalias <SOURCE_ALIAS>
```

```
-deststoretype PKCS12 -destkeypass <CERT_PASSWORD> -deststorepass
<CERT_PASSWORD> -destalias cms_net_encrypt
```

- `<SOURCE_PASSWORD>` is the password for the JKS truststore. For the default Avaya-provided JKS, the default password is cmsweb.
- `<SOURCE_ALIAS>` is the alias for the JKS truststore. For the default Avaya-provided JKS, the alias is cmsweb1.
- `<CERT_PASSWORD>` is the password for the PKCS 12 truststore or certificate you are generating.

4. If you do not know the source alias, run the following command to find it:

```
keytool -list -v -keystore /opt/cmsweb/cert/cmsweb.jks -storepass
<SOURCE_PASSWORD> | grep Alias
```

Enabling Informix network encryption

Before you begin

Note the following for the customer-provided certificate:

- You must upload the certificate to the CMS server.
- Ensure that the certificate meets the criteria described in Managing certificates for Informix TLS and SSL encryption on page 26.
- You need the password for the certificate keystore.

Procedure

1. Log in to the CMS server with root privileges.
2. Run the `cmsadm` command.
3. Enter the number associated with the **`run_cms`** option.
4. Enter `2` to turn off CMS but leave IDS running.
5. Run the `/cms/install/bin/ids_tls_configure -e` command.

   If Informix network encryption is already enabled, the output displays a message such as the following:

   ```
   Informix encryption(TLS/SSL) is already configured. Encryption enable can't
   be
   executed. Exiting.
   ```

   If Informix network encryption is not enabled, the output displays a message such as the following:

   ```
   Informix encryption(TLS/SSL) enable started.
   Provide the PKCS12 certificate for configuring TLS/SSL.
   ```

6. Enter the path on the CMS server where you saved your certificate.
7. Enter the password for the certificate keystore.

If a certificate validation error occurs, the error is reported and encryption is not enabled. The following are examples of error messages you might see if the validation fails:

```
The provided certificate is not PKCS12 format. CERTIFICATE_TYPE
Please make sure your certificate meets the requirements in the CMS ODBC/JDBC
document, then re-execute ids_tls_configure
```

```
The provided certificate does not include the required alias: cms_net_encrypt.
Certificate alias: ALIAS. Please make sure your
certificate meets the requirements in the CMS ODBC/JDBC document,
then re-execute ids_tls_configure.
```

8. Run the `cmsadm` command.
9. Enter the number associated with the **`run_cms`** option.
10. Enter `1` to turn on CMS.

Next steps

After Informix encryption is enabled, install the certificate on the computer where the ODBC and JDBC software is installed. For more information, see Installing the Informix encryption certificate on your Windows computer on page 32.

Updating the Informix network encryption certificate

Before you begin

Informix network encryption must be enabled.

Note the following for the customer-provided certificate:

- You must upload the certificate to the CMS server.
- Ensure that the certificate meets the criteria described in Managing certificates for Informix TLS and SSL encryption on page 26.
- You need the password for the certificate keystore.

Procedure

1. Log in to the CMS server with root privileges.
2. Run the `cmsadm` command.
3. Enter the number associated with the **`run_cms`** option.
4. Enter `2` to turn off CMS but leave IDS running.
5. Run the `/cms/install/bin/ids_tls_configure -u` command.

   If Informix network encryption is not enabled, the output displays a message such as the following:

   ```
   Informix encryption(TLS/SSL) enable started.
   Provide the PKCS12 certificate for configuring TLS/SSL.
   ```

If Informix network encryption is enabled, the output displays a message such as the following:

