Plug-in Configuration

Overview

In CPS, reference data is considered information that is needed to operate the policy engine, but not used for evaluating policies. For example, in the **Reference Data** tab in Cisco Policy Builder, are the forms used to define systems, clusters, and instances, and to set times and dates used for tariff switching. The policy engine needs to refer to this data only to process policies correctly. However, the data does not define the policy itself.

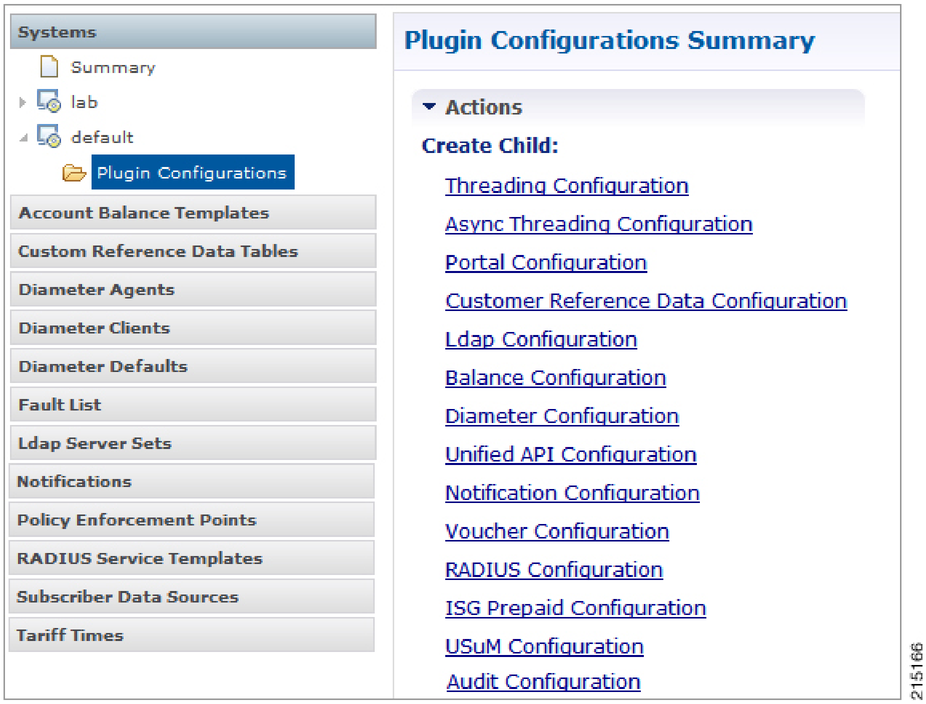
Cisco Policy Builder provides core plug-ins for customizing and optimizing your installation.

- Configurations set at the system level are system-wide except as noted in the bullet items below.
- Configurations set at the cluster level apply to that cluster and the instances in it. A value set here overrides the same value set at the system level.
- Configurations set at the instance level apply to the instance only and override the same value set at the cluster or system level.

Select the **Create Child** action in a **Plug-in Configuration** node in the **Systems** tree to define them. You can change any of the variables from the default, or choose not to use a plug-in, as necessary.

When you create a system from the example, the following configuration stubs appear at the cluster and instance level:

Figure 1: Create Child Action



Systems
- Summary
- lab
- default
  - Plugin Configurations

Account Balance Templates
Custom Reference Data Tables
Diameter Agents
Diameter Clients
Diameter Defaults
Fault List
Ldap Server Sets
Notifications
Policy Enforcement Points
RADIUS Service Templates
Subscriber Data Sources
Tariff Times

Plugin Configurations Summary

Actions

Create Child:

- Threading Configuration
- Async Threading Configuration
- Portal Configuration
- Customer Reference Data Configuration
- Ldap Configuration
- Balance Configuration
- Diameter Configuration
- Unified API Configuration
- Notification Configuration
- Voucher Configuration
- RADIUS Configuration
- ISG Prepaid Configuration
- USuM Configuration
- Audit Configuration

You are notified when a new policy is applied that overrides the existing configuration.

The notification is displayed as a warning icon above the configuration heading. When you hover over the warning icon, it displays the notification message as a tooltip. When there is an error and warning in the plugin configuration, then the error is overridden by a warning message.

