CPS Policy Reporting Guide, Release 20.2.0

First Published: 2020-08-27

Last Modified: 2020-08-27

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/c/en/us/about/legal/trademarks.html. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2020 Cisco Systems, Inc. All rights reserved.

CONTENTS

PREFACE

Preface v

About This Guide v

Audience v

Additional Support vi

Conventions (all documentation) vi

Communications, Services, and Additional Information vii

Important Notes viii

CHAPTER 1

Policy Reporting Overview 1

Features 1

Policy Reporting Interface 1

JDBC CDR (Call Data Record) Replication 2

CSV Replication 2

Realtime CSV Replication 2

Reporting Server 2

CHAPTER 2

Reporting Plug-in Configuration 3

Install Policy Reporting Plug-in 3

Configure Policy Reporting Plug-in 4

Configure a Reporting Server 5

Replicate JDBC CDR 6

Replicate CSV 6

Replicate Real-time CSV 8

Define Policies in Cisco Policy Builder 10

Policy CDR Management 12

Policy Reports 12

Categories of Policy Reporting Field Types 13
View Policy CDR Fields 15
Accumulate CDR Column Values 15
Configure Maximum Number of Files 18
Configure File Transfer Protocol (FTP) for Policy CDRs 19
Store files in GZip Format 21
Non-blocking CDRs 22
Charging Characteristics AVP in Diameter GY CDR's 24
Add Variables to Policy Reporting Field Types 24
Create Call Data Record (CDR) for a Gy Session 25
Define Conditions for a Gy Session 26
Remove MySQL JDBC Connectors from Standard Load Line-up 27
Configuration File Parameters 27

CHAPTER 3 CDR/EDR Field Descriptions 29
Default Policy Reporting Fields 29
Custom Reference Data 35
Field Descriptions: SPR Common 39
Field Descriptions: Diameter 41
Diameter EDR counter List for Gx 49

Preface

- About This Guide, on page v
- Audience, on page v
- Additional Support, on page vi
- Conventions (all documentation), on page vi
- Communications, Services, and Additional Information, on page vii
- Important Notes, on page viii

About This Guide

This document is a part of the Cisco Policy Suite documentation set.

For information about available documentation, see the *CPS Documentation Map* for this release at Cisco.com.

Note The PATS/ATS, ANDSF, and MOG products have reached end of life and are not supported in this release. Any references to these products (specific or implied), their components or functions in this document are coincidental and are not supported. Full details on the end of life for these products are available at: https://www.cisco.com/c/en/us/products/wireless/policy-suite-mobile/eos-eol-notice-listing.html.

Audience

This guide is best used by these readers:

- Network administrators
- Network engineers
- Network operators
- System administrators

This document assumes a general understanding of network architecture, configuration, and operations.

Additional Support

For further documentation and support:

- Contact your Cisco Systems, Inc. technical representative.
- Call the Cisco Systems, Inc. technical support number.
- Write to Cisco Systems, Inc. at support@cisco.com.
- Refer to support matrix at https://www.cisco.com/c/en/us/support/index.html and to other documents related to Cisco Policy Suite.

Conventions (all documentation)

This document uses the following conventions.

Conventions	Indication
bold font	Commands and keywords and user-entered text appear in **bold** font.
italic font	Document titles, new or emphasized terms, and arguments for which you supply values are in *italic* font.
[ ]	Elements in square brackets are optional.
{x | y | z }	Required alternative keywords are grouped in braces and separated by vertical bars.
[x | y | z]	Optional alternative keywords are grouped in brackets and separated by vertical bars.
string	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.
courier font	Terminal sessions and information the system displays appear in courier font.
< >	Nonprinting characters such as passwords are in angle brackets.
[ ]	Default responses to system prompts are in square brackets.
!, #	An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.

Note Means reader take note. Notes contain helpful suggestions or references to material not covered in the manual.

Caution Means reader be careful. In this situation, you might perform an action that could result in equipment damage or loss of data.

Warning IMPORTANT SAFETY INSTRUCTIONS.

Means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. Use the statement number provided at the end of each warning to locate its translation in the translated safety warnings that accompanied this device.

SAVE THESE INSTRUCTIONS

Note Regulatory: Provided for additional information and to comply with regulatory and customer requirements.

Communications, Services, and Additional Information

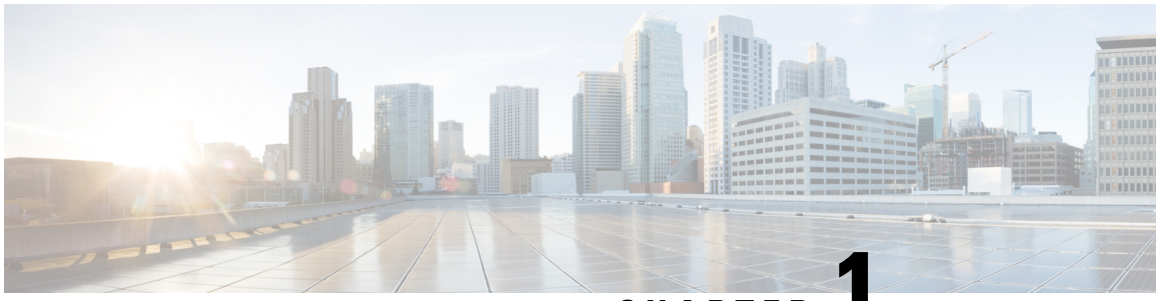
- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.
- To get the business impact you're looking for with the technologies that matter, visit Cisco Services.
- To submit a service request, visit Cisco Support.
- To discover and browse secure, validated enterprise-class apps, products, solutions and services, visit Cisco Marketplace.
- To obtain general networking, training, and certification titles, visit Cisco Press.
- To find warranty information for a specific product or product family, access Cisco Warranty Finder.

Cisco Bug Search Tool

Cisco Bug Search Tool (BST) is a web-based tool that acts as a gateway to the Cisco bug tracking system that maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. BST provides you with detailed defect information about your products and software.

Important Notes

Important Any feature or GUI functionality that is not documented may not be supported in this release or may be customer specific, and must not be used without consulting your Cisco Account representative.



CHAPTER 1

Policy Reporting Overview

- Features, on page 1
- Policy Reporting Interface, on page 1

Features

The Policy Reporting interface is a feature that lets you export subscriber records from the policy engine of Cisco Policy Suite to another system to define file format for further processing.

The Cisco Policy Suite Reporting Interface can export subscriber accounting records in these ways:

- Export to an internal data structure
- Replicate to a MySQL database
- Replicate to a CSV (comma separated value) file

With the Reporting interface installed and configured, you can treat account records in the following ways:

- Define a reporting server that groups similar records for exportation in a similar manner.
- Define a reporting record that contains 1 to n fields, each field of a basic type (String, Long, Decimal, and so on).
- Mark a record as a statistic record. A statistic record indicates to the system that it updates a given set of key fields with statistical data.
- Export records to a CSV file or to a MySQL database.

If preferred, you can enable Redis and disable Mongo for Policy reporting. To do this, you must configure two new parameters in the qns.conf file. See the "Enabling Redis Reporting" section in Configuration File Parameters, on page 27.

Policy Reporting Interface

This section discusses and defines the features used by the Policy Reporting Interface:

- Formats available for replication, JDBC CDR (Call Data Record) Replication, CSV Replication, and Realtime CSV Replication.

- Reporting server indicates to Cisco Policy Suite where the records are physically stored.

For more information on replication parameters, refer to Configuration File Parameters, on page 27.

JDBC CDR (Call Data Record) Replication

Database replication is enabled by adding a JDBC replication object for reporting. All attributes are standard MySQL connections with the exception of the following attributes:

- Run on Instances - The instances where the reporting JDBC replication runs. You can select instances that need to participate in replication of reporting records.
- Replication Period Seconds - How often the temporary JDBC records are updated with data from the work queue.
- Camel Case to DB Name Conversion - Translate names such as "thisIsATest" to the following DB field THIS_IS_A_TEST.

CSV Replication

CSV replication is set up by adding a CSV replication child to the reporting server configuration.

Note Only one CSV configuration should be added under a given server.

- Run on Instances - The instances where the reporting JDBC replication runs. You can select instances that need to participate in replication of reporting records.
- Replication Period Seconds - How often the temporary JDBC records are updated with data from the work queue.

Realtime CSV Replication

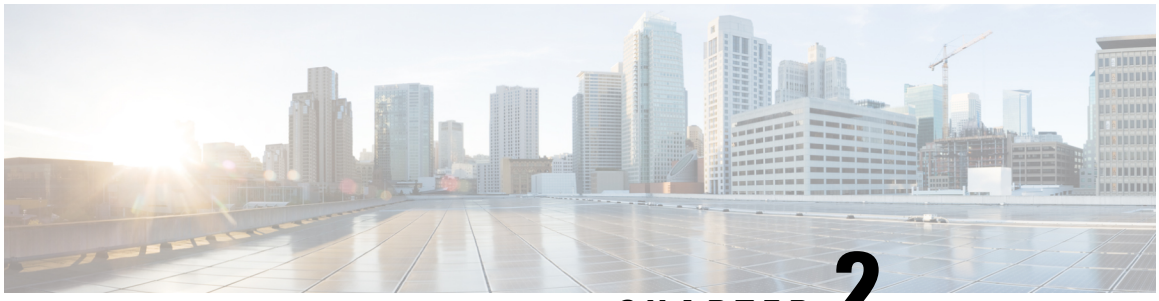
Real time CSV replication is the same as normal CSV except in these ways:

- CSV files are written out even if they are empty.
- The cut over to the next CSV file occurs at the defined time, even if a new file is not needed due to file size.

Reporting Server

A reporting server is a grouping of related reporting records that are exported in the same manner to the same destination. A reporting server is defined in the Reporting Server section of the Reference Data tab.

The purpose of a reporting server is to indicate to Cisco Policy Suite where the records is physically stored.



CHAPTER 2

Reporting Plug-in Configuration

- Install Policy Reporting Plug-in, on page 3
- Configure Policy Reporting Plug-in, on page 4
- Configure a Reporting Server, on page 5
- Define Policies in Cisco Policy Builder, on page 10
- Policy CDR Management, on page 12
- Charging Characteristics AVP in Diameter GY CDR's, on page 24
- Remove MySQL JDBC Connectors from Standard Load Line-up, on page 27
- Configuration File Parameters, on page 27

Install Policy Reporting Plug-in

By default, policy reporting plug-in is not installed in CPS. To install policy reporting plug-in, perform the following steps:

Step 1 Edit the features files on Cluster Manager VM:

a) In the `/etc/broadhop/pb/features` file, add the following line:

```
com.broadhop.client.feature.policyintel
```

b) In the `/etc/broadhop/pcrf/features` file, add the following line:

```
com.broadhop.policyintel.service.feature
```

c) (Optional) In a HA environment, you can enable the service feature for Policy Director (lb) nodes (`/etc/broadhop/iomanangerxx/features`) if you want to enable FTP from those nodes. To enable the service feature, add `com.broadhop.policyintel.service.feature` line in corresponding Policy Director (iomanager).