```
You are about to replace the existing Informix encryption(TLS/SSL)
certificate.
Do you want to proceed? (y/n):
```

6. Enter `y`.

   The output displays the following:

   ```
   Informix encryption(TLS/SSL) certificate update started.
   Provide the PKCS12 certificate for updating TLS/SSL.
   ```

7. Enter the path on the CMS server where you saved your certificate.

   If the certificate file is not accessible, a message such as the following is displayed:

   ```
   The certificate file (/storage/my_cert.p12) does not exist.
   Please verify file location and read permissions exist, then re-enter.
   ```

8. Enter the password for the certificate keystore.

   If a certificate validation error is encountered, the error is reported and encryption is not enabled. The following are examples of error messages you might see if the validation fails:

   ```
   Certificate validated. Informix encryption(TLS/SSL) configuration completed. IDS
   is restarting.
   Informix encryption(TLS/SSL) enable complete.
   Informix network connections are now encrypted.
   ```

   ```
   The provided certificate is not PKCS12 format. CERTIFICATE_TYPE
   Please make sure your certificate meets the requirements in the CMS ODBC/JDBC
   document, then re-execute ids_tls_configure
   The provided certificate does not include the required alias: cms_net_encrypt.
   Certificate alias: ALIAS. Please make sure your
   certificate meets the requirements in the CMS ODBC/JDBC document,
   then re-execute ids_tls_configure.
   ```

9. Run the `cmsadm` command.
10. Enter the number associated with the **`run_cms`** option.
11. Enter `1` to turn on CMS.

Next steps

After the Informix encryption certificate is updated, ensure that the latest certificate is also available on the computer where the ODBC and JDBC software is installed. For more information, see Updating the Informix encryption certificate on a Windows computer on page 35.

Disabling the Informix network encryption

About this task

Disabling the Informix network encryption reverts the Informix network connections back to plain TCP/IP (non-TLS) mode.

Caution:

If you disable Informix network encryption, you cannot just turn it back on. You must re-enable it using the information in Enabling Informix network encryption on page 28.

Procedure

1. Log in to the CMS server with root privileges.
2. Run the `cmsadm` command.
3. Enter the number associated with the **`run_cms`** option.
4. Enter `2` to turn off CMS but leave IDS running.
5. Run the `/cms/install/bin/ids_tls_configure -d` command:

   If Informix network encryption is not enabled, a message such as the following is displayed:

   ```
   Informix encryption(TLS/SSL) is not configured.Disable encryption
   can't be executed.
   Exiting.
   ```

   If Informix network encryption is enabled, a message such as the following is displayed:

   ```
   Informix encryption(TLS/SSL) will be removed and IDS restarted.
   Do you want to continue (y/n):
   ```

6. Enter `y`.

   The output displays the following:

   ```
   Informix encryption(TLS-SSL) disable started.
   Informix encryption(TLS-SSL) disable complete. Restarting IDS.
   Informix is up in plain TCP (non-encrypted) mode.
   ```

7. Run the `cmsadm` command.
8. Enter the number associated with the **`run_cms`** option.
9. Enter `2` to turn off CMS but leave IDS running.

Checking if Informix encryption is enabled

Procedure

Run `/cms/install/bin/ids_tls_configure -s` to check if TLS/SSL encryption is configured.

Viewing the Informix encryption certificate details

About this task

You can view the certificate details from the incorporated Informix configuration. This information is only available if Informix encryption is enabled. This option is useful to determine the certificate expiration date or other significant details about the certificate. The complete certificate details are displayed to the screen, which might be very large. Consider redirecting the output to a file for review.

Procedure

1. Run the `/cms/install/bin/ids_tls_configure -v` command.

   If Informix network encryption is not enabled, the output displays the following:

   ```
   Informix encryption(TLS/SSL) is not configured. There is no Informix encryption
   certificate to view. Exiting.
   ```

   If Informix network encryption is enabled, the certificate details are displayed. This example shows the first few lines of a typical certificate:

   ```
   Label : cms_net_encrypt
   Key Size : 1024
   Version : X509 V3
   Serial : 5a77ca457eadd67f
   . . .
   . . .
   ```

2. To redirect the certificate into a file for easier viewing, run the following commands:

   ```
   /cms/install/bin/ids_tls_configure -v > /tmp/my_cert_details.out
   more /tmp/my_cert_details.out
   ```

Installing the Informix encryption certificate on your Windows computer

About this task

Install the Informix encryption certificate from the CMS server on the computer where the ODBC and JDBC client software is installed. The client certificate must match the certificate on CMS. Perform this procedure when TLS/SSL encryption is enabled on the CMS server.

Before you begin

- Run the `ids_tls_configure -e` command to confirm that TLS/SSL encryption is enabled on the CMS server. To confirm that the TLS/SSL encryption certificate is updated, run the `ids_tls_configure -u` command.
- Ensure that the Informix Client SDK is installed on your computer.
- Create an Informix JKS keystore password if you do not already have one. Remember this password in case you need to update the certificate in the future.

Procedure

1. Log in to Windows as an administrator.
2. Use WinSCP or a similar tool to copy the SSL certificate files from the CMS server to your computer.

   The SSL certificates are in the `/opt/informix/ssl` directory on the CMS server.

   The following is an example of the naming convention used if additional root and intermediate certificates exist:

   - `HOSTNAME_cert1.pem`
   - `HOSTNAME_cert2.pem`
   - `HOSTNAME_cms_net_encrypt.pem`
3. Create a folder on your computer for the Informix TLS/SSL keystore for JDBC access.

   For example, you can create the folder in the `C:\Program Files\HCL Informix Client SDK\ssl` directory.
4. Create the `conssl.cfg` file in the `C:\Program Files\HCL Informix Client SDK\etc\` directory.
5. Insert the following lines into the file:

   ```
   SSL_KEYSTORE_FILE <KeystorePath>\cms_ol.p12
   SSL_KEYSTORE_STH <KeystorePath>\cms_ol.sth
   ```

   `<KeystorePath>` is the folder you created in step 3.

   Do not use spaces in the path. Instead, use a shortened path name. Do not add single or double quotes around the path.
6. Save and close the file.
7. Open the Windows command line interface.
8. Navigate to the `<KeystorePath>` folder created in step 3.
9. Run the following command:

   ```
   gsk8capicmd_64 -keydb -create -db cms_ol.p12 -pw <KS_PASSWORD> -stash
   ```

   In this command, `<KS_PASSWORD>` is the password for the JKS keystore.
10. Run the following command for each SSL certificate file:

    ```
    gsk8capicmd_64 -cert -add -db cms_ol.p12 -stash -label cms_net_encrypt -file
    <SSL_CERT_FILE> -format ascii -trust enable
    ```
11. To create a keystore and add certificates for JDBC, run the following command for each SSL certificate file:

    ```
    keytool -importcert -file <SSL_CERT_FILE> -alias <ALIAS> -keystore cms_ol.ks
    -storepass <KS_PASSWORD>
    ```

    In this command, `<SSL_CERT_FILE>` is the SSL certificate file, `<ALIAS>` is the portion of the certificate file name after the first underscore, and `<KS_PASSWORD>`

is the password for the JKS keystore. For example, if the certificate file name is `HOSTNAME_cms_net_encrypt.pem`, then `cms_net_encrypt` is the alias portion.

Tip:

You can find keytool in the Java directory. Use the full path to run keytool. For example:

```
C:\Program Files\Java\jre1.8.0_172\bin\keytool.exe -importcert -file
<SSL_CERT_FILE> -keystore cms_ol.ks
```

12. Enter `yes` when prompted to trust this certificate.
13. Do the following to verify the keystore file permissions:
    a. In Windows Explorer, navigate to the keystore folder.
    b. Right-click the `cms_ol.p12` and `cms_ol.sth` files, and click **Properties**.
    c. Verify that any users who will run ODBC connections at least have Read permissions.
14. Do the following to update the ODBC data source protocol:
    a. From Control Panel, navigate to **Set up ODBC Data sources (32-bit)** or **Set up ODBC Data sources (64-bit)** as appropriate for your version of Windows.

       The ODBC Data Source Administrator window is dispalyed.
    b. Click the **System DSN** tab.
    c. Select the ODBC data source from the list.
    d. Click **Configure**.
    e. Click the **Connection** tab.
    f. In the **Protocol** list, select **olsocssl**.
    g. Click **Apply**.
15. Do the following to configure a TLS/SSL connection to the database from your Java application:
    a. Set the `javax.net.ssl.truststore` system property to point to the keystore that you created.

       For example:

       ```
       javax.net.ssl.trustStore=<KeystorePath>/cms_ol.ks
       ```
    b. Set the `javax.net.ssl.trustStorePassword` system property to the password that you used for the certificate.

       For example:

       ```
       javax.net.ssl.trustStorePassword=<KS_PASSWORD>
       ```
    c. Set a data source object.
    d. Set the port number to the SSL port 50000.
    e. Set the `setIfxSSLCONNECTION` data source property to `true`.

Updating the Informix encryption certificate on a Windows computer

About this task

When TLS/SSL encryption is updated, perform this procedure on the computer where the ODBC and JDBC client software is installed. You can use one of the following command options to update TLS/SSL encryption on the CMS server:

- Run `ids_tls_configure -u` to perform the update directly.
- Run `ids_tls_configure -r` followed by `ids_tls_configure -e` to remove and re-enable encryption.

Before you begin

- Ensure that the Informix Client SDK is installed on your computer.
- You need the path to the Informix TLS/SSL keystore for JDBC access.
- Ensure that you have the keystore password you used when installing the encryption certificate on your computer.

Procedure

1. Use WinSCP or a similar tool to copy the SSL certificate files from the CMS server to your computer.

   The SSL certificates are in the `/opt/informix/ssl` directory on the CMS server.

   The following is an example of the naming convention used if additional root and intermediate certificates exist:

   - `HOSTNAME_cert1.pem`
   - `HOSTNAME_cert2.pem`
   - `HOSTNAME_cms_net_encrypt.pem`

2. Open the Windows command line interface.
3. From the folder where the Informix TLS/SSL keystore is located, run `gsk8capicmd_64 -cert -list all -db cms_ol.p12 -stash` to view the configured certificates.

   For example, run the following command based on the keystore location:

   ```
   C:\Program Files\HCL Informix ClientSDK\ssl>
   gsk8capicmd_64 -cert -list all -db cms_ol.p12 -stash
   ```

   The following is an example of the output displayed:

   ```
   Certificates found
   * default, - personal, ! trusted, # secret key
   ! "CN=DigiCert SHA2 Secure Server CA,O=DigiCert Inc,C=US"
   ! "CN=DigiCert Global Root CA,OU=www.digicert.com,O=DigiCert Inc,C=US"
   - cms_net_encrypt
   ```

   The certificate alias is under the *default line.

4. Run the following command for each certificate:

   ```
   gsk8capicmd_64 -cert -delete -db cms_ol.p12 -stash -label <CERT_ALIAS>
   ```

   <CERT_ALIAS> is the certificate alias identified in the previous step.

5. Run the following command to view the certificates in the JDBC keystore:

   ```
   keytool -list -keystore cms_ol.ks -storepass <KS_PASSWORD>
   ```

   <KS_PASSWORD> is the password for the keystore.

   Tip:

   You can find keytool in the Java directory. Use the full path to run keytool. For example:

   ```
   C:\Program Files\Java\jre1.8.0_172\bin\keytool.exe -importcert
   -file <SSL_CERT_FILE> -keystore cms_ol.ks
   ```

6. From the command output, determine the alias for the configured certificates.

   The alias is the first part of each certificate line indicated by a date value. For example:

   ```
   Keystore type: PKCS12
   Keystore provider: SUN

