



Reporting Plug-in Configuration

- [Install Policy Reporting Plug-in, on page 1](#)
- [Configure Policy Reporting Plug-in, on page 2](#)
- [Configure a Reporting Server, on page 3](#)
- [Define Policies in Cisco Policy Builder, on page 8](#)
- [Policy CDR Management, on page 10](#)
- [Charging Characteristics AVP in Diameter GY CDR's, on page 22](#)
- [Remove MySQL JDBC Connectors from Standard Load Line-up, on page 25](#)
- [Configuration File Parameters, on page 25](#)

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/iomanagerxx/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/iomanager01/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 screenshot shows the 'Policy Reporting Configuration' pane with the following fields and options:

- *Staging Db Host Primary:** sessionmgr05
- *Staging Db Host Secondary:** sessionmgr05
- *Staging Port:** 27017
- *Staging Write Concern:** OneInstanceSafe
- *Staging Failover Sla:** 3000
- *Staging Max Replication Time:** 100
- *Cdr Staging Size Mb:** 100
- Cdr Db Host Primary:** sessionmgr01
- Cdr Db Host Secondary:** (empty)
- *Cdr Port:** 27017
- *Cdr Write Concern:** OneInstanceSafe
- *Cdr Failover Sla:** 3000
- *Cdr Max Replication Time:** 100
- *Time To Live In Days:** 5
- Disabled Policy Reports:** Location Usage, System Usage, Location Duration, Mac Address Usage, Session Duration. Includes 'Add' and 'Remove' buttons.
- Keep U T C Timing In C D R
- Jdbc Replication:**
- Ftp Server Configuration:**
- Actions:** Create Child: ...

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 from the Step 3 in [Configure a Reporting Server, on page 3](#).

-
- 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 3](#).

-
- 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 every 60 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 <i><dbname><separator><collection name><separator><date format mask><.suffix></i> .
Date Format Mask	This variable impacts the <i><date format mask></i> part of the name. Normally the format is <i>yyymmddmmss</i> (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: <i><db name><separator><collection name><separator><date format mask><.suffix></i> .

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 3](#).

- 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	<p>You can limit offline reporting to specific machines. You can select instances that need to participate in replication of reporting records.</p> <p>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.</p>
Override File Name Mask	This field is used to override the default file name for the generated CSV report. If not 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.

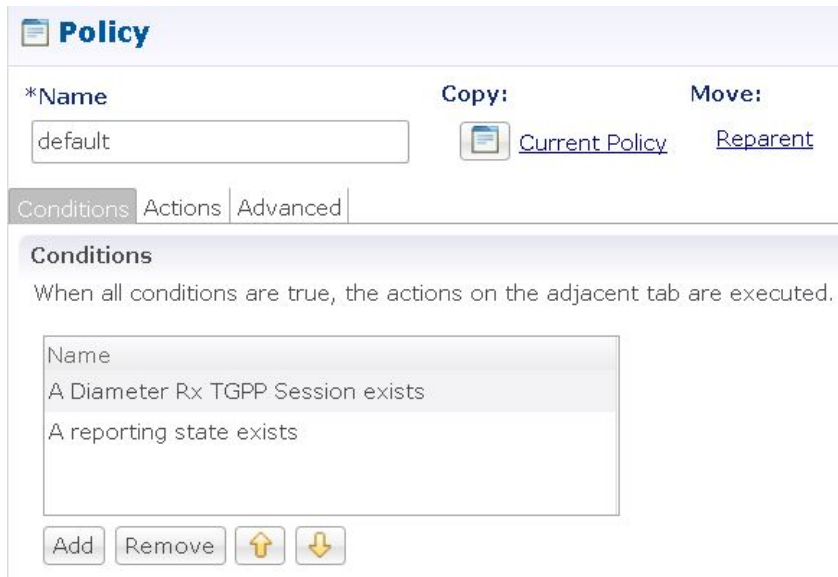
- b) Navigate to the data field that matches the field defined in the Reporting CDR column and click **OK**.

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



Policy

*Name: default

Copy:  Current Policy



Move: Reparent

Conditions | Actions | Advanced

Conditions

When all conditions are true, the actions on the adjacent tab are executed.