For example, for iomanager01, user needs to add the following line in `/etc/broadhop/iomananger01/features`:

```
com.broadhop.policyintel.service.feature
```

Step 2 After modifying the feature files, execute the following commands from Cluster Manager:

```
/var/qps/install/current/scripts/build_all.sh
```

If VMs are already deployed, after modifying the feature files, execute the following commands from Cluster Manager:

```
/var/qps/install/current/scripts/build_all.sh

/var/qps/install/current/scripts/upgrade/reinit.sh
```

Configure Policy Reporting Plug-in

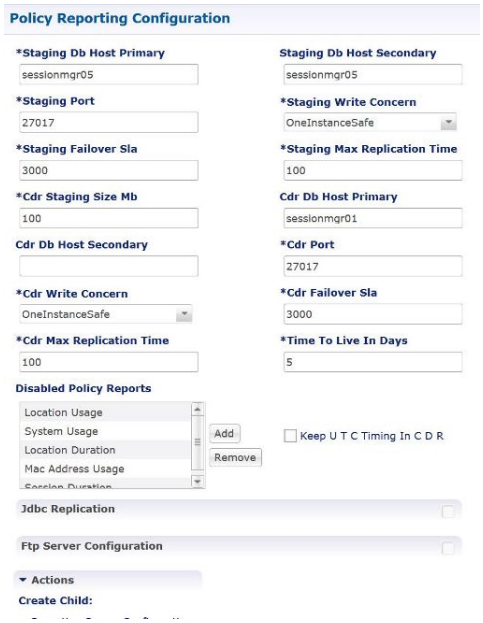
To configure the policy reporting plug-in feature, perform the following steps:

Step 1 Login to the Cisco Policy Builder. The default **Reference Data** tab opens up displaying **Summary** pane on the left side.

Step 2 Expand the **Systems** created. Click **Plugin Configurations** to display **Plugin Configurations Summary** pane on the right side.

Step 3 Click **Policy Reporting Configuration** and the configuration pane is displayed.

Figure 1: Policy Reporting Configuration



The following parameters can be configured under **Policy Reporting Configuration**:

Table 1: Policy Reporting Configuration Parameters

Parameter	Description
Staging Db Host Primary	Enter the name of the primary host database
Staging Db Host Secondary	Enter the name of the secondary host database
Staging Port	Enter the staging port number.
Staging Write Concern	Select staging write concern from the drop-down list.

Parameter	Description
Staging Failover Sla	Enter the staging failover Sla.
Staging Max Replication Time	Enter the staging maximum replication time.
Cdr Staging Size Mb	Enter the CDR staging size in Mb.
Cdr Db Host Primary	Enter the name of the primary CDR host database.
Cdr Db Host Secondary	Enter the name of the secondary CDR host database.
Cdr Port	Enter the CDR port number.
Cdr Write Concern	Select CDR write concern from the drop-down list.
Cdr Failover Sla	Enter the CDR failover Sla.
Cdr Max Replication Time	Enter the maximum CDR replication time.
Time To Live In Days	Enter the time to live in days.
Disabled Policy Reports	Click **Add**, a window appears asking you to select Policy Reporting Field. Select the required policy reporting configuration object and click **OK** to add the selected object in **Disabled Policy Reports** pane.
Keep UTC Timing in CDR	When we enable this check box, the system will keep the timing in UTC when replicating the CDRs to different databases.
Use separate DB per CDR collection	Enabled when there are multiple CDR types.

Configure a Reporting Server

To configure a reporting server, perform the following steps:

Step 1 On the **Policy Reporting Configuration** page, under **Create Child:** click **Reporting Server Configuration**.

Step 2 The **Reporting Server Configuration** page opens up. Click **select** near **Related Cdr** field.

Step 3 Select the required policy CDR object from **Please select a 'PolicyCdr' object...** and click **OK**. The added policy CDR is added in the **Related Cdr** field.

Note Using a Reporting Server, the user can create JDBC CDR replication, CSV replication and Realtime CSV replication. The user can also copy the current reporting server configuration.

Replicate JDBC CDR

Use this procedure if your deployment stores records for offline accounting as JDBC. To enable JDBC CDR database replication, perform the following steps:

The following steps resumes form the Step 3 in Configure a Reporting Server, on page 5.

Step 1 Begin from **Reference Data** > **Systems** > ***name of the system*** > **Plugin Configurations** > **Policy Reporting Configuration** > **Reporting Server Configuration**.

Step 2 Click **Jdbc Cdr Replication** to open JDBC CDR Replication page.

Replicate CSV

Use this procedure if your deployment uses a CSV format to store subscriber records. This screen specifies the location of the subscriber records in the output directory.

Note Only one CSV configuration should be added under a given server. You can also copy the current CSV Replication configuration.

The **File Generation Schedule Location** and **File Naming Rules** related sections under Csv replication are not used for logging based CDR implementation and instead are configured via logback configuration).

To enable CSV Replication, perform the following steps:

The following steps resume from Step 3 in Configure a Reporting Server, on page 5.

Step 1 Begin from **Reference Data** > **Systems** > ***name of your system*** > **Plugin Configuration** > **Policy Reporting Configuration** > **Reporting Server Configuration**.

Step 2 Click **CSV Replication** to open CSV Replication page.

The following parameters can be configured under **Csv Replication**:

Table 2: CSV Replication Parameters

Parameter	Description
Separator (Records)	Enter the separator character to use when writing out fields in a record. The delimiter between fields, for example a comma or semicolon. Default is ,(comma).
Quote	Enter the quote character to use when writing out records. This is an optional field. Not setting a value results in a CSV file free of quotation marks. Set to a specific character, perhaps ’ single quote) or " (double quote) to use those characters in the csv file.
Escape	Enter the escape character to use when writing out records.
Attribute Mask for Date Time	This can be used to specify the date time format used for logging any Date time fields in the report. If not specified the default format **yyyyMMddhhmmss** is used.

Parameter	Description
Date Attributes As Timestamp	When checked, converts date type fields into time stamps (and ignores the **Attribute Mask for Date Time** field) while writing to CDRs (millisec since epoch).
Store In Gzip Format	When checked, the policy reports in the configured directory are stored in the GZip format.
Max Minutes For File	Enter the maximum number of minutes to keep the tmp file open for writing. Using the default of 60 minutes, if CPS starts writing to the file at 1:05 pm, it stops writing to the file at 2:05 pm. Using the default, CPS generates a new file every60 minutes regardless of file size it may attain. Choose either **Max Minutes For File** or **Max File Size Bytes**, not both.
Max File Size Bytes	Enter the maximum file size to write. When the tmp file reaches the size defined here, CPS opens a new file. Choose either **Max File Size Bytes** or **Max Minutes For File**, not both.
Output Directory	Enter the file path where to write out the files.
Max Number Of Files	This field represents the maximum number of files that can exist in the configured output directory. On reaching the limit, addition of files takes place by deleting the oldest file in the configured output directory. Default: 200
Replication Period Seconds	Enter the replication time in seconds. That is, how often to update the temporary CSV file with data from the work queue of CSV records.
Run on Instances	You can limit offline reporting to specific machines. You can select instances that need to participate in replication of reporting records. Click **Add** to display the instances that are defined under cluster in Policy Builder configuration. User needs to make sure that the Policy Reporting plugin is also installed on the specified instances otherwise the instance will not be participating in replication of recording records even if it is specified in the list. If the list is empty then all the instances having Policy Reporting plugin installed may participate in replication of reporting records.
File Part Separator	Enter the separator character to use when writing out file names. The default is a hyphen (-). The file name syntax by default is file part file part *<dbname><separator><collection name><separator><date format mask><.suffix>*.
Date Format Mask	This variable impacts the <date format mask> part of the name. Normally the format is yyyymmddmmss (year month day minutes seconds). However, you can set this variable to the special word "long" to use the Unix timestamp that includes hours and seconds. Example:1310998213 (2011-07-18 14:10:13Z) **Note** If using the special word "long", HH provides 24-hour clock time and hh, lower case letters, provide 12-hour clock time. The file name syntax by default is: *<db name><separator><collection name><separator><date format mask><.suffix>*.

Parameter	Description
Suffix	Enter the decimal point and three-letter suffix you want to append to your filename. This could be .csv, .xls, .txt, and so on. **Note** This field has no default. Be sure to specify it.
File Name includes Db Name check box	Database name is added to csv file name if the checkbox is selected.
File Name includes Collection Name check box	Collection name is added to csv file name if the checkbox is selected.

Replicate Real-time CSV

Use this procedure if your deployment uses a realtime CSV format to store subscriber records. This screen specifies the location of the subscriber records in the output directory.

Note Only one realtime CSV configuration should be added under a given server. The user can also copy the current realtime CSV Replication configuration.

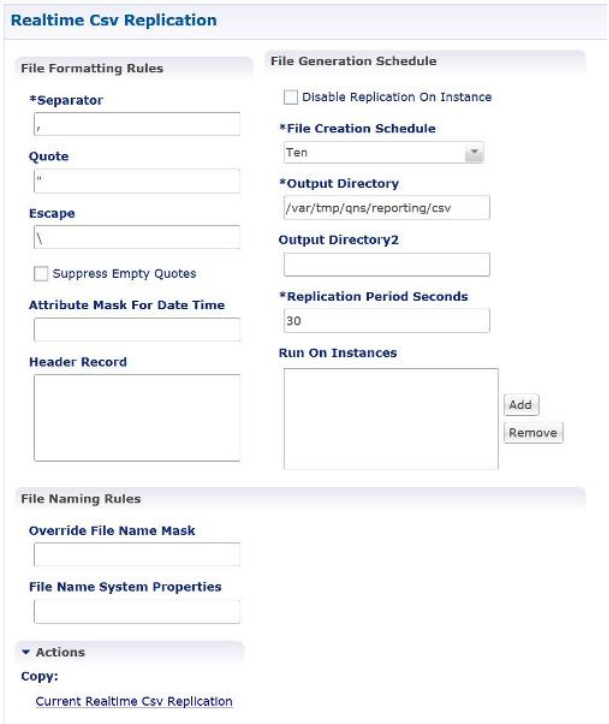
To enable Realtime CSV Replication, perform the following steps:

The following steps resume from Step 3 in Configure a Reporting Server, on page 5.

Step 1 Begin from **Reference Data** > **Systems** > ***name of your system*** > **Plugin Configuration** > **Policy Reporting Configuration** > **Reporting Server Configuration**.

Step 2 Click **Realtime CSV Replication** to open Realtime CSV Replication page.

Figure 2: Realtime CSV Replication



The following parameters can be configured under **Realtime Csv Replication**:

Table 3: Realtime CSV Replication Parameters

Parameter	Description
Separator (Records)	Enter the separator character to use when writing out fields in a record. The delimiter between fields, for example a comma or semicolon. Default is comma (,).
Quote	Enter the quote character to use when writing out records. This is an optional field. Not setting a value results in a CSV file free of quotation marks. Set to a specific character, perhaps ’ single quote) or " double quote to use those characters in the csv file.
Escape	Enter the escape character to use when writing out records.
Attribute Mask For Date Time	This can be used to specify the date time format used for logging any Date time fields in the report. If not specified the default format **yyyyMMddhhmmss** is used.
File Creation Schedule	This field represents the frequency in minutes of the time schedule to write into the csv files for real time replication.
Output Directory	Enter the file path to write the files into
Output Directory2	This is an additional path to store the CSV file. This field is optional

Parameter	Description
Replication Period Seconds	Enter the replication time in seconds. That is, how often to update the temporary realtime CSV file with data from the work queue of CSV records
Run on Instances	You can limit offline reporting to specific machines. You can select instances that need to participate in replication of reporting records. Click **Add** to display the instances that are defined under cluster in Policy Builder configuration. User needs to make sure that the Policy Reporting plugin is also installed on the specified instances otherwise the instance will not be participating in replication of recording records even if it is specified in the list. If the list is empty then all the instances having Policy Reporting plugin installed may participate in replication of reporting records.
Override File Name Mask	This field is used to override the default file name for the generated CSV report. Ifnot specified, a default file name of the format **<PolicyCDRName-TableNameyyyyMMddhhmmss>** is used.
File Name System Properties	This option can be specified to replace any system properties with actual run-time values when Override File Name Mask is selected. A list of system properties separated by commas can be specified. The value in Override File Name Mask is compared against each matching value from this list and replaced with the run time system property. The final replaced value is used for the filename.