   Your keystore contains 3 entries

   cert1, Oct 23, 2020, trustedCertEntry,
   Certificate fingerprint (SHA-256):
   15:4C:43:3C:49:19:29:C5:EF:68:6E:83:8E:32:36:64:A0:0E:6A:0D:82:2C:CC:95:8F:B4:DA:B
   0:3
   E:49:A0:8F

   cert2, Oct 23, 2020, trustedCertEntry,
   Certificate fingerprint (SHA-256):
   43:48:A0:E9:44:4C:78:CB:26:5E:05:8D:5E:89:44:B4:D8:4F:96:62:BD:26:DB:25:7F:89:34:A
   4:4
   3:C7:01:61

   cms_net_encrypt, Oct 23, 2020, trustedCertEntry,
   Certificate fingerprint (SHA-256):
   75:F4:E8:73:CE:EF:3C:B6:E3:0A:6F:76:2E:1B:71:C2:3B:C6:2B:75:8B:60:81:3F:D8:73:06:2
   9:E
   6:6C:63:DB
   ```

7. Run the following command for each certificate:

   ```
   keytool -delete -noprompt -alias <CERT_ALIAS> -keystore cms_ol.ks -storepass
   <KS_PASSWORD>
   ```

   <CERT_ALIAS> represents the aliases listed in the example above.

8. Run the following commands for each PEM certificate file copied from the CMS server:

   ```
   gsk8capicmd_64 -cert -add -db cms_ol.p12 -stash -label
   cms_net_encrypt -file <SSL_CERT_FILE> -format ascii -trust enable
   ```

   ```
   keytool -importcert -file <SSL_CERT_FILE> -alias <ALIAS>
   -keystore cms_ol.ks -storepass <KS_PASSWORD>
   ```

The alias is the portion of the SSL certificate file name after the first underscore. For example, if the certificate file name is `HOSTNAME_cms_net_encrypt.pem`, then the alias portion is `cms_net_encrypt`.

9. If you are prompted to trust the certificate, enter `yes`.

Chapter 7: Troubleshooting

This section presents general troubleshooting procedures and error messages for ODBC and JDBC.

Important:

If you choose to develop an application for the ODBC or JDBC driver, Avaya cannot provide support for that application or for any other third-party software or related mapping.

ODBC and JDBC encryption and certificates

This section provides the resolution for common ODBC and JDBC client and server communication issues:

Failure 1

You see the following error message:

```
Microsoft .NET Framework Unhandled exception: Access to registry key:
HKEY_LOCAL_MACHINE\SOFTWARE\Informix\SqlHosts
```

This exception might occur when executing the ODBC Data Sources program or the Informix Client-SDK ConnectTest program. A permission issue exists for the following registry key: `HKEY_LOCAL_MACHINE\SOFTWARE\Informix\SqlHosts`.

Resolution 1

Run the ODBC Data Sources program or Informix Client-SDK ConnectTest program as an administrator.

When you run the programs as administrator, an unhandled JIT exception may occur after resolution. This exception can be ignored and you can click **Continue** to finish running the program.

Failure 2

You see the following error message:

```
IBM Informix ODBC Error Message: GSK_KEYRING_OPEN_ERROR
```

This error occurs when executing an ODBC connection. This typically occurs when configuring the System DSN in the ODBC Data Sources program (and executing Apply & Test) or executing query in the ConnectTest program. An access issue exists to the file `cli_cms_ol.p12` or `cli_cms_ol.sth`, which are both referenced in the `conssl.conf` file.

Resolution 2

Verify the following:

- Double or single quotes are not used.
- The short path name is correct.
- There are no spaces in the path.
- The `SSL_KEYSTORE_FILE` and `SSL_KEYSTORE_STH` must have Read permissions at minimum.

Failure 3

You see the following error message:

```
HCL Informix ODBC Error Message: GSK_BAD_KEYFILE_PASSWORD
```

This error occurs when executing the ODBC Data Sources program or the Informix Client SDK ConnectTest program and you attempt to access the database. There is an access issue with the `cms_ol.sth` file, which is referenced in the `conssl.conf` file.

Resolution 3

Set Read permissions or higher for the `cms_ol.sth` file.

Failure 4

You see the following error message:

```
HCL Informix ODBC Error Message: GSK_ERROR_BAD_CERT
```

This error occurs with the ODBC connection. This typically occurs when configuring the System DSN in the ODBC Data Sources program or running a query in the ConnectTest program. The configured client certificate in the `cms_ol.p12` file, referenced in the `conssl.conf` file, is inconsistent with the CMS server database certificate.

Resolution 4

Peform the procedure Updating the Informix encryption certificate on a Windows computer on page 35.

Failure 5

You see the following error message:

```
HCL Informix ODBC Error Message: INFORMIXSERVER does not match either INFORMIXSERVER
or DATABASESERVERALIASES
```

This error occurs when trying to select a database or when running a query.

Resolution 5

The **Server** field must be `cms_net` or `cms_<hostname>`.

Failure 6

You see the following error message:

```
HCL Informix ODBC Error Message: Invalid message received during connection attempt
```

This error occurs when trying to connect or when running a query.

Resolution 6

If using an encrypted ODBC or JDBC connection, select **olsocssl** in the **Protocol** list.

When using a plain non-encrypted TCP ODBC or JDBC connection, select **olsoctcp** in the **Protocol** list.

Failure 7

You see the following error message:

```
HCL Informix ODBC Error Message: Database Locale mismatch.
```

Resolution 7

In the ODBC Data Sources program:

1. Click the **Environment** tab.
2. Click **Use Database Locale**.
3. Click **Apply**.
4. Run ConnectTest.

   The database connection is verified, so you can ignore the error.

Network support

Avaya does not control customer network configuration or ODBC-enabled client applications. Installation and ongoing maintenance support is limited to determining if data is being transferred correctly in the most basic client/server relationship. This is defined as a CMS system running ODBC on the same network hub as the client PC.

Verify that the trouble occurs on the same network subnet. Then continue with troubleshooting procedures. If the trouble does not occur on the same network subnet, contact the Avaya helpline.

Server log files and monitoring

The HCL Informix database logs information including failed ODBC login attempts to the server database log file.

The default location of the database log file is found at: `/opt/informix/cmsids.log`

CMS provides the following ODBC and JDBC encryption logging:

High-level logging (such as start, fail, or complete) is provided in the following log file:

`/cms/install/logdir/admin.log`

Detailed logging for all primary activities and errors is provided in the following log file:

`/cms/install/logdir/security/cms_sec.log`

To obtain the current HCL Informix IDS software version, perform the following steps while logged into the CMS server with an appropriately privileged user ID. For more information, see Providing secure access to the CMS database on page 22.

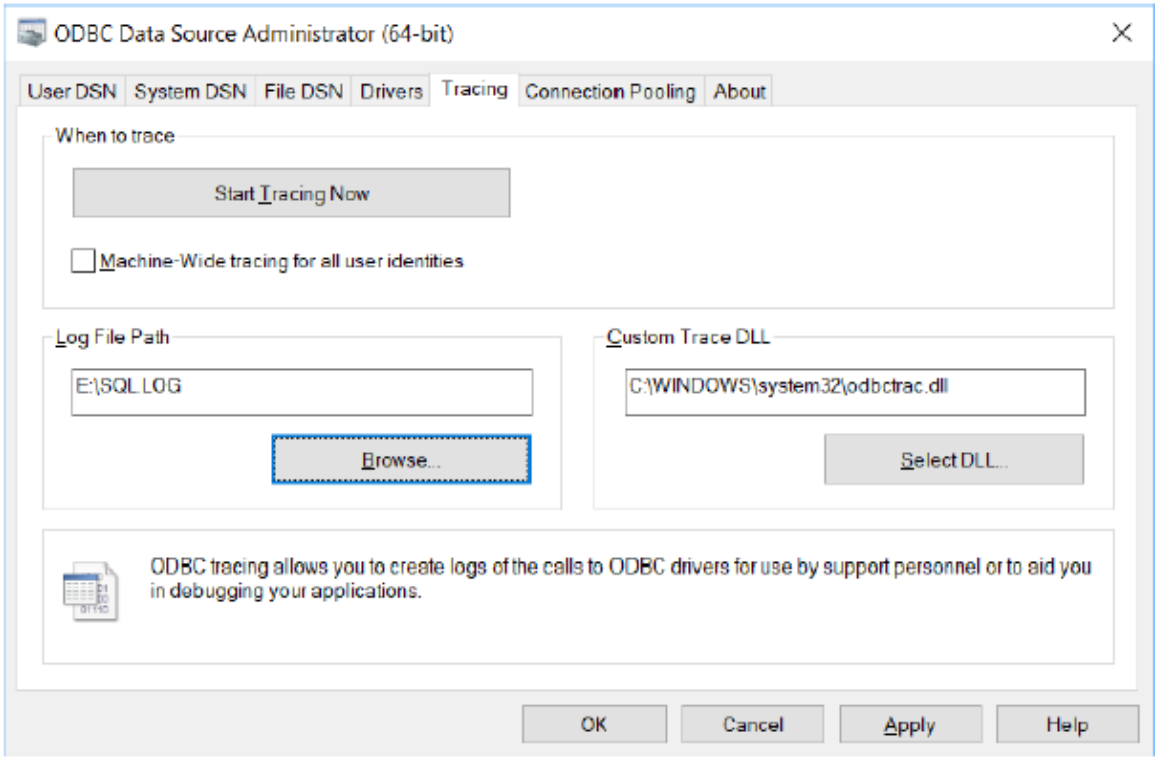
1. Set the environment: `. /opt/informix/bin/setenv`
2. View the current HCL Informix IDS version: `onstat -`

To monitor the active database sessions, perform the following steps while logged into the CMS server with an appropriately privileged user ID. For more information, see Providing secure access to the CMS database on page 22.

1. Set the environment: `. /opt/informix/bin/setenv`
2. View active database sessions: `onstat -g ses`
3. View the active sql statements: `onstat -g sql`

Client trace

The Windows ODBC Data Source Administrator (64-bit) configuration utility, located in the Windows **Control Panel** under **Administrative** tools, allows you to enable or disable ODBC trace logging under the **Tracing** tab.



Trace logging provides you with:

- Records of your entire ODBC session, including all ODBC calls made by the ODBC-compliant application you are using.
- Native database error messages that might not have been replaced by the ODBC-compliant application you were using.
- See: Configuring ODBC tracing options on page 18 for more information on configuring this utility.

Chapter 8: Resources

Documentation

CMS and CMS Supervisor documents

Title	Description	Audience
Overview		
Avaya Call Management System Overview and Specification	Describes tested product characteristics and product capabilities including feature descriptions, interoperability, performance specifications, security, and licensing requirements.	All users
Installation and maintenance		
Deploying Avaya Call Management System	Describes how to install and configure CMS in a virtualized VMware or KVM environment.	Implementation engineers, administrators
Deploying Avaya Call Management System in an Infrastructure as a Service Environment	Describes how to deploy CMS in an Amazon Web Services or Google Cloud Platform environment.	Implementation engineers, administrators
Maintaining and Troubleshooting Avaya Call Management System	Describes how to configure, maintain, and troubleshoot CMS.	Administrators, support personnel
Avaya Call Management System and Communication Manager Connections, Administration, and Troubleshooting	Describes how to connect and administer the Automatic Call Distribution (ACD) systems used by CMS.	Administrators, installation personnel, support personnel
Avaya Call Management System High Availability Connectivity, Upgrade and Administration	Describes how to connect to HA servers and upgrade to HA.	Administrators, installation personnel, software specialists involved with HA
Using Avaya Call Management System High Availability and Admin-Sync	Describes how to install and maintain your CMS High Availability (HA) system.	Administrators, support personnel
Upgrading		

Table continues…

Title	Description	Audience
Upgrading Avaya Call Management System	Describes the procedures required to upgrade to a new CMS release. This document is focused on full software or platform upgrades.	System administrators, implementation engineers
Avaya Call Management System Base Load Upgrade	Describes how to perform a simplified base load upgrade. You can perform a base load upgrade within a CMS release or for other approved scenarios. Not all releases support base load upgrades.	System administrators, implementation engineers
Administration		
Administering Avaya Call Management System	Provides instructions on administering a call center using CMS Supervisor.	Avaya support personnel, Administrators
Avaya Call Management System Call History Interface	Describes the format of the Call History data files and how to transfer these files to another computer.	Administrators, supervisors
Using ODBC and JDBC with Avaya Call Management System	Describes how to use Open Database Connectivity (ODBC) and Java Database Connectivity (JDBC) with CMS.	Administrators, support personnel
Avaya Call Management System Database Items and Calculations	Describes each database item and calculation that CMS tracks and how CMS calculates the values displayed on CMS reports and CMS Supervisor reports.	Administrators, support personnel
Avaya Call Management System Custom Reports	Describes how to design and create custom reports in CMS.	Administrators, report designers