A warning message is displayed under the following conditions:

- At the System level, if the selected plugin configuration is overridden by cluster or Instance plugin configuration.
- At the Cluster level, if the selected plugin configuration overrides the same plugin configuration at the system level or is overridden by the same plugin configuration at an Instance level.
- At the Instance level, if the selected plugin configuration overrides the same plugin configuration at system or cluster level.

Threading Configuration

A threading configuration utility is provided for advanced users.

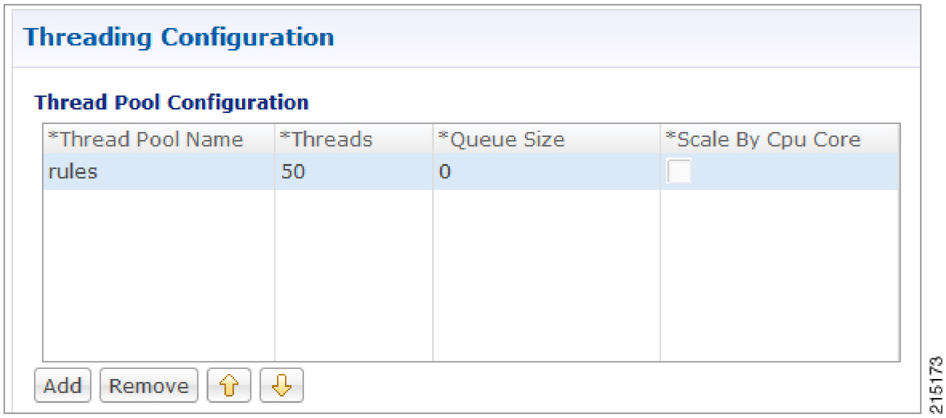
Click **Threading Configuration** in the right pane to add the threading configuration to the system. This is a performance tuning parameter and can be changed in case of a performance issue according to the call model and hardware. For further information, contact your Cisco Account representative.

The Threading Plug-in is for Mobility. The only value to set is **rules**. It controls the total number of threads in the Policy Engine (QNS) that are executing at any given time. The default value is 50.

It is recommended not to configure the value below 50. It can be set higher to help increase performance in certain situations where the queue full issue or performance issue is being observed. The value also depends on call model, hardware type.

A configuration example is shown below:

Figure 2: Thread Pool Configuration



Threading Configuration

Thread Pool Configuration

*Thread Pool Name	*Threads	*Queue Size	*Scale By Cpu Core
rules	50	0	□

The following parameters can be configured under Threading Configuration:

Table 1: Threading Configuration Parameters

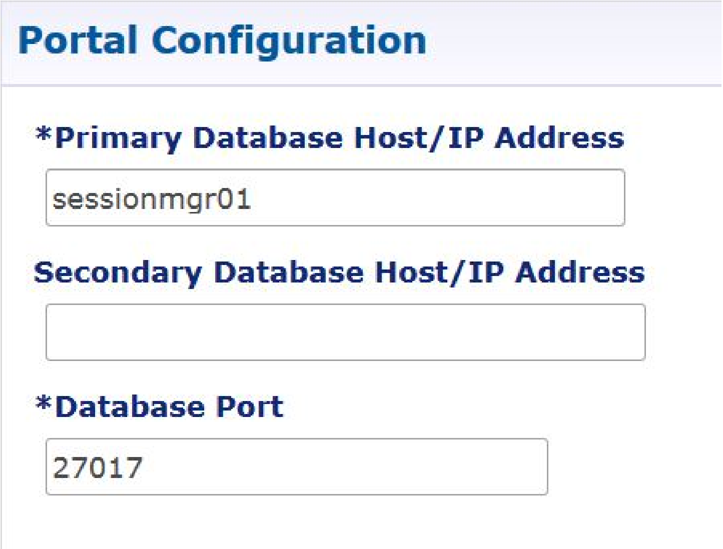
Parameter	Description
Thread Pool Name	Name of the Cisco thread pool i.e., rules.
Threads	Specify the threads to set in the thread pool. You can set rules thread ranging from 50 to 100 depending on the call flow (based on number of lookup operations). • rules = 50; Queue Size = 0; Scale By Cpu Core = unchecked • rules = 100; Queue Size = 0 (If TPS is > 2000 per Policy Server (QNS) depending on call model used; for example, if LDAP is enabled); Scale By Cpu core = unchecked The threads are driven based upon average response time of the message. The response time is call model dependent.