- Name
- A Diameter Rx TGPP Session exists
- A reporting state exists

Add Remove  

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:

- Select **Actions** tab.
- Select **Add global reporting data**.
- 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 its 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

Policy Reporting Field Type (Read Only)

Name
NETWORK

Policy Reporting Fields

*Code	*Db Field Name	*Db Type	*Precision
accessType	access_type	VARCHAR	30
cellSiteId	cell_site_id	VARCHAR	20
chargingId	charging_id	VARCHAR	60
circuitId	circuit_id	VARCHAR	20
deviceRatingGroup	device_rating_group	VARCHAR	30
framedIo	framed_io	VARCHAR	20

Add Remove Up Down

Actions

Copy:
[Current Policy Reporting Field Type](#)

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** field. New policy reporting fields can be added to this category.
- Step 4** Click **Add** to create a field.
- Provide a name to the field in the **Code** column.
 - Provide a name to the field in the **Db Field Name** column.
 - 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

Policy Reporting Field Type

Name
test

Policy Reporting Fields

*Code	*Db Field Name	*Db Type
testfield	testfield_d	VARCHAR

Add Remove Up Down

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

The screenshot shows the Cisco Policy Builder interface. The left sidebar contains a navigation menu with categories like Systems, Account Balance Templates, and Policy Reporting. The main area is titled 'Policy Cdr' and contains several sections:

- Policy Cdr Configuration:** Fields for *Name (PCRF-CDR), *Table Name (PCRF-CDR), Date Time Format, and *Version (1).
- Closing Reasons:** A table with columns *Code, Time Limit, Usage Limit, and Usage Field. One row is visible with *Code 'SESSION_CLOSED', Time Limit '0', Usage Limit '0', and Usage Field.
- Copy:** A link for 'Current Policy Cdr'.
- Reporting Cdr Columns:** A table with columns Code, Cdr Field Type, Type, Export Field, and Default Value. The row for 'balanceUsed' is highlighted with a red border, showing Cdr Field Type 'Data', Type 'accumulation', and Export Field checked.

- 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

The screenshot shows the 'Policy' configuration window for 'PCRF-CDR'. The 'Actions' tab is active, displaying a list of actions. The 'Add reporting data' action is selected. Below the list, there are 'Add', 'Remove', and arrow buttons. The 'Input Variables' section is partially filled with the following configuration:

Input Variables	Type	Operator	Value	Required
IReportingState (IReportingState)*	Output	default		Required
Name (String)*	Literal	default		Required
Value (Object)*	Literal	default		Required

Below the table, there is a section for 'Available Input Variables' with a link 'Add All' and a list item 'Add Reporting Scope (Object)'.

- 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

Policy

*Name: PCRF-CDR

Copy: [Current Policy](#) [Reparent](#)

Move: [Reparent](#)

Conditions **Actions** Advanced

Actions

Executed when all conditions are true.

Name

- Add reporting data
- Add reporting data
- Add reporting data

Add Remove ↑ ↓

Input Variables	Type	Operator	Value	
IReportingState (IReportingState)*	Output	default	IReportingState (A reporting state exists)	Required
Name (String)*	Literal	default	balanceUsed	Required
Value (Object)*	Output	default	Amount Charged1 (An OCSCargeReservationResponse exists)	Required
Reporting Scope (Object)	Output	default	Imsi (A Diameter Gx TGPP Session exists)	Remove

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

Disabled Policy Reports

Add Remove Keep U T C Timing In C D R

Jdbc Replication

Ftp Server Configuration

Frequency In Minutes
60

*Primary Server
10.10.1.1

*Primary User Name
test

*Primary Password

*Primary Destination Path
/

Secondary Server

Secondary User Name

Secondary Password

Secondary Destination Path
/

Actions

Create Child:
Reporting 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 b) 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.

- Enter the variable name in the **Code** column.
- Enter the database field name in the **Db Field Name** column.
- Select the database type from the **Db Type** drop-down list. By default, the database type is set to *VARCHAR*.
- 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

Policy Reporting Field Type

Name

Policy Reporting Fields

*Code	*Db Field Name	*Db Type	*Precision
chargingRuleBaseName	charging_rule_base_name	VARCHAR	0
requestedTotalOctets	requested_total_octets	BIGINT	0

Add Remove ↑ ↓

▼ Actions

Copy:
[Current Policy Reporting Field Type](#)

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:

- Click **Add** to add a new row to the table.
- 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
```