CDR Analysis and reporting tool

The Cisco Unified Communications Manager CDR Analysis and Reporting (CAR) tool generates reports of information for quality of service, traffic, user call volume, billing, and gateways.

Generate CDR Analysis and reporting

Generate CDR Analysis and reporting, on page 1 provides an overview of the steps for configuring CDR Analysis and Reporting.

Table 1: CAR Configuration Checklist

Configuration Steps		Related Procedures and Topics
	Activate the CDR services on the appropriate servers.	Activate CAR, on page 3
	Configure the CDR Repository Manager.	See the "Configuring CDR Repository Manager" chapter in the Cisco Unified Serviceability Administration Guide.

Configuration Steps		Related Procedures and Topics
	Enable the following Cisco Unified Communications Manager enterprise parameters: • **CDR File Time Interval** • **Cluster ID** • Allowed CDRonDemand get_file Queries Per Minute • **Allowed CDRonDemand get_file_list Queries Per Minute**	CDR enterprise parameters, on page 5
	Enable the Cisco Unified Communications Manager service parameters, **CDREnabled Flag** and **CallDiagnosticsEnabled, to ensure that the CDR records write to flat files and that CMR records are created**. Enable any of the following service parameters that are required for your specific installation: **Add Incoming Number Prefix to CDR**, **CDR Log Calls with ZeroDurationFlag**, **Display FAC in CDR**, and **Show Line Group Member DN in finalCalledPartyNumber CDR Field**.	CDR service parameters, on page 6
	Set up CAR administrators, managers, and users in Cisco Unified CM Administration.	Generate CAR users, on page 8
	Configure CAR system parameters for report generation: • Configure mail server. • Configure dial plan. • Configure gateway. • Set system preferences.	• Set up mail server parameters • Set up dial plan • Set up gateway • Set up system preferences
	Specify the value ranges that you consider good, acceptable, fair, and poor for jitter, latency, and lost packets.	CAR reports QoS values
	If desired, set a base monetary rate for the cost of calls on the basis of a time increment. You can further qualify the cost by applying the time-of-day and voice-quality factors.	CAR rating engine
	Enable the reports that you want to automatically generate by using the Automatic Generation/Alert Option window.	Automatic generation of CAR reports and alerts

Configuration Steps		Related Procedures and Topics
	Configure the CAR system scheduler to schedule when CAR loads CDRs as well as daily, weekly, and monthly reports.	CAR system scheduler
	Set the parameters for automatic purging of the CAR database. You can set the percentage of the CAR database that you want the system to use for CAR data and the age of CAR data that you want to delete when the CAR data exceeds the database size limit. You can disable automatic database purging, but the system enables purging by default.	CAR system database
	Set up the generation of event logs.	Generate event log
	Set the charge limit notification that indicates when the daily charge limit for a user exceeds the specified maximum and the QoS notification that indicates when the percentage of good calls drops below a specified range or the percentage of poor calls exceeds a specified limit.	CAR reports notification limits
	If your users want to view localized user and manager reports, install the proper locales.	Cisco Unified Communications Operating System Administration Guide
	Back up CAR, including the database and the pregenerated reports. Use the Cisco Unified Communications Manager Disaster Recovery System (DRS).	Backup database

Related Topics

Activate CAR

CAR comprises a group of complementary services, which you can activate in the Service Activation window in Cisco Unified Serviceability. Before you can launch CAR from the Tools menu in Cisco Unified Serviceability, you must activate the CAR services by using the following procedure.

Procedure

Step 1   Choose **Tools** > **Service Activation**.
The Service Activation window appears.

Step 2   Go to the Servers drop-down list box:

- For Cisco Unified Communications Manager, choose the first node of the cluster server name.

The window displays the service names for the server that you chose, the service type, and the activation status of the services.