Parameter	Description
Queue Size	Specify the size of the queue before the threads are rejected. If value is greater than 50, performance may degrade because it holds the number of tasks in queue waiting for threads to be executed when TPS is high. If the value is lower than 50, the requests start dropping when all worker threads are busy in executing actions. The queue belongs to each Policy Server (QNS) process, and it holds incoming messages from Policy Directors (LB), but also internal events/messages (for example, an internal time change that triggers a policy evaluation). This is a performance tuning parameter and can be changed in case of a performance issue according to the call model and hardware. Default value is 0. **Note** In most of the setups, keep the queue size value default.
Scale By Cpu Core	Select this check box to enable the processor cores to scale the maximum number of threads. By default, this check box is unchecked.

Portal Configuration

Click **Portal Configuration** from right pane to add the configuration in the system.

Figure 3: Portal Configuration



Portal Configuration

*Primary Database Host/IP Address

sessionmgr01

Secondary Database Host/IP Address

*Database Port

27017

Parameter	Description
Primary Database Host/IP Address	IP address or a host name of the sessionmgr database.

Parameter	Description
Secondary Database Host/IP Address	Optional, this field is the IP address or a host name of a secondary, backup, or failover sessionmgr database.
Database Port	This is required. This is the port the Balance database uses, that is, the port of sessionmgr.

Async Threading Configuration

Click **Async Threading Configuration** under **Systems** > ***Name of the system*** > **Plugin Configuration** in the right pane to add the configuration in the system.

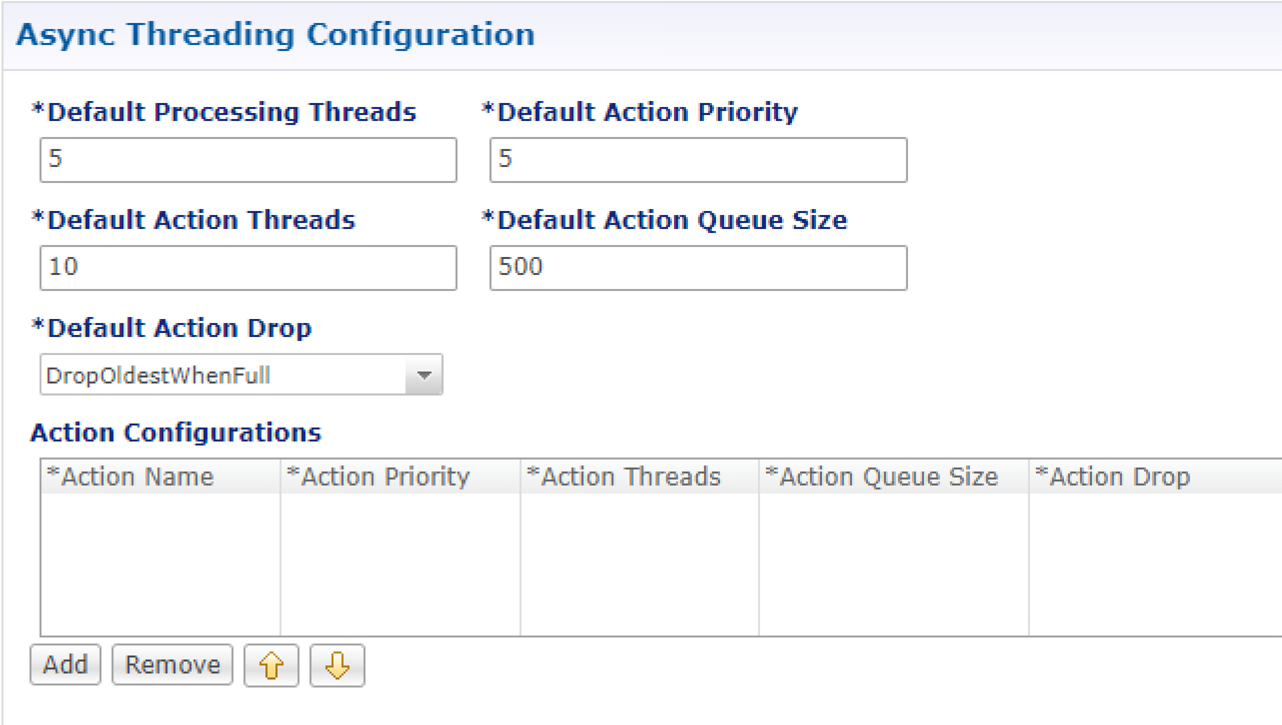
Use the default values for the Async Threading Plug-in. Similar to the Threading Plug-in, the Async configuration controls the number of asynchronous threads operating in the Policy Engine. The Policy Engine handles two basic types of messages - synchronous and asynchronous. Synchronous messages block and expect a response.