Define Policies in Cisco Policy Builder

When configuring extension points under Initial Blueprint for Policy Reporting:

- Send outbound messages records the CDRs before the outbound message is sent by the CPS.
- Post outbound message policies are executed after the outbound message is sent across by the CPS.

Based on the extension point used for configuration, the results may differ.

For example, in cases of session termination, the conditions depending on the presence of a session are not satisfied.

If *A Diameter Gx TGPP Session exists* is configured in the **Conditions** pane under **Send outbound messages**, it captures CDRs for all messages including CCR-T message.

But if *A Diameter Gx TGPP Session exists* is configured for **Post outbound message** policies, it can capture blank CDRs for CCR-T message. This is due to the session being deleted once the CCR-T message is sent.

As mentioned above, since post outbound message policy is executed after the outbound message is sent across by the CPS, the condition *A Diameter Gx TGPP Session exists* does not hold true for CCR-T message, resulting in blank CDRs being captured.

To define a policy in the Policy Builder, add the required fields in the Policy CDR using the data fields available in the Policy Reporting field category.

Note The CDR in the reporting database should be load balanced across the session managers. If high CDR (approx. 8k) is reported on primary reporting replica-set member, there is a chance of getting an issue "`Secondary replica lagging behind the Primary replica`" which leads to the diagnostics output in the hang state. So, the load balancing has to be done as a policy change and can be configured based on the customer environment. For more information, contact your Cisco Account representative.

Step 1 To add a field into a report, use the following steps:

a) Log in to Cisco Policy Builder. Select **Reference Data** tab.

b) Click **Policy Reporting** > **Policy Cdrs**.

c) In the **Actions** tab, click **Policy Cdr** to create a report.

d) In the **Policy Cdr** window, under **Reporting Cdr Columns**, click **Add** to add a new column in the report.

The default *Cdr Field Type* value is set to **Literal**. If the CDR Field Type **Data** is selected, the field name entered should have the same name as that of the data fields in the **Policy Reporting Field Type**.

e) To set a particular CDR field type, click on the default value, a drop-down appears from which you can select the required CDR Field type.

The field added into the report should be mapped with the data fields under the **Policy Reporting Field Type**.

Step 2 To map the fields, use the following steps:

a) Select the field in the **Reporting Cdr Columns** table to be mapped, and click **select** under **Reporting Column Details** > **Data** > **Field**. A window appears asking you to select Policy Reporting Field.

Important **Field** is available only when **Cdr Field Type** is **Data** under **Reporting Cdr Columns** table.

b) Navigate to the data field that matches the field defined in the Reporting CDR column and click **OK**.

Step 3 Once the fields are defined for a report, conditions and policies need to be defined, which are available in the **Policies** tab. To specify a condition, use the following steps:

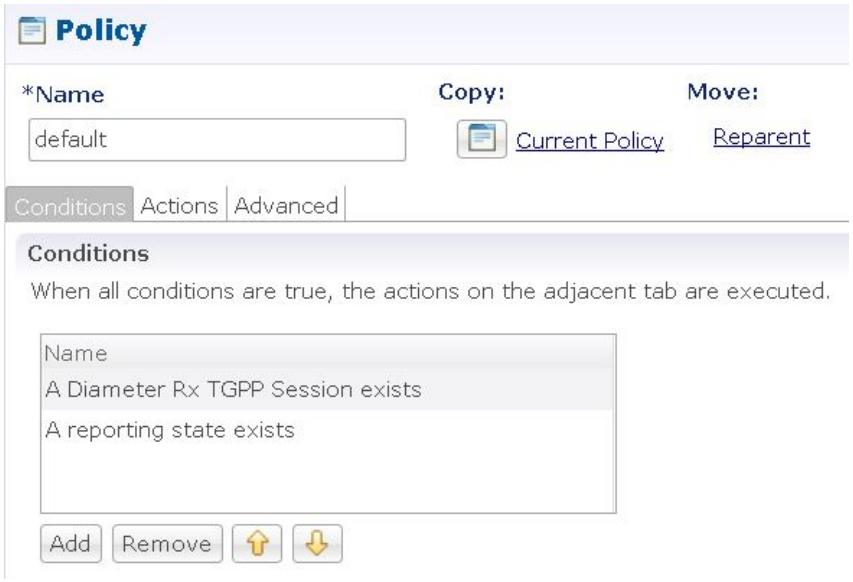
a) In the Policy Builder, select **Policies** tab.

b) Expand **Initial Blueprint** > **Send outbound messages**. A default policy window appears. Enter a policy name of your choice in the **Name** field.

c) Select **Conditions** tab to specify your condition.

d) To add a new condition, click **Add**. A window appears asking you to select a condition phrase. Select the required condition phrase and click **OK**.

Figure 3: Policy



Step 4 The user needs to initialize the Input Variables, Type and Operator Value to establish a connection with the Report. To initialize the values, use the following steps:

a) Select **Actions** tab.
b) Select **Add global reporting data**.
c) Set the **Input Variables** required, the **Type** and **Operator Value**.

Note The Operator Value for the Input Variable Name should be the same as that of the data field defined in the Reporting CDR columns table.

Policy CDR Management

Cisco Policy Suite (CPS) generates Call Data Records (CDR). For improved management, the generated CDRs are moved onto a server, which provides external tools and dashboards for Reporting.

The following topics briefs you on the Policy CDR Management:

- Policy Reports
- Configuring Maximum Number of Files
- Configure File Transfer Protocol (FTP) for Policy CDRs
- Store files in GZip format

Policy Reports

The Policy Reports are designed to provide all its relevant details in a single page.

Viewing of the Policy Reports can be classified in two ways:

- Categorized Policy Reporting Field Types
- View Policy CDR Fields

Categories of Policy Reporting Field Types

Data Fields that are available for the Policy Reporting field Types are categorized into the following:

- NETWORK
- TRAFFIC
- PCRF
- SUBSCRIBER
- BALANCE
- SESSION

The Data Fields for each of the above mentioned Policy Reporting Fields are displayed in columns on the same page.

For example, The Data Fields for NETWORK is displayed in columns on the same page, along with its other relevant details.

View Data Fields of a Category

To view a categorized list of Policy Reporting Fields and it's Data Fields, use the following steps:

Step 1 Log in to Cisco Policy Builder. By default, the screen displays **Reference Data** > **Summary** window.

Step 2 Click **Policy Reporting**.

Step 3 Select **Policy Reporting Field Types**.

Step 4 Select a Policy Reporting Field Type from the categorized list.

For example, click NETWORK to view the list of data fields that belong to NETWORK on the right side.

The data fields related to NETWORK are displayed.

Figure 4: Policy Reporting Field Type - NETWORK

Apart from the fields in the categorized list mentioned, extra fields can be created and configured separately under a new category. These extra fields are called non-default fields.

Create a Non-default Field

To create a non-default field, perform the following steps:

Step 1 Click **Policy Reporting** > **Policy Reporting Field Types**.

Step 2 On the right side, under **Create Child:**, click **Policy Reporting Field Type** to open policy reporting field type page.

Step 3 Provide a name to the category in the **Name** filed. New policy reporting fields can be added to this category.

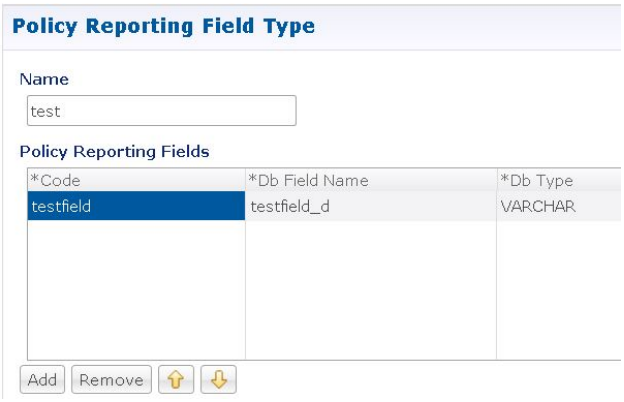
Step 4 Click **Add** to create a field.

a) Provide a name to the field in the **Code** column.

b) Provide a name to the field in the **Db Field Name** column.

c) By default, **Db Type** is set to VARCHAR. To change the database type, click on the default field, a drop-down list appears. Select the **Db Type** required from the drop-down list.

Figure 5: Policy Reporting Field Type - Customized



View Policy CDR Fields

The Policy CDR provides for the configuration of all the Policy Reporting Fields in the same page, avoiding the creation of multiple child pages for each Policy Report.

To view and configure the Policy Reporting Fields, perform the following steps:

Step 1 Log in to Cisco Policy Builder.

Step 2 Click **Policy Reporting** > **Policy Cdrs**.

Step 3 Click **Policy Cdr** under **Create Child:**.

A single report that can be configured along with its relevant details is displayed on the same page.

Accumulate CDR Column Values

You can configure a CDR column to report an accumulated value. For example, as shown in the following figure, if you want to report an accumulated value for balance used, you can set the **Type** for the **balanceUsed** column to **accumulation**, which displays the accumulated balance used reported by each CCR-U during a Gx session.

Step 1 In Policy Builder in the **Reference Data** tab, select **Policy Reporting** > **Policy Cdrs** in the left pane.