Step 3 Check the check boxes next to the following CDR Services:

a) Cisco SOAP-CDRonDemand Service (optional). If you are using a third-party billing application that accesses CDR data via an HTTPS/SOAP interface, activate this service.

b) Cisco CAR Web Service

    Tip Unchecking the check boxes next to the CDR Services and clicking **Update** deactivates the services. If you deactivate the Cisco CAR Web Service, the system removes CAR from the Tools menu in Cisco Unified Serviceability.

Step 4 After you have finished making the appropriate changes, click **Update**.

Related Topics

CDR repository manager

The CDR Repository Manager sends CDR files to up to three preconfigured destinations (billing servers) using FTP/SFTP. It also maintains files on disk to make sure the storage usage does not exceed predefined limits. If you exceed the predefined limits, the CDR Repository Manager deletes old files to reduce the disk usage to the preconfigured low mark. Files get preserved for a certain number of days based on configuration. Files that are old enough to fall outside of the preservation window get automatically deleted.

Note Cisco allows you to use any SFTP server product but recommends SFTP products that have been certified with Cisco through the Cisco Technology Developer Partner program (CTDP). CTDP partners, such as GlobalSCAPE, certify their products with specified version of Cisco Unified Communications Manager.

Cisco uses the following servers for internal testing. You may use one of the servers, but you must contact the vendor for support:

- Open SSH

- Cygwin

- Titan

Note For issues with third-party products that have not been certified through the CTDP process, contact the third-party vendor for support.

Cisco has tested and will support the following versions of FTP or SFTP for CAR billing servers:

- Linux/Unix

◦ FTP: Unix (SunOS 5.6 Generic_105181-10) and Linux server (2.4.21-47.ELsmp and 2.6.9-42.7.ELsmp)

◦ SFTP: Unix (SunOS 5.6 Generic_105181-10) and Linux server (2.4.21-47.ELsmp and 2.6.9-42.7.ELsmp)

• Windows

◦ FTP: Microsoft FTP service (Windows 2000 5.00.2195 sp4, IIS 5.0) and WAR FTP Daemon (1.82.0.10)

Use the CDR Management configuration window in Cisco Unified Serviceability to configure the following items:

• Set the amount of disk space to allocate to call detail record (CDR) and call management record (CMR) files.

• Configure the high water mark (HWM) and low water mark (LWM).

• Configure the number of days to preserve CDR/CMR files before deletion.

• Disable CDR/CMR files deletion based on the HWM.

To access the CDR Repository Manager configuration window, open Cisco Unified Serviceability and choose **Tools** > **CDR Management**.

See the "CDR Repository Manager" chapter in the Cisco Unified Serviceability Administration Guide for additional information.

Related Topics

CDR enterprise parameters

Configure these CDR parameters on the Enterprise Parameters Configuration window in Cisco Communications Manager Administration. To access the Enterprise Parameters Configuration window, open Cisco Unified Communications Manager and choose **System** > **Enterprise Parameters**.

• CDR Parameters

◦ **CDR File Time Interval** - This parameter specifies the time interval for collecting CDR data. For example, if this value is set to 1, each file will contain 1 minute of CDR data (CDRs and CMRs, if enabled). The CDR database will not receive the data in each file until the interval has expired, so consider how quickly you want access to the CDR data when you decide what interval to set for this parameter. For example, setting this parameter to 60 means that each file will contain 60 minutes of data, but that data will not be available until the 60-minute period elapses, and the records are written to the CDR database. The default value specifies 1. The minimum value specifies 1, and the maximum value specifies 1440. The unit of measure for this required field represents a minute. You can set the parameter time interval to collect CDR data at any time you want. The newly set value comes into effect after generating the last flatfile with the previous parameter value. You need not restart the Cisco CallManager Service to generate flatfiles with the new value. In case the Cisco CallManager Service restarts on a specific system, the flatfile that is

in the progress state is written successfully, irrespective of the existing interval. When the Cisco CallManager Service resumes, it will use the newly set value to generate flatfiles.

◦ **Cluster ID** - This parameter provides a unique identifier for the server or cluster. Because the parameter gets used in CDRs, collections of CDRs from multiple clusters can be traced to the sources. The default value specifies StandAloneCluster. The maximum length comprises 50 characters and provides a valid cluster ID that comprises any of the following characters: A-Z, a-z, 0-9, . -.