Asynchronous messages are sent into the Policy Engine but do not expect a response. Therefore, the Policy Engine can defer those to worker threads that operate along side the main Policy Engine threading execution without causing too much traffic for performance.

For example, when an NDM calls an aynsc action based on call flow and the same threads are used to perform async action across async submissions into engine from multiple NDM's.

Note Always select the link for Async Threading Configuration to configure your CPS system.

Figure 4: Async Threading Configuration



Async Threading Configuration

*Default Processing Threads: 5

*Default Action Priority: 5

*Default Action Threads: 10

*Default Action Queue Size: 500

*Default Action Drop: DropOldestWhenFull

Action Configurations

*Action Name	*Action Priority	*Action Threads	*Action Queue Size	*Action Drop

The following parameters can be configured under Async Threading Configuration.

Table 2: Async Threading Configuration Parameters

Parameter	Description
Default Processing Threads	Specifies the number of threads that are allocated to process actions based on priority. When you increase the value of this parameter, the number of asynchronous threads in the pool increases and more number of threads are able to execute asynchronous actions. Although the value depends on TPS, if increased too much, it degrades the performance. That is because these threads would occupy more resources to execute more actions simultaneously. By decreasing the value, the number of threads in pool decrease and there may be a delay in processing actions. Default value is 5.

Parameter	Description
Default Action Priority	Specifies the priority assigned to an action when it is not specified in the Action Configurations table. Default value is 5. If default action priority is set when there is no action specified in the action table, there is no impact. However, if action priority is specified in the action table and also in the default action priority, then the action with the higher priority takes precedence. **Example 1:** • Action Configuration table: 600 (task priority) • Default Action Priority: 700 In the preceding example, the default action takes priority over the action defined in the action configuration table. **Example 2:** • Action Configuration table: 600 (task priority) • Default Action Priority: 500 In the preceding example, the action defined in the action configuration table takes priority over the action defined in the default action priority.
Default Action Threads	Specifies the number of threads assigned to process the action when it is not specified in the Action Configurations table. These are action specific threads, therefore, based on the increased or decreased value, the number of threads are allocated to a specific action. It is recommended that the default action thread value be maintained. However, if there are actions that are executed more frequently, then enter a value in the action table that is higher than the one in the default action thread. Default value is 10.

Parameter	Description
Default Action Queue Size	Specifies the number of actions that can be queued up for an action when it is not specified in the Action Configurations table. Increasing this value increases the action-specific queue size. For example, if action specific threads are 10 and queue size is defined as 600, then CPS accepts 610 specific action threads. That is, 10 threads are executed while the balance 600 are in queue. **Note** It is recommended that the default action queue size should not be changed. If required, insert an action in the action table and increase the queue size of that action such that it takes precedence over the default action queue size. Decreasing this value decreases the action-specific queue size. For example, if action specific threads are 10 and queue size is defined as 400, then CPS at accept 410 specific action threads. That is, 10 threads are executed while the balance 400 are in queue. If total action specific requests are 500, the balance 90 are dropped. **Note** It is recommended that the default action queue size should not be changed. If a specific action is executed lesser number of times, insert an action in the action table and decrease the queue size of that action Default value is 500.
Default Action Drop	When **DropOldestWhenFull** action is selected, CPS drops the oldest queued action when a new action is added to the full queue. When **DropWhenFull** action is selected, CPS drops the new queued action when it is added to the already full queue. When **DoNotDrop** action is selected, none of the actions are dropped. This makes sure that all the actions are processed. Default value is **DropOldestWhenFull**.
Action Configurations Table	
Action Name	The name of the action. This must match the implementation class name. For example, com.broadhop.notifications.actions.ISendSMSNotificationRequest.
Action Priority	The priority of the action. Used by the default processing threads to determine which action to execute first. **Note** Based on the action, value should be defined. There is no default or recommended value.
Action Threads	Specifies the number of threads dedicated to processing this specific action. **Note** Based on the action, value should be defined. There is no default or recommended value.