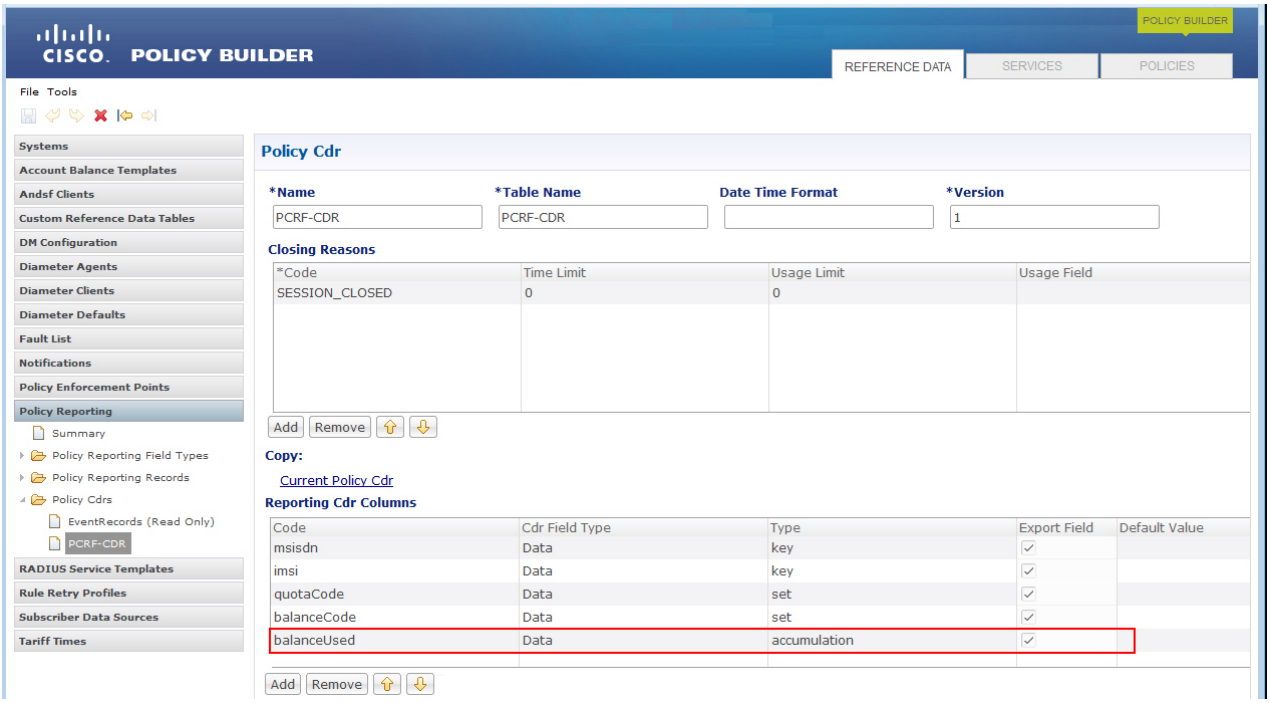
Step 2 Click **Policy Cdrs** under **Create Child**.

Step 3 Configure the relevant details for the report.

Step 4 Under **Reporting Cdr Columns**, select a **Type** of **accumulation** beside the name of the column whose values you want to accumulate.

Notice that, in this example configuration, the **imsi** CRD column is the key column.

Figure 6: Selecting a Type of accumulation for reporting CDR columns



Step 5 Select the Policy Builder **Policies** tab.

Step 6 In the left pane, select **Initial Blueprint** > **Send outbound messages**.

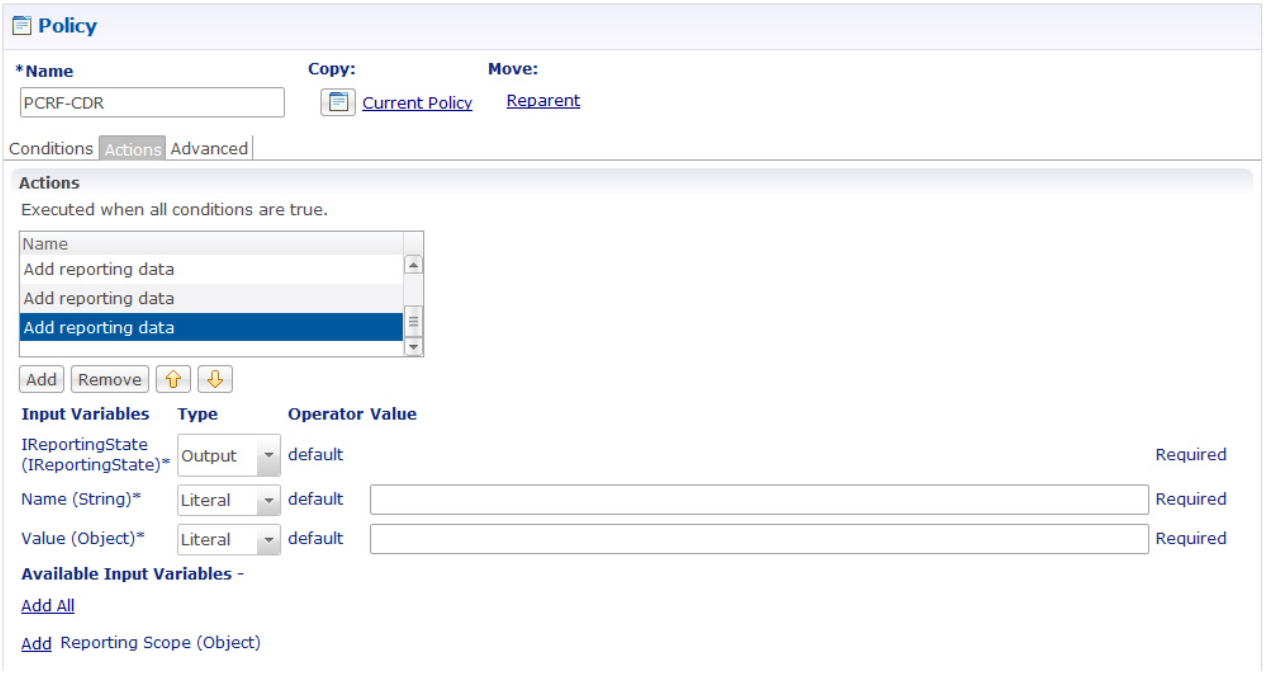
Step 7 Select **PCRF-CDR** (the name of the policy CDR created above), and click the **Actions** tab in the **Policy** pane.

Step 8 Under **Actions**, click **Add**.

Step 9 In the dialog box, search for and select **Add reporting data**, and click **OK**.

Step 10 Select the new **Add reporting data** action in the **Actions** list. The **Policy** pane now looks like the following figure.

Figure 7: Select Add reporting data Action



Step 11 Under **Type**, select **Output** for **IReportingState (IReportingState)**. The **Available Output Variables** dialog box opens.

Step 12 Select **IReportingState** under **A reporting state exists**, and click **OK**.

Step 13 For **Name (String)**, type the name of the CRD column that you configured as an accumulation type (**balanceUsed** in our example).

Step 14 Under **Type**, select **Output** for **Value (Object)**. The **Available Output Variables** dialog box opens.

Step 15 Select the appropriate variable, and click **OK**. In our example, for the **balanceUsed** column, you would select **Amount Charged1** under **An OCSChargeReservationResponse exists**.

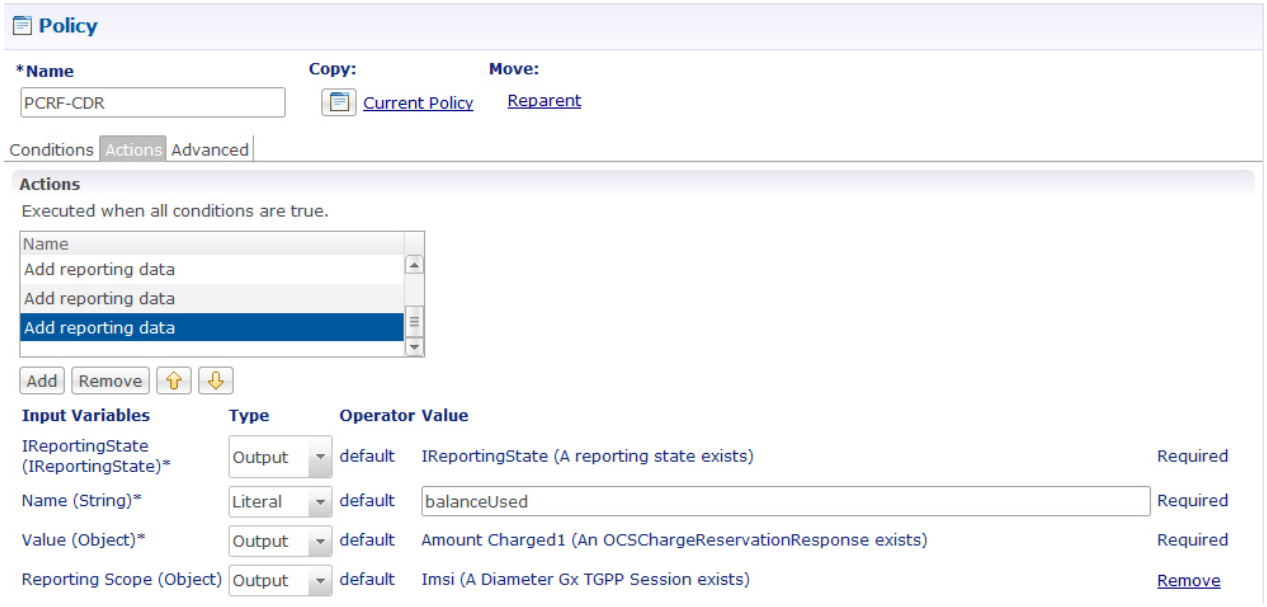
Step 16 Under **Available Input Variables**, click **Add** beside **Reporting Scope (Object)**.

Step 17 Under **Type**, select **Output** for **Reporting Scope (Object)**. The **Available Output Variables** dialog box opens.

Step 18 Select the name of the key CDR column under **A Diameter Gx TGPP Session exists** (**imsi** is the key column in our example) and click **OK**.

The configuration should now look like that shown in the following figure.

Figure 8: Final configuration



Configure Maximum Number of Files

Using maximum number of files field, you can configure the maximum limit of files that can be stored in the configured output directory. On reaching the maximum limit, the oldest report is deleted.

To set the maximum number of files, perform the following steps:

Step 1 Log in to Cisco Policy Builder.

Step 2 Click **Reference Data** > **Systems** > ***select an existing system***.

Step 3 Expand the existing system to navigate to **Plugin Configurations**.

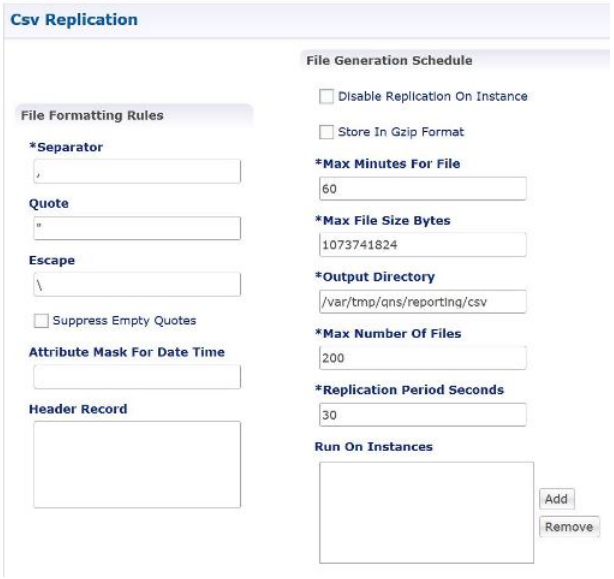
Step 4 Select **Policy Reporting Configuration** under the **Plugin Configuration** summary page. The **Policy Reporting Configuration** page is displayed.

Step 5 Scroll down to locate **Reporting Server Configuration**, under **Actions** and click on the link.

Step 6 From the **Reporting Server Configuration** page, under **Actions** select **Csv Replication**.

Step 7 Under **File Generation Schedule**, in the **Max Number of Files** configure the maximum value in the field provided.