• CCM Web Services Parameters

◦ **Allowed CDRonDemand get_file Queries Per Minute** - This parameter specifies the maximum number of CDRonDemand get_file queries that are allowed per minute for the system. For this required field, the default value specifies 10. The minimum value equals 1, and the maximum value equals 20.

◦ **Allowed CDRonDemand get_file_list Queries Per Minute** - This parameter specifies the maximum number of CDRonDemand get_file_list queries that are allowed per minute for the system. For this required field, the default value specifies 20. The minimum value equals 1, and the maximum value equals 40.

See the .

CDR service parameters

CAR relies on the data in the CDR and CMR records to generate both the CAR and CDR reports. CAR requires that the CDRs be available in flat files on the server where you access CAR. To ensure that the CDR records are generated, and generated in the manner you can use for your particular system, you must enable certain Cisco Unified Communications Manager service parameters:

You can configure these parameters on the Service Parameters Configuration window in Cisco Unified CM Administration. To access the Service Parameters Configuration window, open Cisco Unified CM Administration and choose **System** > **Service Parameters**. Choose the **Advanced** button to display the complete list of Service Parameters. The following list of service parameters can affect CDR/CMR records:

• System Parameters

◦ **CDR Enabled Flag -** This parameter determines whether CDRs are generated. Valid values specify True (CDRs are generated) or False (CDRs are not generated). For this required field, the default value specifies False. Enable this parameter on all servers.

◦ **CDR Log Calls With Zero Duration Flag -** This parameter enables or disables the logging of CDRs for calls which were never connected or which lasted less than 1 second. Cisco Unified Communications Manager logs unsuccessful calls (calls that result in reorder, such as might occur because of a forwarding directive failure or calls that attempt to go through a busy trunk) regardless of this flag setting. This represents a required field. The default value specifies False.

• Clusterwide Parameters (Device - General)

◦ **Call Diagnostics Enabled -** This parameter determines whether the system generates call management records (CMRs), also called diagnostic records. Valid values specify Disabled (do not generate CMRs), Enabled Only When CDR Enabled Flag is True (generate CMRs only when the CDR Enabled Flag service parameter is set to True), or Enabled Regardless of CDR Enabled

Flag (generates CMRs without regard to the setting in the CDR Enabled Flag service parameter). This represents a required field. The default value specifies Disabled.

◦ **Display FAC in CDR** - This parameter determines whether the Forced Authorization Code (FAC) that is associated with the call displays in the CDR. Valid values specify True (display authorization code in CDRs) or False (do not display authorization code in CDRs) for this required field. The default value specifies False.

◦ **Show Line Group Member DN in finalCalledPartyNumber CDR Field** - This parameter determines whether the finalCalledPartyNumber field in CDRs shows the directory number (DN) of the line group member who answered the call or the hunt pilot DN. Valid values specify True (the finalCalledPartyNumber in CDRs will show the DN of the phone that answered the call) or False (the finalCalledPartyNumber in CDRs will show the hunt pilot DN). This parameter applies only to basic calls that are routed through a hunt list without feature interaction such as transfer, conference, call park, and so on. This parameter does not apply to Cisco Unified Communications Manager Attendant Console. The default value for this required field specifies False.

• Clusterwide Parameters (Device - Phone)

◦ **Add Incoming Number Prefix to CDR** - This parameter determines whether Cisco Unified Communications Manager adds the incoming prefix (as specified in the National Number Prefix, International Number Prefix, Subscriber Number Prefix, and Unknown Number Prefix service parameters) to the calling party number in the CDRs for that call. If the prefix is applied on the inbound side of the call, it always will be added to the calling party number in the CDRs for that call, even if this parameter is set to False. If the prefix is applied on the outbound side, the prefix will be added to the calling party number in the CDR(s) for that call, only if this parameter is set to True. If the destination of the call is a gateway, Cisco Unified Communications Manager will not add the prefix to the CDRs even if this parameter is enabled. This parameter applies cluster wide. The default value for this required field specifies False.