Parameter	Description
Action Queue Size	Specifies the number of actions that can be queued up. **Note** Based on the action, value should be defined. There is no default or recommended value.
Action Drop	When **DropOldestWhenFull** action is selected, CPS drops the oldest queued action when a new action is added to the full queue. When **DropWhenFull** action is selected, CPS drops the new queued action when it is added to the already full queue. When **DoNotDrop** action is selected, none of the actions are dropped. This makes sure that all the actions are processed. Default value is **DropOldestWhenFull**.

Custom Reference Data Configuration

Configure your system, cluster, and instance for the first time to use Custom Reference Data Table plug-in. Then you can create as many tables as needed.

Important When you add new fields in CRD, manually update the new fields with appropriate values for all the existing entries in CRD. Otherwise DRA doesn't show any values for these new fields for existing entries and this can cause routing failures.

Click **Custom Reference Data Configuration** from right pane to add the configuration in the system.

- HA example:
  - Primary Database Host/IP Address: sessionmgr01
  - Secondary Database Host/IP Address: sessionmgr02
  - Database Port: 27717

The following parameters can be configured under Custom Reference Data Configuration.

Table 3: Custom Reference Data Configuration Parameters

Parameter	Description
Primary Database Host/IP Address	IP address or a host name of the sessionmgr database. For example, sessionmgr01.
Secondary Database Host/IP Address	(Optional) This field is the IP address or a host name of a secondary, backup, or failover sessionmgr database. For example, sessionmgr02.

Parameter	Description
Database Port	Port number of the sessionmgr. **Note** Make sure that the value for this field is same as filled in for both the Primary Database Host/IP Address and Secondary Database Host/IP Address fields. Default value is 27717.
Db Read Preference	Describes how sessionmgr clients route read operations to members of a replica set. Select one of the following options from drop-down list: • Primary: All operations read from the current replica set primary member. • PrimaryPreferred: In most situations, operations read from the primary database host. However, if this host is unavailable, operations read from the secondary databse host. • Secondary: All operations read from the secondary members of the replica set. • SecondaryPreferred: In most situations, operations read from secondary members. However, if a secondary database host is unavailable, operations read from the primary database host. Default value is Primary. For more information, see http://docs.mongodb.org/manual/core/read-preference/.
Connection Per Host	Number of connections that are allowed for each database host. Default value is 100. Connection Per Host is a performance tuning parameter and can be changed in case of a performance issue according to the call model and hardware.
Avp Persists	Use this table to configure certain AVPs that you want to store in the session database. AVPs that are not configured as part of this table, are not persisted. • Name: Enter the name for the AVP value. • Avp Name: The name of the CRD/policy derived AVP. To retrieve the stored AVPs from the session, use the Customer Reference Data Debug AVPs. This retriever is used to send the stored AVPs in any diameter message, and available in the **PolicyState/Session data to Custom AVP Mapping** under Custom AVP Profiles. **Restriction** When you configure the AVP Persists table in the Policy Builder, for each AVP, configure both the AVP name and name. If no values are added for these fields, then the particular AVP is not added to the Gx session. This scenario leads to unavailability of the specific AVP and hence, no custom AVP are sent.

For more information on Custom Reference Data API Usage, see the *CPS Operations Guide* for this release.

Balance Configuration

Click **Balance Configuration** in the right pane to add the configuration in the system.

The following parameters can be configured under Balance Configuration:

Table 4: Balance Configuration Parameters

Parameter	Description
Primary Database Host/IP Address	IP address or a host name of the sessionmgr database.
Secondary Database Host/IP Address	Optional, this field is the IP address or a host name of a secondary, backup, or failover sessionmgr database.
Database Port	This is required. This is the port the Balance database uses, that is, the port of sessionmgr.
Db Write Concern	Controls the write behavior of Session Manager and for what errors exceptions are raised. Db Write Concern defined in Cluster page applies only to Admin, Trace and Endpoint databases. Select one of the following options from drop-down list: • OneInstanceSafe: This means the system waits for confirmation of writing in primary member. • TwoInstanceSafe: This means the system waits for confirmation in primary and one secondary member. Default value is OneInstanceSafe. For more information, see MongoDB documentation.
Db Read Preference	Read preference describes how sessionmgr clients route read operations to members of a replica set. You can select from the following drop-down list: • Primary • PrimaryPreferred • Secondary • SecondaryPreferred For more information, see http://docs.mongodb.org/manual/core/read-preference/.
Failover Sla Ms	This parameter is used to enter the amount of time to wait before starting failover database handling. The time is in milliseconds.