Avaya Call Management System Security	Describes how to implement security features in CMS.	Administrators, support personnel
CMS Supervisor		
Avaya CMS Supervisor Clients Installation and Getting Started	Describes how to install and configure CMS Supervisor.	Implementation engineers, system administrators
Avaya CMS Supervisor Reports	Describes how to use CMS Supervisor reports.	Supervisors, administrators
Avaya CMS Supervisor Report Designer	Describes how to create new reports and to edit existing reports through Report Designer and Report Wizard.	Supervisors, administrators

Avaya Solutions Platform Documents

Title	Description	Audience
Avaya Solutions Platform Overview and Specification	Describes the key features of Avaya Solutions Platform server	All users

Table continues…

Title	Description	Audience
Installing the Avaya Solutions Platform 130 Series	Describes how to install Avaya Solutions Platform 130 Series servers.	Implementation engineers, solution architects, support personnel
Maintaining and Troubleshooting Avaya Solutions Platform 130 Series	Describes procedures to maintain and troubleshoot Avaya Solutions Platform 130 Series servers.	Implementation engineers, solution architects, support personnel

Finding documents on the Avaya Support website

Procedure

1. Go to https://support.avaya.com.
2. To log in, click **Sign In** at the top of the screen and then enter your login credentials when prompted.
3. Click **Product Support** > **Documents**.
4. In **Search Product**, start typing the product name and then select the appropriate product from the list displayed.
5. In **Select Release**, select the appropriate release number.

   This field is not available if there is only one release for the product.
6. **(Optional)** In **Enter Keyword**, type keywords for your search.
7. From the **Select Content Type** list, select one or more content types.

   For example, if you only want to see user guides, click **User Guides** in the **Select Content Type** list.
8. Click to display the search results.

Avaya Documentation Center navigation

For many programs, the latest customer documentation is available on the Avaya Documentation Center website at https://documentation.avaya.com. Some functionality is only available when you log in to the Avaya Documentation Center. The available functionality depends on your role.

Important:

If the documentation you are looking for is not available on the Avaya Documentation Center, you can find it on the Avaya Support website.

While navigating through the Documentation Center, you can click the **Avaya Documentation Center** logo at the top of the screen to return to the home page anytime. On the Avaya Documentation Center, you can do the following:

- Click **Avaya Links** in the top menu bar to access other Avaya websites, including the Avaya Support website.

- Click **Languages** ( ) in the top menu bar to change the display language and view localized documents.
- In the **Search Documentation** field, search for keywords and click **Filter** to filter by solution category, product, or user role.

  You can select multiple items in each filter category. For example, you can select a product and multiple user roles.
- Click **Library** in the top menu bar to access the complete library of documents. Use the filtering options to refine your results.
- After performing a search or accessing the library, you can sort content on the search results page. When you find the item you want to view, click it to open it.
- Use the table of contents in a document for navigation. You can also click **<** or **>** next to the document title to navigate to the previous topic or the next topic.
- Click **Share** ( ) to share a topic by email or copy the URL.
- Download a PDF of the current topic in a document, the topic and its subtopics, or the entire document.
- Print the section you are viewing.
- Add content to a collection by clicking **Add to My Topics** ( ). You can add the topic and its subtopics or add the entire publication.
- View the topics in your collections. To access your collections, click your name in the top menu bar and then click **My Topics**.

  You can do the following:

  - Create, rename, and delete a collection.
  - Set a collection as the default or favorite collection.
  - Save a PDF of the selected content in a collection and download it to your computer.
  - Share content in a collection with others through email.
  - Receive collections that others have shared with you.
- Click **Watch** ( ) to add a topic to your watchlist so you are notified when the content is updated or removed.
- View and manage your watchlist by clicking **Watchlist** from the top menu with your name.

  You can do the following:

  - Enable **Email notifications** to receive email alerts.
  - Unwatch the selected content or all topics.
- Send feedback for a topic.

Viewing Avaya Mentor videos

Avaya Mentor videos provide technical content on how to install, configure, and troubleshoot Avaya products.

About this task

Videos are available on the Avaya Support website, listed under the video document type, and on the Avaya-run channel on YouTube.

- To find videos on the Avaya Support website, go to https://support.avaya.com/ and do one of the following:
  - In **Search**, type `Avaya Mentor Videos`, click **Clear All** and select **Video** in the **Select Content Type**.
  - In **Search**, type the product name. On the Search Results page, click **Clear All** and select **Video** in the **Select Content Type**.

    The **Video** content type is displayed only when videos are available for that product.

  In the right pane, the page displays a list of available videos.
- To find the Avaya Mentor videos on YouTube, go to www.youtube.com/AvayaMentor and do one of the following:
  - Enter a keyword or keywords in the **Search Channel** to search for a specific product or topic.
  - Scroll down Playlists, and click a topic name to see the list of videos available. For example, Contact Centers.

Note:

Videos are not available for all products.

Support

Go to the Avaya Support website at https://support.avaya.com for the most up-to-date documentation, product notices, and knowledge articles. You can also search for release notes, downloads, and resolutions to issues. Use the online service request system to create a service request. Chat with live agents to get answers to questions, or request an agent to connect you to a support team if an issue requires additional expertise.

Using the Avaya InSite Knowledge Base

The Avaya InSite Knowledge Base is a web-based search engine that provides:

- Up-to-date troubleshooting procedures and technical tips.
- Information about service packs.

- Access to customer and technical documentation.
- Information about training and certification programs.
- Links to other pertinent information.

If you are an authorized Avaya Partner or a current Avaya customer with a support contract, you can access the Knowledge Base without extra cost. You must have a login account and a valid Sold-To number.

Use the Avaya InSite Knowledge Base for any potential solutions to problems.

1. Go to https://support.avaya.com.
2. To log in, click **Sign In** at the top of the screen and then enter your login credentials when prompted.
3. Click **Product Support** > **Products**.
4. In **Search Product**, start typing the product name and then select the appropriate product from the list displayed.
5. Select the release number, if applicable.
6. Click the **Technical Solutions** tab to view articles for resolving technical issues.

Glossary

Abandoned call	A call in which a caller hangs up before receiving an answer from an agent. The call can be queued to a split/skill or in a vector/vector directory number (VDN) or ringing at an agent before it is abandoned.
Access permissions	Permissions assigned to a Call Management System (CMS) user so that the user can access different subsystems in CMS or administer specific elements (splits/skills, trunks, vectors, and so on) of the ACD. Access permissions are specified as read or write permission. Read permission means the CMS user can access and view data (for example, run reports or view the Dictionary subsystem). Write permission means the CMS user can add, modify, or delete data and execute processes.
ACD Call	A call that queued to a split/skill and was answered by an agent in that split/skill,or a call that queued as a direct agent call and was answered by the agent for whom it was queued.
Adjunct/Switch Applications Interface (ASAI)	An open application interface through which processors and switches can jointly provide services that require applications to initiate, receive, and control calls or make use of switch features. (See Open Application Interface.)
After Call Work (ACW)	An agent state generally representing work related to the preceding ACD call.
Application Programming Interface (API)	A set of related functions that a computer programmer uses to obtain some kind of service from another piece of software. Programmers of Windows based applications use the Windows API to create windows, draw text on the screen, access files, and perform all other services provided by Windows. Despite the use of the word application in this term, applications might not be the only software using an API; lower-level software components such as network drivers also have APIs, but these components are not “applications” and are not used directly by applications.
Automatic Call Distribution (ACD)	A switch feature using software that channels high-volume incoming and outgoing call traffic to agent groups (splits or skills). Also an agent state where the extension is engaged on an ACD call.

Avaya Supervisor	The Call Management System application for the Microsoft Windows operating environment.
Backup	The process of protecting data by writing the contents of the disk to an archive (or tape) that can be removed from the computer environment and stored safely.
Calculation	The abbreviated name (calculation name) for the formula calculation that generates the data for a field in a report.
Call Management System (CMS)	A software product used by business customers that have Avaya telecommunications switches and receive a large volume of telephone calls that are processed through the Automatic Call Distribution (ACD) feature of the switch. The CMS collects call-traffic data, formats management reports, and provides an administrative interface to the ACD feature in the switch.
Call Management System Query Language (CMSQL)	A tool that allows direct queries of the historical database. This tool is the interactive interface typically used to view the Informix database. For CMS purposes, CMSQL is used instead of Informix SQL.
Call Vectoring	A switch feature that provides a highly flexible method for processing ACD calls. A call vector is a set of instructions that controls the routing of incoming and outgoing calls based on current conditions. Examples of call vector conditions include time of day and the number of calls in queue.
Call Work Code (CWC)	An ACD capability that allows the agent to enter a string of digits during or after the call and send them to CMS for management reporting.
CMS database	A group of files that store ACD data according to a specific time frame: current and previous intrahour real-time data and intrahour, daily, weekly, and monthly historical data.
CMS database tables	CMS uses these tables to collect, store, and retrieve ACD data. Standard CMS items (database items) are names of columns in the CMS database tables.