◦ displays an example of how this service parameter works. The following table shows values of the prefix that are applied on the inbound and outbound side of the call.

	Inbound Side of Call	Outbound Side of Call
National Number Prefix	1214	
International Number Prefix		011
Subscriber Number Prefix	214	
Unknown Number Prefix		972

If the service parameter **applyIncomingPrefixToCDR** is disabled, the CDR will contain the prefix that is added to the calling party number when the type of number for the call is

• National number.

• Subscriber number.

If the service parameter **applyIncomingPrefixToCDR** is enabled, the CDR will contain the prefix that is added to the calling party number when the type of number for the call is

- National number.

- International number only when the destination is not a gateway.

- Subscriber number.

- Unknown number only when the destination is not a gateway.

Related Topics

CAR system settings

CDR Analysis and Reporting sets default values for all system parameters. Before you generate any reports in CAR, Cisco recommends that you customize several system parameters. Because default values are provided for all system parameters, Cisco recommends customizing but does not require it.

> **Note** The following system parameters refer to the CAR system parameters. Be aware that they are separate and distinct from the Cisco Unified Communications Manager enterprise and service parameters that are discussed in the previous sections.

CAR allows you to set the following parameters:

- Mail server criteria - CAR uses this information to successfully connect to the e-mail server to send alerts and reports by e-mail. If you do not want to send alerts or reports by e-mail, you do not need to specify this information.

- Dial plan - The default dial plan in CAR specifies the North American numbering plan (NANP). Ensure the dial plan is properly configured, so call classifications are correct in the reports. If you have modified the default NANP that Cisco Unified CM Administration provides, or if you are outside the NANP, be sure to configure the dial plan according to your Cisco Unified Communications Manager dial plan.

- Gateways - To utilize the gateway reports, you need to configure gateways in CAR. You should do this after installation of any existing gateways in your Cisco IP telephony system and when you add gateways to the system. If the system deletes any gateways, CAR gets the latest list of gateways, and any configuration that is specified in CAR for the deleted gateways gets deleted. CAR uses the area code information to determine whether calls are local or long distance. You must provide the Number of Ports information for each gateway to enable CAR to generate the Utilization reports.

- System preferences - You can set CAR system preferences for the Company Name parameter.

See the .

Generate CAR users

Any user can act as a CAR administrator (including application users); however, you must add the end user to the Cisco CAR Administrators User Group in Cisco Unified CM Administration (Standard CAR Admin

Users). End users who have been identified as CAR administrators have full control over the CAR system. The administrator can modify all the parameters that relate to the system and the reports. End users who have not been identified as CAR administrators can access only designated CAR reports.

Note An application user that acts as a CAR administrator can configure all reports except the Individual Bill report. An application user that acts as a CAR administrator cannot access end user (CCM user) windows. CAR notifications do not get sent to the application user because no mail ID exists for the application user.

Tip To use CAR, ensure at least one CAR administrator exists in the Cisco Unified Communications Manager database.

Before you log in to CAR, you must configure at least one CAR user that has administrative privileges in CAR. To configure CAR administrators, managers, and users, perform the following procedure:

Procedure

Step 1 In Cisco Unified CM Administration, add an end user by choosing **User Management** > **End User**. For additional information on how to perform this task, see the *Cisco Unified Communications Manager Administration Guide*. To create a manager, make sure that you enter a value in the Manager User ID field.

Note After creating the End User, edit the user password credentials by clicking the button **Edit Credentials** near the password text box. Uncheck the **User Must Change at Next Login** check box. If this action is not taken, you will get IMS_ERROR_CODE_5 (See Log on to CAR, on page 10 for the Log on to CAR, on page 10) and will not be allowed to log in to CAR. Then, you must log in to Cisco Unified CM Administration to manually reset the password.

Tip Cisco recommends that you configure at least one CAR user that has administrative privileges in CAR before you start using CAR. If you have not configured a CAR administrator or want to configure another CAR administrator, continue with this procedure.