Figure 9: File Generation Schedule



The following parameters can be configured under **File Generation Schedule**:

Table 4: File Generation Schedule Parameters

Parameter	Description
Max Number of Files	This field represents the maximum number of files that can exist in the configured output directory. On reaching the limit, addition of files takes place by deleting the oldest file in the configured output directory.
Allowed value	Integer
Default value	200

Configure File Transfer Protocol (FTP) for Policy CDRs

When the FTP server is configured, the generated Policy CDR reports are copied to the configured destination directory on the primary remote server using File Transfer Protocol. If the primary remote server is not reachable, the Policy CDR reports are copied to the configured destination directory on the secondary remote server.

To configure FTP server, perform the following steps:

Step 1 Log in to Cisco Policy Builder.

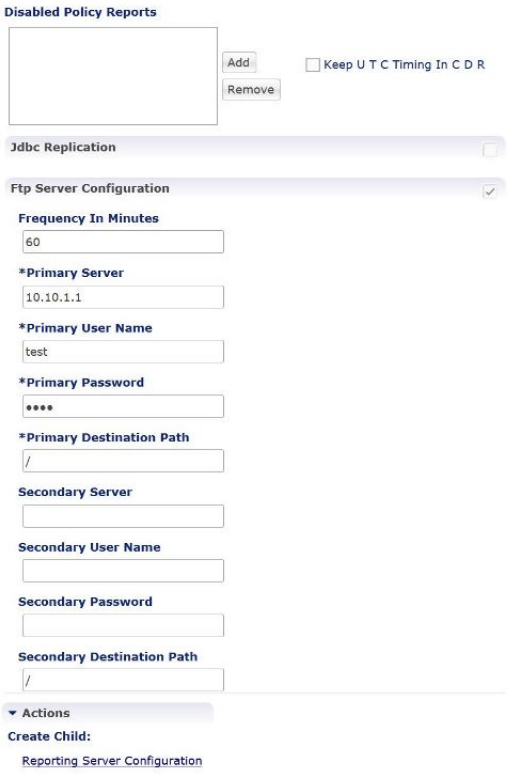
Step 2 Click **Reference Data** > **Systems** > ***select an existing system***.

Step 3 Navigate to **Plugin Configuration**.

Step 4 Select **Policy Reporting Configuration** under the **Plugin Configurations**. The **Policy Reporting Configuration** page appears.

Step 5 Locate **Ftp Server Configuration** check box and select it.

Figure 10: FTP Server Configuration



The following parameters can be configured under **Ftp Server Configuration**:

Table 5: FTP Server Configuration Parameters

Parameter	Description
Frequency In Minutes	This field represents the time interval after which the files are pushed (FTP'ed) to the remote destination. Allowed values = Integer Default = 60
Primary Server	This field represents the host name or IP address of the primary server to which the files are pushed (FTP'ed). Allowed values = String Default = None

Parameter	Description
Primary User Name	This field represents the user name of the FTP account on the primary server. Allowed values = String Default = None
Primary Password	This field represents the password of the FTP account on the primary server. Allowed values = String Default = None
Primary Destination Path	This field represents the destination folder of the FTP account on the primary server. Note that this folder is the path relative to the FTP home folder of the user. Allowed values = String Default = None
Secondary Server	This field represents the host name or IP address of the backup server or secondary server to which the files are pushed (FTP'ed) if the primary host is not reachable. Allowed values = String Default = None
Secondary User Name	This field represents the user name of the FTP account on the secondary server. Allowed values = String Default = None
Secondary Password	This field represents the password of the FTP account on the secondary server. Allowed values = String Default = None
Secondary Destination Path	This field represents the destination folder of the FTP account on the secondary server. Note that this folder is path relative to the FTP home folder of the user. Allowed values = String Default = None

Store files in GZip Format

The policy reports in the configured directory can be stored in the GZip format.

To store the file in the GZip format, perform the following steps:

Step 1 Log in to Cisco Policy Builder.

Step 2 Click **Reference data** > **Systems** > **Summary** > **Plugin Configurations** > **Policy Reporting Configuration**. The Policy Reporting Configuration page appears on the right side.

Step 3 Under **Actions**, click **Reporting Server Configuration** > **Csv Replication**.

Step 4 Under **File Generation Schedule**, select **Store In Gzip Format** check box.

By default this check box is unchecked. If this check box is enabled, the files are stored in GZip format in the configured output directory. Otherwise, files are not zipped.

Non-blocking CDRs

During the time when CDR database is down/slow, CDR attempts be logged in the Policy Server (QNS) logger (to its best but not 100% writes) and not in database, so that live traffic can be served. CDR can be made non-blocking and non-guaranteed (best effort to make it available), so that policy engine performance does not get degraded. CPS does best try to preserve CDR, however there is no guarantee.

Note Cisco recommends disabling blocking CDRs and enable compression.

Step 1 Configure non-blocking CDR: Non-blocking CDR do not block the processing threads when CDR writing takes time. This prevents performance degradation of live traffic.

a) Add the following parameter in `/etc/broadhop/qns.conf` file:

```
-Dcisco.cdr.disableBlocking=true
```

b) In Cluster Manager, execute the following command to synchronize the changes to the VM nodes:

```
copytoall.sh /etc/broadhop/qns.conf /etc/broadhop/qns.conf
```

c) Execute the following commands to publish configuration and restart CPS:

```
/var/qps/bin/control/restartall.sh
```

```
restartall.sh script process will prompt for either Y/N to restart process. Enter Y to restart
the process.
```

Caution Executing `restartall.sh` will cause messages to be dropped.

Step 2 Configure CDR compression: CDR compression is used to compress CDR records and adds padding to improve the write performance. It also helps in preventing database lock (%) to grow over period.

a) Add the following parameter in `/etc/broadhop/qns.conf` file:

```
-Dcisco.cdr.compression=true
```

b) In Cluster Manager, execute the following command to synchronize the changes to the VM nodes:

```
copytoall.sh /etc/broadhop/qns.conf /etc/broadhop/qns.conf
```

c) Execute the following commands to publish configuration and restart CPS:

```
/var/qps/bin/control/restartall.sh
```

```
restartall.sh script process will prompt for either Y/N to restart process. Enter Y to restart
the process.
```

Caution Executing `restartall.sh` will cause messages to be dropped.

Step 3 Configure CDR mongo parameters:

a) Add the following parameters in `/etc/broadhop/qns.conf` file:

```
-Dcisco.cdr.disableBlocking=true
-Dcisco.cdr.compression=true
-Dcisco.cdr.batch=1000
-DdbSocketTimeout.cdrrep=10000
-DdbConnectTimeout.cdrrep=1200
-Dmongo.client.thread.maxWaitTime.cdrrep=1200
-Dmongo.connections.per.host.cdrrep=10
-Dmongo.threads.allowed.to.wait.for.connection.cdrrep=10
-DdbSocketTimeout.cdr=10000
-DdbConnectTimeout.cdr=1200
-Dmongo.client.thread.maxWaitTime.cdr=1200
-Dmongo.connections.per.host.cdr=10
-Dmongo.threads.allowed.to.wait.for.connection.cdr=10
-Dcisco.cdrrep.corePoolSize=5
-Dcisco.cdrrep.maxPoolSize=5
```

Note You must change `-Dcisco.cdr.compression=false` if the CDR size is less than 400 bytes (or less than 10 fields).

b) In Cluster Manager, execute the following command to synchronize the changes to the VM nodes:

```
copytoall.sh /etc/broadhop/qns.conf /etc/broadhop/qns.conf
```

c) Execute the following commands to publish configuration and restart CPS:

```
/var/qps/bin/control/restartall.sh
```

```
restartall.sh script process will prompt for either Y/N to restart process. Enter Y to restart
the process.
```

Caution Executing `restartall.sh` will cause messages to be dropped.

Step 4 Configure logger, to see dropped message. When non-blocking CDR is configured, CDR may dropped.

Note Configuring logger does not make sure that 100% records will be captured in logs. Writing too many logs impacts the performance.

a) Edit the `/etc/broadhop/controlcenter/logback.xml` file and add the following in appender section:

```
<appender name="CONSOLIDATED-REPORTING"
         class="ch.qos.logback.core.rolling.RollingFileAppender">
         <file>${com.broadhop.log.dir:-/var/log/broadhop}/consolidated-reporting.log</file>
         <rollingPolicy
           class="ch.qos.logback.core.rolling.FixedWindowRollingPolicy">
           <fileNamePattern>
             ${com.broadhop.log.dir:-/var/log/broadhop}/consolidated-reporting.%i.log.gz
           </fileNamePattern>
           <minIndex>1</minIndex>
           <maxIndex>5</maxIndex>
         </rollingPolicy>
         <triggeringPolicy
           class="ch.qos.logback.core.rolling.SizeBasedTriggeringPolicy">
           <maxFileSize>100MB</maxFileSize>
         </triggeringPolicy>
         <encoder>
              <pattern>%property{HOSTNAME}  ${DEFAULT_PATTERN}</pattern>
         </encoder>
     </appender>
```

b) Edit the `/etc/broadhop/controlcenter/logback.xml` file and add the following in logger section:

```
<logger name="remote.com.broadhop.reporting.errors" level="info" additivity="false">
         <appender-ref ref="CONSOLIDATED-REPORTING" />
     </logger>
```

c) Edit the `/etc/broadhop/logback.xml` file and add the following in logger section:

```
<logger name="com.broadhop.reporting.errors" level="info" additivity="false">
         <appender-ref ref="SOCKET" />
     </logger>
```

d) Copy logger files to all VMs.

```
copytoall.sh /etc/broadhop/logback.xml /etc/broadhop/logback.xml

copytoall.sh /etc/broadhop/controlcenter/logback.xml /etc/broadhop/controlcenter/logback.xml
```

Step 5 Configure grafana to see the average number of CDR drops and writes.

Jmx counters:

- `cdr.drop`: CDR has dropped.
- `cdr.write`: CDR has written.

Sample grafana query: `groupByNode(cisco.quantum.qps.*qns*.node1.counters.cdr.*, 6, 'sum')`

Charging Characteristics AVP in Diameter GY CDR's

Cisco Policy Suite(CPS) provides the ability to produce reports on Gy Charging Characteristics AVP in Call Data Records (EDR/CDRs).

When a Gy session takes place, PS-Information in the AVPs is processed from the Gy CDR messages and populated in the reporting records. The Policy Builder is configured to populate the CDRs with the required fields, when a Gy Session is initiated.

This section covers the following topics:

- Add Variables to Policy Reporting Field Types
- Create Call Data Record (CDR) for a Gy Session
- Define Conditions for a Gy Session

Add Variables to Policy Reporting Field Types

To add variable to a non-default Policy Reporting Field Type, perform the following steps:

Step 1 Log in to Policy Builder.

Step 2 Click **Reference Data** > **Policy Reporting** > **Policy Reporting Field Types**. A summary window appears on the right side.

Step 3 In the summary window, click **Policy Reporting Field Type** to create a non-default policy reporting field type.

Step 4 Provide a name for the policy reporting field type in the **Name** field.

Step 5 In the **Policy Reporting Fields** table, click **Add** to add a variable.

Step 6 To create the CDR for the Gy Session, the AVP (variables) need to be added.

a) Enter the variable name in the **Code** column.
b) Enter the database field name in the **Db Field Name** column.
c) Select the database type from the **Db Type** drop-down list. By default, the database type is set to *VARCHAR*.
d) Enter the value of precision in the **Precision** column.

Step 7 Click **Add** to add more variables to the Policy Reporting Field Type.