Current interval	Represents the current intrahour interval, which can be 15, 30, or 60 minutes. The current interval is part of the real-time database. CMS starts collecting ACD cumulative data at the beginning of the interval (on the hour, half-hour, or quarter hour) and continues collecting ACD cumulative data until the end of the interval. When the current interval changes, all cumulative data is cleared and CMS begins counting cumulative data again starting from zero. The length of the interval is set in the System Setup: Storage Intervals window and is called the intrahour interval.
Daily data	Interval data that has been converted to a 1-day summary.

Database item	A name for a specific type of data stored in one of the CMS databases. A database item can store ACD identifiers (split numbers or names, login IDs, VDNs, and so on) or statistical data on ACD performance (number of ACD calls, wait time for calls in queue, current states of individual agents and so on).
Database Management System (DBMS)	The software that manages access to structured data. For example, the Microsoft SQL Server is a database management system. Database management system can also be used generally to include PC database products such as Microsoft Access, as well as any other software that can provide data access services.
Dictionary	A CMS subsystem that can be used to assign names to various call center elements such as login IDs, splits/skills, trunk groups, VDNs and vectors. These names are displayed on reports, making them easier to interpret. Dictionary also allows customized calculations to be created for use in reports.
Driver manager	A dynamic link library that loads drivers on behalf of an application.
Dynamic link library	A dynamic link library is another name for a driver or a driver manager. A dynamic link library is specific to the DBMS of the data being accessed. For example, an Informix specific dynamic link library will be used to access data in an Informix database, such as the CMS database.
Entity	A generic term that refers to one of the following: Agent, Split/Skill, Trunk, Trunk Group, VDN, or Vector.
Exception	A type of activity in the ACD which falls outside the limits you have defined. An exceptional condition is defined in the CMS Exceptions subsystem, and usually indicates abnormal or unacceptable performance of the ACD (by agents, splits/ skills, VDNs, vectors, trunks, or trunk groups).
Historical database	A database that contains intrahour records for up to 62 days, daily records for up to 5 years, and weekly/monthly records for up to 10 years for each CMS table.
Historical reports	Reports that display past ACD data for various CMS tables.
Informix	A relational database management system used to organize CMS historical data.
Informix SQL	A query language tool that is used to extract data from an Informix database.
Intrahour interval	A 15-, 30-, or 60-minute segment of time starting on the hour. An intrahour interval is the basic unit of CMS report time.

Local area network (LAN)	A private interactive communication network that allows computers to communicate over short distances, usually less than one mile, at high data transfer rates from 1 Mbps to as high as 100 Mbps.
Monthly data	Daily data that has been converted to a monthly summary.
Open Database Connectivity (ODBC)	Open Database Connectivity is a standard application programming interface (API) for accessing data in both relational and non-relational databases.
Previous interval	Represents one intrahour interval and is part of the real-time database. At the end of each intrahour interval, the contents of the current intrahour interval are copied to the previous intrahour interval portion of the real-time database.
Read permission	The CMS user with read permission can access and view data (for example, run reports or view the Dictionary subsystem). Read permission is granted from the User Permissions subsystem.
Real-time database	Consists of the current and previous intrahour data on each CMS-measured agent, split/skill, trunk, trunk group, vector, and VDN.
Single-user mode	Only one person can log into CMS. Data continues to be collected if data collection is “on.” This mode is required to change some CMS administration.
Structured query language (SQL)	A language used to interrogate and process data in a relational database (such as Informix).
Switch	A private switching system providing voice-only or voice and data communications services (including access to public and private networks) for a group of terminals within a customer's premises.
Trunk	A telephone line that carries calls between two switches, between a Central Office (CO) and a switch, or between a CO and a phone.
Trunk group	A group of trunks that are assigned the same dialing digits - either a phone number or a Direct Inward Dialed (DID) prefix.
Vector	A list of steps that process calls in a user-defined manner. The steps in a vector can send calls to splits/skills, play announcements and music, disconnect calls, give calls a busy signal, or route calls to other destinations. Calls enter vector processing via VDNs, which can have received calls from assigned trunk groups, from other vectors, or from extensions connected to the switch.
Vector directory number (VDN)	An extension number that enables calls to connect to a vector for processing. A VDN is not assigned an equipment location. It is assigned to a vector. A VDN can connect calls to a vector when the calls arrive over an assigned automatic-in trunk group, dial-repeating (DID) trunk group, or

	ISDN trunk group. The VDN by itself can be dialed to access the vector from any extension connected to the switch.
Weekly data	Daily data that has been converted to a weekly summary.
Write permission	The CMS user can add, modify, or delete data and execute processes. Write permission is granted from the User Permissions subsystem.

Index

O

P

R

S

T

U

V

W