Step 2 Choose **User Management** > **User Group**; click **Find**.
The Find and List User Groups window displays.

Step 3 Click **Standard CAR Admin Users**.
The CAR User Group window displays.

Step 4 Click the **Add End Users to Group** button.

Step 5 Check the check box(es) for the users that you want to add to the group and click **Add Selected**.
The user displays in the Users in Group group box.

Tip To revoke CAR administrative privileges, check the check box of the user in Users in Group group box and click **Delete Selected**. When the warning message displays, click **OK**. The system revokes the privileges immediately.

Related Topics

Related topics, on page 13

Log on to CAR

Only CAR administrators and normal end users can log on to the CAR web interface. Users do not need to be a member of a standard CAR administrator group to be a CAR administrator. Any user who has the role "Standard Admin Rep Tool Admin" associated with the user ID can access CAR as a CAR administrator. The user ID role association gets done by adding the user to a user group that has the role associated with it. "Standard CAR Admin Group" and "Standard CCM Super Users" comprise two groups that have the role "Standard Admin Rep Tool Admin" associated with them. The default application user that gets created at installation, who is a member of the "Standard CCM Super Users" group, can log in to CAR as a CAR administrator but only as an application user. This user cannot access the Individual Bills report.

CAR supports custom CAR Admin groups. Any custom group that has the role "Standard CAR Admin Group" associated with it can add users who are considered to be CAR administrators when logging into the CAR web interface.

End users who are not CAR administrators can log in to CAR only if they have the role "Standard CCM End Users" associated with them. You can do this user ID - role association by adding the end user to the "Standard CCM End Users" group or any other group that has the specified role associated. Any end user without the "Standard CCM End Users" group association cannot log in to the CAR web interface.

Any user without the "Standard CCM End Users" or "Standard Admin Rep Tool Admin" role cannot log in to CAR. An attempt by this user to log in to CAR generates a 403 error, and the user gets redirected to the login window with no error message. CAR Web Service traces will log the username of the user who tried to access the application.

CAR facilitates users to change their password by using a Change Password window if the user password has expired. When users with an expired password try to log into CAR, they receive IMS_Error_Code 5, 6, or 8. CAR uses the ChangePasswordFilter of ccmadmin to redirect the user to change-password.jsp when any of the preceding error codes are received.

> **Note** The database throttle limits the concurrent users to 100; because of this limit, IMS also supports only 100 users with a login rate of approximately 112 ms.

If an error occurs while you are resetting the user password, the following message displays on the Change-Password window: "System error while changing password for user. Please contact system administrator."

Even though the CAR Administrator status extends to any user with the role "Standard Admin Rep Tool Admin," CAR notifications, alerts, and pregen reports only get sent to users who are members of the group "Standard CAR Admin Group" and not all CAR administrators.

To log on to CAR, perform the following procedure:

Before You Begin

Perform the following tasks:

- Before you can log in to CAR, verify that the Cisco CAR Web Service and the Cisco CAR Scheduler service run on the first server.After you activate the services, the option CDR Analysis and Reporting displays under the Tools menu in Cisco Unified Serviceability. For information on how to activate services, see the Activate CAR, on page 3.

- Configure CAR administrators, managers, and users as described in Generate CAR users, on page 8.

Procedure

Step 1 To log on to CAR, perform one of the following tasks:

   a) For CAR system administrators only - From Cisco Unified Serviceability, choose **Tools** > **CDR Analysis and Reporting**.

   b) For CAR users or administrators - From the web browser, enter **https://<Server-ip/name>:8443/car/**

Step 2 After the CAR logon window displays, enter your user ID in the User Name field.

Step 3 In the Password field, enter your password. Click **Login**.
The CAR window displays.

If the user ID or password is invalid, CAR displays one of the Identity Management System (IMS) messages that are listed in .