Figure 11: Add Variables to Policy Reporting Field Types

Step 8 Click the **Save** icon to save the new policy reporting field type.

Create Call Data Record (CDR) for a Gy Session

To create a CDR for a Gy session, perform the following steps:

Step 1 Log in to Policy Builder.

Step 2 Click **Reference Data** > **Policy Reporting** > **Policy Cdr**. A summary window appears on the right side.

Step 3 In the summary window, click **Policy Cdr** to create a new report.

Step 4 Provide name and table name to the new report in the **Name** field and the **Table Name** field respectively.

Step 5 Enter a value for the **Version** field.

Step 6 In the **Reporting Cdr Columns** table, add the variables required as defined in the **Policy Reporting Field Types** created for the Gy session. To add required the required variables:

a) Click **Add** to add a new row to the table.
b) Enter the variable name in the **Code** column. The variable being added should be the same as the variable defined in the Policy Reporting Field Type.

c) Set the **Cdr Field Type** value by selecting a type from the drop-down list. By default, the value is *Literal*.
d) Set the **Type** using the values from the drop-down list. By default, the value is *key*.

After the addition of all the required variables in the **Reporting Cdr Columns** table, the variables need to be associated to its field defined in the Policy Reporting Field Type.

Step 7 To associate the variables with the Policy Reporting Field Type:

Repeat the following steps for all the variables defined in **Reporting Cdr Columns** table.

a) Select the variable from the Reporting Cdr Column to be associated.
b) In the **Reporting Column Details** > **Data** > **Field**, click **select**. A window is displayed.
c) Select the field to which the variable needs to be associated with and click **OK**.

Important **Field** is active only for those reporting CDR column entries for which **Cdr Field Type** is *Data*.

Define Conditions for a Gy Session

When a Gy session is initiated the Policy Report defined in the above sections is populated with the Call Data Records (CDR).

In order to populate the policy report when a Gy session is initiated, conditions are needed to be defined. These conditions are defined under the **Policies** tab. When a Gy session is initiated if the conditions is matched, the policy report is populated for the required fields in the CDR.

To define a condition, perform the following steps:

Step 1 Click on the **Policies** Tab, a summary window is displayed.

Step 2 In the left pane, click **Initial Blueprint** > **Post outbound message policies** > **GyCDR** .

Step 3 In the **Policy**page, select **Conditions** tab.

Step 4 Select the required condition from the **Conditions** tab.

A list of available input variables are displayed, which can be assigned to the condition in the **Actions** tab, where all the defined conditions are executed.

Step 5 Select **Actions** tab and click **Add** to add an action. A window is displayed requesting the user to select an **Action Phrase**.

Step 6 Select *Add reporting data* and click **OK**. For the selected action, assign the Input Variables, Type and Operator Value.

Step 7 For the input variable, *IReportingState*, assign the output variable type from the drop-down list. Select *Output*. A window displaying the available output variables is displayed. Select the required output variable and click **OK**.

Step 8 For the input variable, *Value*, assign the output variable type from the drop-down list. Select *Output*. A window displaying the available output variables is displayed. Select the required output variable and click **OK**.

Step 9 For the input variable, *Name*, enter the field name such that the field name is matched with the Gy field name created in Policy Cdr field.

The output field name defined for **Name** should be the same as defined in the Policy Cdr to populate the column in the policy report accordingly.

When a Gy session is initiated, the condition *A Gy V8 session exists* is checked. If the condition is matched, the values that are defined in the **Actions** tab are executed and the fields in the policy report are populated respectively.

Remove MySQL JDBC Connectors from Standard Load Line-up

Step 1 Add the following entry to `qns.conf` file on all the Cisco Policy Suite boxes.

```
-DmysqlDriver=file:///var/broadhop/jdbc/jdbc_5_1_6.jar
```

Step 2 Download MySQL jdbc 5.1.6 binary jar from http://ebr.springsource.com (search for com.springsource.com.mysql.jdbc and download version 5.1.6 from the link).

Step 3 Rename the downloaded jar file to `jdbc_5_1_6.jar` and copy the jar file to `/var/broadhop/jdbc/` directory on all the system boxes.

Step 4 Synchronize all the boxes and then restart the system.

Configuration File Parameters

In addition to the configurations mentioned in the above sections, the following parameters need to be set in qns.conf file.

- Parameter `disableCdrReplication` in `qns.conf` file:

  This flag is used to specify whether the process should participate in doing CDR replication or not.

  - If `disableCdrReplication` is set to true (as `disableCdrReplication=true`) then the processes using corresponding configuration file will not participate in CDR replication.
  - If `disableCdrReplication` is set to false (as `disableCdrReplication=false`) then the processes using corresponding configuration file will participate in CDR replication.
  - If `disableCdrReplication` is not specified then `disableCdrReplication=false` will be used as default and corresponding behavior is applicable.

  By default, this flag is set as false. Configuration is applicable only for processes for which `com.broadhop.policyintel.service.feature` is installed. It does not have any effect on other processes.

  Example:

  - With `disableCdrReplication=true` in `/var/broadhop/qns.conf` file, none of the processes will participate in CDR replication as `/var/broadhop/qns.conf` is used by all processes.
  - With `disableCdrReplication=true` in `/etc/broadhop/pcrf/qns.conf` file, Policy Server (QNS) VMs processes will not participate in CDR replication as `/etc/broadhop/pcrf/qns.conf` is used by process on Policy Server VMs.

For synchronizing configuration files from Cluster Manager to VM, refer to *CPS Installation Guide* for 9.0.0 and prior releases or *CPS Installation Guide for VMware* for 9.1.0 and later releases.

- Parameter oracleDriver in `qns.conf` file.

  This flag is used to specify the oracle driver to be used for replication to database.

  Configuration is applicable only for processes that have `com.broadhop.policyintel.service.feature` installed and are participating in database replication. It does not have any effect for other processes.

  Example:

  ```
  -DoracleDriver=file:///var/broadhop/odbc7.jar
  ```

  Oracle ODBC jar can be downloaded from http://www.oracle.com/technetwork/database/features/jdbc/.

  Downloaded jar may need to be renamed to the name specified in configuration and needs to be copied to all required VMs at the same path that is specified in above configuration.

Enabling Redis Reporting

You can add the following parameters in the qns.conf file to enable Redis for reporting purposes. When you enable these parameters, the current Mongo storage is bypassed, and each Policy Server node writes the CDRs to a Redis queue.

- The `enableRedisReporting` parameter enables Redis reporting and bypasses Mongo when set to true. This parameter should be configured on each Policy Server and Policy Director. Possible values are true and false. If this parameter is not present in the qns.conf file, the default value is false.

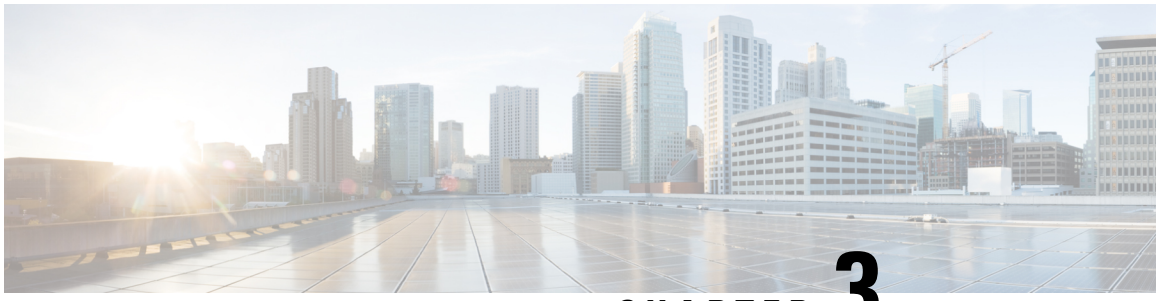
  Example:

  ```
  -DenableRedisReporting=true
  ```

- The `reporting.redisSLA` parameter sets the time an incoming message from the Redis server remains in the reporting queue before being dropped. This parameter should be configured on all Policy Director nodes, or on any node that is performing replication. The value is in milliseconds, and the default value is 500. You may want to increase this value based on your requirements.

  Example:

  ```
  -Dreporting.redisSLA=1000
  ```



CHAPTER 3

CDR/EDR Field Descriptions

- Default Policy Reporting Fields, on page 29
- Diameter EDR counter List for Gx, on page 49

Default Policy Reporting Fields

Note RADIUS-based policy control is no longer supported in CPS 14.0.0 and later releases as 3GPP Gx Diameter interface has become the industry-standard policy control interface.

Table 6: Default Policy Reporting Fields

Group	Type	Field Name	Field Data Type	Descriptions
Default Policy Reporting Fields				
	ANDSF			
		PolicyType	VARCHAR	Indicates type of policy. For example, ISMP or ISRP.
		devId	VARCHAR	Indicates Id of the device from where the request is received.
		LocationType	VARCHAR	Indicates type of location such as. • wlan • 3GPP • 3GPP2 • WiMAX • Geo

Group	Type	Field Name	Field Data Type	Descriptions
		Location	VARCHAR	Name of the location.
		PolicyName	VARCHAR	Name of the policy or MO Tree name provided to subscriber / UE.
		PolicyUpdateCount	INT	Indicates the number of times policy is updated in the UE.
		authUserName	VARCHAR	Authentication user name provided by the UE.
		devType	VARCHAR	Indicates the type of device. For example, IPhone or Android.
		clientName	VARCHAR	Name of the ANDSF client in UE.
		uuid	VARCHAR	IPhone UE uuid.
	NETWORK			
		Access Type	VARCHAR	IPCAN types such as: • 3GPP • GPS • EPS
		Cell Site Id	VARCHAR	Unique identifier for Cell site.
		chargingId	VARCHAR	A subscriber might have a unique charging ID. Using this, usage by members of a sub account, or ‘children’ of the subscriber can be billed to their ‘parent’.
		Circuit Id	VARCHAR	Information specific to which circuit the request came in on.

Group	Type	Field Name	Field Data Type	Descriptions
		Device Rating Group	VARCHAR	The Rating-Group AVP is of type Unsigned32 (AVP Code 432) and contains the identifier of a rating group. All the services subject to the same rating type are part of the same rating group. The specific rating group the request relates to is uniquely identified by the combination of Service-Context-Id and Rating-Group AVPs.
		Framed IP	VARCHAR	This Attribute indicates the address to be configured for the user. It MAY be used in Access-Accept packets. It MAY be used in an Access-Request packet as a hint by the NAS to the server that it would prefer that address, but the server is not required to honor the hint.
		Imei Sv	VARCHAR	IMEISV (16 digits) includes information on the origin, model, and serial number of the device.
		IMSI	VARCHAR	International mobile Subscriber Identity is a unique identification associated with all cellular networks. It is stored as a 64 bit field and is sent by the phone to the network.
		MAC Address	VARCHAR	A unique identifier assigned to network interfaces for communications on the physical network segment.
		MSISDN	VARCHAR	A number uniquely identifying a subscription in a GSM or a UMTS mobile network.
		NAS IP	VARCHAR	IP address for the Network Access Server
		RAT Type	VARCHAR	Unique identifier for Radio Access Type.

Group	Type	Field Name	Field Data Type	Descriptions
		SGSN Address	VARCHAR	Diameter based network node - can be used for location reporting
	TRAFFIC			
		In Bytes	BIGINT	In Bytes per Accounting Record
		Out Bytes	BIGINT	The number of output bytes.
		Total Bytes	BIGINT	The number of Total bytes.
		Traffic Type	VARCHAR	Streaming, Gaming - This is Diameter Dependent.
	PCRF			
		Device Service	VARCHAR	The current Active Device Service.
		Device Session Id	VARCHAR	Unique identifier for a single session on a single device.
		NAS ID	VARCHAR	Unique identifier for the Network Access Server.
		Service	VARCHAR	The current Active Service Code.
		Service Code	VARCHAR	The current Active Service Code
		User Domain Info	VARCHAR	The domain associated to the subscriber.
		User Name	VARCHAR	User name
	SUBSCRIBER			
		SubscriberExternalId	VARCHAR	Occasionally, a subscriber may need to connect with or relate to an external third-party system. This field identifies the subscriber to that external service.
		Subscriber Realm	VARCHAR	Default Login Realm, Ex. USuM Auth, AAA Proxy
		Subscriber Status	VARCHAR	Active, Expired

Group	Type	Field Name	Field Data Type	Descriptions
		Sub User Name	VARCHAR	The networkId is a unique string value that identifies the subscriber. This can be any value such as MSISDN, MAC Address, IP Address, IMPI, Email Address, Telephone number, etc.
		User Location Info	VARCHAR	Location code corresponding to one of several possible location identifiers (MAC, SSID, IP subnet).
	BALANCE			
		Balance Code	VARCHAR	Account Balance Code is the code of the balance template defined in the Policy Server (QNS) reference data that corresponds to the balance (group of quotas) to be credited, debited, provisioned, etc.
		Balance Remaining	BIGINT	The exact balance remaining. The balanceRemaining (Long) field is rounded to a whole number.
		Balance Used	BIGINT	Amount of balance used currently by subscriber.
		Credit End Date	DATETIME (E MMM dd HH:mm:ss time zone)	Date credit expires.
		Credit Start Date	DATETIME (E MMM dd HH:mm:ss time zone)	Start and End date are when you want the credit to become valid and when you want it to expire. If not specified, the start date defaults to now.
		Original Amount	BIGINT	Original amount of subscriber balance before any debits applied.

Group	Type	Field Name	Field Data Type	Descriptions
		Quota Code	VARCHAR	Quota Code is the code of the quota template defined in the Policy Server (QNS) reference data that corresponds to the quota (actual bucket) to be credited.
		Rate	VARCHAR	Rate at which balance is charged. 1x, 3x.
		Rated Total Amount	VARCHAR	Total amount with the rate applied.
		Rate Plan Code	VARCHAR	Optional Rate Plan Code.
		Refresh Date of Credit	DATETIME (E MMM dd HH:mm:ss time zone)	Date credit is refreshed to pre-configured amount.
		Refresh Day of Month Of Credit	DATETIME (E MMM dd HH:mm:ss time zone)	Date when Balance/Quota refreshes to original amount.
		Reservation_Amount	BIGINT	Quota reservation amount.
		Tariff Code	VARCHAR	Code linked to subscriber service. Different service options can be applied to services at specified time ex. Holidays.
		Tariff Time Id	VARCHAR	Time of day boundary.
		Unrated Total Amount	VARCHAR	Total amount with no rate applied.
	SESSION			
		Rejected Start	BIGINT	If any value of the received Attributes is not acceptable, then the RADIUS server MUST transmit a packet with the Code field set to 3 (Access-Reject). It MAY include one or more Reply-Message Attributes with a text message which the NAS MAY display to the user.
		Session Duration	BIGINT	The amount of time the session has been up, in clock time

Group	Type	Field Name	Field Data Type	Descriptions
		Start Session	BIGINT	Number of Start Sessions.
		Stop Session	BIGINT	This number increments when a session stops for reporting purposes.

Custom Reference Data

Note RADIUS-based policy control is no longer supported in CPS 14.0.0 and later releases as 3GPP Gx Diameter interface has become the industry-standard policy control interface.

Table 7: Custom Reference Data

Group	Type	Field Name	Field Data Type	Descriptions
Custom Reference Data				
	User	Name		This Attribute indicates the name of the user to be authenticated. It MUST be sent in Access-Request packets if available. It MAY be sent in an Access-Accept packet, in which case the client SHOULD use the name returned in the Access-Accept packet in all Accounting-Request packets for this session. If the Access- Accept includes Service-Type = Rlogin and the User-Name attribute, a NAS MAY use the returned User-Name when performing the Rlogin function.
	Any registered AVP of RADIUS or Diameter	Value		Type and description applies based on AVP chosen, which cannot be specified explicitly.
Policy Report Fields				
	Reference Data Field			
		Device Service	VARCHAR	

Group	Type	Field Name	Field Data Type	Descriptions
		Session Duration	BIGINT	The amount of time the session has been up, in clock time.
		NAS ID	VARCHAR	Unique identifier for the Network Access Server.
		Access Type	VARCHAR	IPCAN types, 3GPP, GPS, EPS
		MAC Address	VARCHAR	A unique identifier assigned to network interfaces for communications on the physical network segment.
		Device Rating Group	VARCHAR	The Rating-Group AVP is of type Unsigned32 (AVP Code 432) and contains the identifier of a rating group. All the services subject to the same rating type are part of the same rating group. The specific rating group the request relates to is uniquely identified by the combination of Service-Context-Id and Rating-Group AVPs.
		MSISDN	VARCHAR	A number uniquely identifying a subscription in a GSM or a UMTS mobile network.
		Rejected Start	BIGINT	If any value of the received attributes is not acceptable, then the RADIUS server transmits a packet with the Code field set to 3 (Access-Reject). The packet might include one or more Reply-Message Attributes with a text message, which the NAS displays to the user.
		Balance Remaining	BIGINT	The exact balance remaining. The balanceRemaining (Long) field is rounded to a whole number.
		Out Bytes	BIGINT	The number of output bytes as reported by the SCE.
		Tariff Code	VARCHAR	Code linked to subscriber service. Different service options can be applied to services at specified time.
		Balance Used	BIGINT	Amount of balance used currently by subscriber.

Group	Type	Field Name	Field Data Type	Descriptions
		Original Amount	BIGINT	Original amount of subscriber balance before any debits applied.
		Balance Code	VARCHAR	Account Balance Code is the code of the balance template defined in the Policy Server (QNS) reference data that corresponds to the balance (group of quotas) to be credited, debited, provisioned, etc.
		Cell Site Id	VARCHAR	Unique identifier for Cell site.
		RAT Type	VARCHAR	Unique identifier for Radio Access Type.
		Tariff Time Id	VARCHAR	Time of day boundary.
		Reservation_ Amount	BIGINT	Quota reservation amount.
		Refresh Date of Credit	DATETIME (E MMM dd HH:mm:ss time zone)	Date credit is refreshed to pre-configured amount.
		User Domain Info	VARCHAR	This drop-down list lets you assign the subscriber a domain. Domains themselves are created in the Cisco Policy Builder interface.
		Circuit Id	VARCHAR	Information specific to which circuit the request came in on.
		Quota Code	VARCHAR	Quota Code is the code of the quota template defined in the Policy Server (QNS) reference data that corresponds to the quota (actual bucket) to be credited.
		Start Session		Number of Start Sessions.
		Rate	VARCHAR	Rate at which balance is charged. 1x, 3x
		Refresh Day of Month Of Credit	DATETIME (E MMM dd HH:mm:ss time zone)	Date when Balance/Quota refreshes to original amount.
		Total Bytes	BIGINT	Total Bytes based of Radius Accounting packet.

Group	Type	Field Name	Field Data Type	Descriptions
		Device Session Id	VARCHAR	Unique identifier for a single session on a single device.
		Stop Session	BIGINT	This number increments when a session stops for reporting purposes.
		Rated Total Amount	VARCHAR	Total amount with the rate applied.
		Credit Start Date	DATETIME (E MMM dd HH:mm:ss time zone)	Start and End date are when you want the credit to become valid and when you want it to expire. If not specified, the start date defaults to now.
		Framed IP	VARCHAR	This Attribute indicates the address to be configured for the user. It is used in Access-Accept packets or used in an Access-Request packet as a hint by the NAS to the server for the required address.
		Imei Sv	VARCHAR	IMEISV (16 digits) includes information on the origin, model, and serial number of the device.
		IMSI	VARCHAR	International mobile Subscriber Identity is a unique identification associated with all cellular networks. It is stored as a 64 bit field and is sent by the phone to the network.
		Unrated Total Amount	VARCHAR	Total amount with no rate applied.
		User Name	VARCHAR	User name.
		Device Service	VARCHAR	ISG, WLC, CAR
		In Bytes	BIGINT	In Bytes per Accounting Record.
		SGSN Address	VARCHAR	Diameter based network node - can be used for location reporting.
		Traffic Type	VARCHAR	Streaming, Gaming - This is Diameter Dependent
		Policy Server (QNS) Service	VARCHAR	Unique identifier for the Policy Server (QNS) service type.

Group	Type	Field Name	Field Data Type	Descriptions
		User Location Info	VARCHAR	Location code corresponding to one of several possible location identifiers (MAC, SSID, IP subnet).
		Credit End Date	DATETIME (E MMM dd HH:mm:ss time zone)	Date credit expires.
		NAS IP	VARCHAR	IP address for the Network Access Server.
		Sub User Name	VARCHAR	The networkId is a unique string value that identifies the subscriber. This can be any value such as MSISDN, MAC Address, IP Address, IMPI, Email Address, Telephone number, etc.
		Subscriber Realm	VARCHAR	Default Login Realm, Ex. USuM Auth, AAA Proxy.
		Subscriber Status	VARCHAR	Active, Expired
		Service Code	VARCHAR	Their Active Service.
		Rate Plan Code	VARCHAR	Optional Rate Plan Code
Common				
	Session			
		next Evaluation Date	Date (YYYY-MM-DD)	Checks for change of service
		expiration Date	Date (YYYY-MM-DD)	Session expiration

Field Descriptions: SPR Common

Note RADIUS-based policy control is no longer supported in CPS 14.0.0 and later releases as 3GPP Gx Diameter interface has become the industry-standard policy control interface.

Table 8: Field Descriptions: SPR Common

Group	Type	Field Name	Field Data Type	Description
SPR Common				
	Credential	type	String	Credential type specifies the type of unique identifier (username/Password, Network ID).
	Credential	description	String	Description of the unique identifier.
	Credential	networkID	String	The networkId is a unique string value that identifies the subscriber. This can be any value such as MSISDN, MAC Address, IP Address, IMPI, Email Address, Telephone number, etc.
	Credential	expiration Time Remaining	Integer	Defines the time remaining.
	Schedule	State	String	Indicates whether the time/date and cron values evaluate from a positive or negative perspective.
	Schedule	Enabled	Boolean	This code specifies whether or not a service schedule is enabled or disabled.
	Schedule	End time	String	The service's end time.
	Schedule	Start time	String	The service's starttime.
	Schedule	Repeat	Repeat	Handles how the schedule repeats within that timeframe.
	Schedule	End date	Date (YYYY-MM-DD)	The service’s end date.
	Schedule	Start date	Date (YYYY-MM-DD)	The service's end date.
	Service	Enabled	Boolean	This code specifies whether or not a service is enabled or disabled.
	Service	Code	String	Service code.