Table 2: CAR Invalid Logon Messages

Error Code	Message
IMS_ERROR_CODE 1	Either the User Name or the Password entered is invalid. Ensure that you are logging into CAR as a CAR administrator or a regular End User.
IMS_ERROR_CODE 2	The account has been locked by System Administrator. Please contact the administrator.
IMS_ERROR_CODE 3	The account has been temporarily locked. Please contact the System Administrator or try after sometime.
IMS_ERROR_CODE 4	The account has been deactivated due to lack of activity. Please contact the System Administrator.
IMS_ERROR_CODE 5	The account has been locked as the password has expired. Please reset the password or contact the System Administrator.
IMS_ERROR_CODE 6	The account has been locked as the password has expired. Please contact the System Administrator.
IMS_ERROR_CODE 7 = ERROR: LDAP_INACTIVE	The system has changed over to using LDAP authentication and the user is still in the old database. Please contact the System Administrator. This error code is not used for Cisco Unified Communications Manager Business Edition 5000.
IMS_ERROR_CODE 8	The account has been locked as the user needs to log in manually and change the credential first. Please reset the password from the Cisco Unified Communications Manager Administration page or contact the System Administrator.

Error Code	Message
IMS_ERROR_CODE UNKNOWN	System error. Please contact the System Administrator.
IMS_EXCEPTION (any exception returned by IMS) = AUTHENTICATION FAILURE	Unable to Authenticate User due to System Error. Please contact System Administrator.

After you log on to CAR, the following warning messages are displayed on a dashboard, if any:

1 Displays a list of nodes where CallManager service is activated but **CDR Enabled** flag is not enabled. Also, specifies that the CDRs will not be generated on the listed nodes.

2 If cluster wide parameter **Call Diagnostics Enabled** flag is disabled, it displays that the flag is disabled and states that the QoS information will not be generated on calls.

3 Displays the status of CAR Scheduler service and Cisco Repository Manager Service, if they are stopped on publisher.

4 Displays the breach status, if either the limit 2M or HWM is breached.

5 Displays the status of CDR loader.

a) If the loader is disabled, it states that the loader is disabled.
b) If the loader is enabled, it checks for the last load status of CDR loader. If the last load status of CDR loader is failed, it displays that the loading of CDR loader is failed and informs you to check the CAR scheduler logs.

1 If any of the Tbl_System_Preferences table columns does not have expected values, the dashboard displays the exceptions along with a **Restore Defaults** button. You can click the **Restore Defaults** button, to populate the Tbl_System_Preferences table with default values required for the smooth functioning of CAR loader and reports.

The following list of notice messages are displayed on the dashboard, if any:

2 If **CDR Log Calls with Zero Duration** flag is activated, the dashboard displays that the flag is activated, and states that large number of CDRs of zero duration may be generated. Due to this, the billing tables may be filled quickly which in turn cause the 2M or HWM limit to be breached soon.

3 Displays whether the loader schedule is continuous or intermittent.

4 If CDR Load Only option is selected in the CDR Load page, the dashboard states that CMRs are not loaded into CAR database.

5 If the mail parameters are not configured, the dashboard displays that you have not configured the mail parameters and provides the path for configuring the mail parameters.

6 If the mail ID of CAR Administrator is not configured, the dashboard displays that you have not configured the mail ID of CAR Administrator.

7 Displays the following status of Billing tables:

  • Number of records present in Tbl_Billing_Data.

  • Number of records present in Tbl_Billing_Error.

• Maximum and minimum date of Tbl_Billing_Data and Tbl_Billing_Error tables.

Related Topics

Log out of CAR

This section describes how to log out of CAR.

Procedure

Step 1 At the CAR window, choose **Logout**.

Step 2 A prompt message "For security reasons, it is advisable to close the browser window on Logout. Do you want to close the browser window?" displays. To close the CAR window (browser), click **OK**; clicking Cancel displays the CAR Logon window.

Related Topics

Related topics

• CDR Analysis and reporting

Additional documentation

• Cisco Unified Communications Operating System Administration Guide

• Cisco Unified Serviceability Administration Guide

• Cisco Unified Communications Manager Call Detail Records Administration Guide