Group	Type	Field Name	Field Data Type	Description
	User	Name	Name	The name of the user the accounting record is being logged for.
	User	Status	String	Represents the type of accounting record and maps to the RADIUS acct-status-type attribute. A value of 1=start, 2=stop, and 3=update.
	User	End date	Date (YYYY-MM-DD)	Use the calendar to specify the start and stop date and time of service to the subscriber.
	User	Role	String	When the subscriber logs in to your subscriber portal, this field determines how much read-write privilege is granted to them.
	User	External ID	String	Occasionally, a subscriber may need to connect with or relate to an external third-party system. This field identifies the subscriber to that external service.
	User	Charging ID	String	A subscriber might have a unique charging ID. Using this, usage by members of a sub-account, or 'children' of the subscriber can be billed to their 'parent'.
	User	startDate	Date (YYYY-MM-DD)	Use the calendar to specify the start and stop date and time of service to the subscriber.

Field Descriptions: Diameter

Table 9: Field Descriptions: Diameter

Group	Type	Field Name	Field Data Type	Description
Diameter: GxSce				
		destHost	String	This contains the host the message must be routed to.
		destRealm	String	This contains the realm the message must be routed to.

Group	Type	Field Name	Field Data Type	Description
		appId	Long	All Diameter messages contain an Application Identifier, which is used in the message forwarding process.
		userName	String	The User-Name AVP which contains the User-Name, in a format consistent with the NAI specification.
		appName	String	String representing the application name for the appId.
		imsi	String	International mobile Subscriber Identity is a unique identification associated with all cellular networks. It is stored as a 64 bit field and is sent by the phone to the network.
		msisdn	String	A number uniquely identifying a subscription in a GSM or a UMTS mobile network.
Diameter: GxV9				
		mnc	String	Portion of IMSI containing the Mobile Network Code.
		mcc	String	Portion of IMSI containing the Mobile Country Code.
		rai	String	Routing Area Identity. A routing area is normally a subdivision of a location area.
		ipcanType	Integer	It indicates the type of Connectivity Access Network in which the user is connected.
		ratType	Integer	This is used to identify the radio access technology that is serving the UE.
		destHost	String	This contains the host the message must be routed to.
		destRealm	String	This contains the realm the message must be routed to.
		appId	Long	All Diameter messages contain an Application Identifier, which is used in the message forwarding process.
		mccmnc	String	Combination of MCC and MNC.

Group	Type	Field Name	Field Data Type	Description
		appName	String	String representing the application name for the appId.
		imsi	String	International mobile Subscriber Identity is a unique identification associated with all cellular networks. It is stored as a 64 bit field and is sent by the phone to the network.
		msisdn	String	A number uniquely identifying a subscription in a GSM or a UMTS mobile network.
		framedIp	String	This Attribute indicates the address to be configured for the user. It MAY be used in Access-Accept packets. It MAY be used in an Access-Request packet as a hint by the NAS to the server that it would prefer that address, but the server is not required to honor the hint.
		lac	Integer	To each location area, a unique number called a location area code is assigned.
		userLocationInfo	String	Location code corresponding to one of several possible location identifiers (MAC, SSID, IP subnet).
		sgsnIpAddress	String	IP Address of Diameter based network node - can be used for location reporting
		tgppRatType	Integer	This is used to identify the radio access technology that is serving the UE.
		eventTriggers	Integer	When sent from PCRF to PCEF, this AVP indicates that an event shall cause a re-request of PCC rules. When sent from the PCEF to the PCRF this AVP indicates that the corresponding event has occurred at the gateway.
		outOfCredit	Boolean	True or false option indicating if the subscriber is out of credit.
		qosUpgradeSupported	Boolean	True or false option indicating if Quality of Service upgrade is supported for the subscriber.

Group	Type	Field Name	Field Data Type	Description
		rac	Integer	Routing Area Code is a fixed length code of 1 octet identifying a routing area within a location area.
		sac	Integer	Service Area Code has a length of two octets and is unique within the location Area.
		ci	Integer	Cell identity for GSM or Service Area Code (SAC) at the time of Record Opening Time.
		cgi	String	Cell Global Identity is a standard identifier for mobile phones cells, providing means to geographically locate connected mobile phones.
		ecgi	String	E-UTRAN Cell Global Identifier.
		tai	String	Tracking Area Identifier
		sai	String	Service Area Identifier
		tac	Integer	Type Allocation Code (TAC) is the initial eight-digit portion of the 15-digit IMEI code.
		ect	Integer	Explicit Communication Transfer
		imeisv	String	IMEISV (16 digits) includes information on the origin, model, and serial number of the device.
		bcm	Integer	Bearer control mode applied to the IP-CAN session.
		framedIpv6Prefix	String	The IPv6 prefix allocated for the user.
Diameter: GxTGPP				
		mnc	String	Portion of IMSI containing the Mobile Network Code.
		mcc	String	Portion of IMSI containing the Mobile Country Code.
		rai	String	Routing Area Identity. A routing area is normally a subdivision of a location area.
		ipcanType	Integer	It indicates the type of Connectivity Access Network in which the user is connected.

Group	Type	Field Name	Field Data Type	Description
		ratType	Integer	This is used to identify the radio access technology that is serving the UE.
		destHost	String	This contains the host the message must be routed to.
		destRealm	String	This contains the realm the message must be routed to.
		appId	Long	All Diameter messages contain an Application Identifier, which is used in the message forwarding process.
		mccmnc	String	Combination of MCC and MNC
		appName	String	String representing the application name for the appId.
		imsi	String	International mobile Subscriber Identity is a unique identification associated with all cellular networks. It is stored as a 64 bit field and is sent by the phone to the network.
		msisdn	String	A number uniquely identifying a subscription in a GSM or a UMTS mobile network.
		framedIp	String	This Attribute indicates the address to be configured for the user. It MAY be used in Access-Accept packets. It MAY be used in an Access-Request packet as a hint by the NAS to the server that it would prefer that address, but the server is not required to honor the hint.
		lac	Integer	To each location area, a unique number called a location area code is assigned.
		userLocationInfo	String	Location code corresponding to one of several possible location identifiers (MAC, SSID, IP subnet).
		sgsnIpAddress	String	IP Address of Diameter based network node - can be used for location reporting.
		tgppRatType	Integer	This is used to identify the radio access technology that is serving the UE.

Group	Type	Field Name	Field Data Type	Description
		eventTriggers	Integer	When sent from PCRF to PCEF, this AVP indicates that an event shall cause a re-request of PCC rules. When sent from the PCEF to the PCRF this AVP indicates that the corresponding event has occurred at the gateway.
		outOfCredit	Boolean	True or false option indicating if the subscriber is out of credit.
		qosUpgradeSupported	Boolean	True or false option indicating if Quality of Service upgrade is supported for the subscriber.
		rac	Integer	Routing Area Code is a fixed length code of 1 octet identifying a routing area within a location area.
		sac	Integer	Service Area Code has a length of two octets and is unique within the location Area.
		ci	Integer	Cell identity for GSM or Service Area Code (SAC) at the time of Record Opening Time.
		cgi	String	Cell Global Identity is a standard identifier for mobile phones cells, providing means to geographically locate connected mobile phones.
		ecgi	String	E-UTRAN Cell Global Identifier
		tai	String	Tracking Area Identifier
		sai	String	Service Area Identifier
		tac	Integer	Type Allocation Code (TAC) is the initial eight-digit portion of the 15-digit IMEI code.
		ect	Integer	Explicit Communication Transfer
		imeisv	String	IMEISV (16 digits) includes information on the origin, model, and serial number of the device.
		bcm	Integer	Bearer control mode applied to the IP-CAN session.
		framedIpv6Prefix	String	The IPv6 prefix allocated for the user.

Group	Type	Field Name	Field Data Type	Description
Diameter: RxTGPP				
		appId	Long	All Diameter messages contain an Application Identifier, which is used in the message forwarding process.
		appName	String	String representing the application name for the appId.
		serviceInfoStatus	Integer	Status of the service being executed.
		specificAction	Integer	Within an initial AA request the AF may use the Specific-Action AVP to request specific actions from the server at the bearer events and to limit the contact to such bearer events where specific action is required.
		serviceURN	String	It indicates whether an AF session is used for emergency traffic.
		isEmergency	Boolean	Indication of Emergency Session
Diameter: GyV8				
		shared Bucket Reservation	String	Reservation amount for quota when more than one subscriber shares the quota.
		destHost	String	This contains the host the message must be routed to.
		destRealm	Long	This contains the realm the message must be routed to.
		appId	String	All Diameter messages contain an Application Identifier, which is used in the message forwarding process.
		userName	String	The User-Name AVP which contains the User-Name, in a format consistent with the NAI specification
		appName	String	String representing the application name for the appId.
		msisdn	String	A number uniquely identifying a subscription in a GSM or a UMTS mobile network.

Group	Type	Field Name	Field Data Type	Description
		userLocationInfo	String	Location code corresponding to one of several possible location identifiers (MAC, SSID, IP subnet).
		sgsnIpAddress	String	IP Address of SGSN, a Diameter based network node - can be used for location reporting.
		ggsnIpAddress	String	IP Address of GGSN, a Diameter based network node.
		apn	String	Access point name is the name of the gateway between the mobile network and another network.
		sessionId	String	Unique identifier of a session.
Diameter: Gy/Ro				
		inOctets	Long	It contains the number of requested, granted, or used octets that can be/have been received from the end user.
		outOctets	Long	It contains the number of requested, granted, or used octets that can be/have been sent to the end user.
		totalTime	Long	This indicates the length of the requested, granted, or used time in seconds.
		cmdCode	Long	The possible values for command-code are credit-control-request and credit-control-answer.
		serviceCode	String	The current active service.
		terminationCause	Integer	The Termination-Cause AVP contains information about the termination reason.
		totalOctets	Long	It contains the total number of requested, granted, or used octets.
		resultCode	Integer	This indicates any error present in the Credit-Control-Request message.
		requestType	integer	This contains the reason for sending the credit-control request message. It MUST be present in all Credit-Control-Request messages.

Group	Type	Field Name	Field Data Type	Description
		requestNumber	Long	Uniquely identifies the request within a session.
		redirectURL	String	The URL to which session is redirected to.
		ratingGroup	String	It contains the charging key. Each quota allocated to a Diameter CC session has a unique Rating Group value.
		sessionId	String	Unique identifier of a session.

Diameter EDR counter List for Gx

- To enable EDR to be written by CPS internally, EDR_ENABLE flag needs to be set as true in `qns.conf` file.
- Required counter that the customer wants in EDR must be configured in policy reporting configuration. The names of different EDR counters are mentioned in the following table:

Table 10: Diameter EDR counter List for Gx

Counter Name	Description
session_id	Session ID of Gx session
command_code	Command code of Message
request_type	Request type of CCR message
apn_original	Called station ID
apn_modified	Called station ID for CPS overrides
framed_ip	Framed IP
Ci	Parsed from user location
Lac	Parsed from user location
rat_type	Radio Access Type
Timezone	Timezone comes in Diameter AVP
eventTrigger	Event trigger value
chargingRuleRemove	Rule which is removed over Gx
chargingRuleAdd	Rule which is installed over Gx
timestamp2	Time of Message in or out from CPS