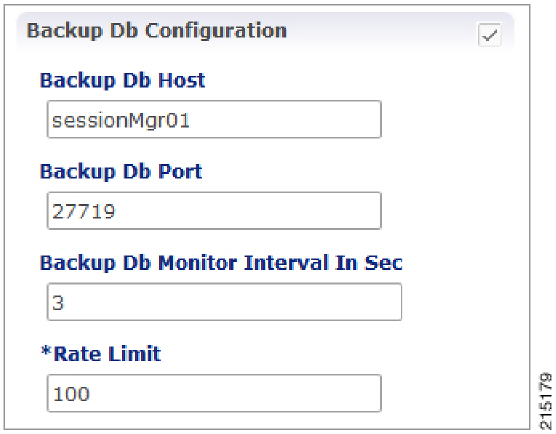
Parameter	Description
Max Replication Wait Time Ms	This option specifies a time limit, in milliseconds, for the write concern. This parameter is applicable only if you select TwoInstanceSafe in Db Write Concern. This parameter causes write operations to return with an error after the specified limit, even if the required write concern eventually succeeds. When these write operations return, MongoDB does not undo successful data modifications performed before the write concern exceeded the replication wait time limit. This time is in milliseconds.
Default Minimum Dosage Time Based	This field is optional but recommended. This is the minimum amount of time that is granted for a reservation, assuming quota is not exhausted. If you want to manage subscriber balances on the basis of time used, check with the network device administrator and configure this value to be slightly larger than the minimum amount of time the network device such as an SCE or ISG accepts for a reservation. Minimum value is 2 seconds.
Default Minimum Dosage Volume Based	This field is optional but recommended. This is the minimum amount of volume that is granted for a reservation, assuming quota is not exhausted. If you try to make a reservation for 1 KB, and your minimum is 10 KB, the router rejects it because it is too small an amount to bother with.
Expired Reservations Purge Time (minutes)	The amount of time a record of expired reservations is retained and Cisco MsBM attempts to charge them. Expired reservations are charged only if sufficient quota is still available; that is, expired reservations do not retain the lock on quota that current reservations do. Default value is 0.

<table>
<tr><th>Parameter</th><th>Description</th></tr>
<tr><td>Recurring Refresh Max Delay (minutes)</td><td>The amount of time refreshing of recurring quotas are staggered across randomly, for sessions that are not actively using quota but are still established.
This parameter is used in cases where subscribers always have a session, but is not using their quota actively. This allows staggering of recurring refreshes where you have set all their subscribers to refresh at the same time, say midnight. It avoids spiking the CPU.
Default value is 0.
To calculate the Recurring Refresh Max Delay, use the following:
Recurring Refresh Max Delay = (Number of sessions / Max Timer TPS) * 2
For example:
If 30 million sessions are present on the system, and Max Timer TPS is configured to 2000, then<table><tr><td>Recurring Refresh Max Delay</td><td>= (30,000,000 / 2000) * 2</td></tr><tr><td></td><td>= 500 minutes ~ 8.33 hours</td></tr></table>In case you want to configure a lesser time for the Recurring Refresh Max Delay, then the Max Timer TPS needs to be increased accordingly.
<b>Note</b> Cisco recommends using Re-evaluation diffusion buckets and Re-evaluation diffusion interval (in milliseconds) instead of Recurring Refresh Max Delay (minutes). For more information, see Adding an HA Cluster.</td></tr>
<tr><td>Remote Database Lookup Filter Type</td><td>This drop-down list is used to do a lookup in remote databases bases on selected filter type. This is similar to Filter Type drop-down under API Router Configuration.
By default, NetworkId is selected.
<b>Note</b> Filter type must be same in API Router Configuration and Balance Configuration in Policy Builder.</td></tr>
<tr><td>Reduce Dosage on Threshold</td><td>When checked, reservation dosages are reduced as a Cisco MsBM threshold is approached. This way, a dosage does not pass a threshold by a large amount before notification of the breach is sent out. When unchecked, normal dosage is granted. Recall that when enabled, messaging becomes much more chatty, but threshold breach accuracy is enhanced.</td></tr>
<tr><td>Submit Balance Events To Reporting</td><td>Submits balance transaction to the policy engine, and these can be reflected in reporting.</td></tr>
</table>

Parameter	Description
Enable Crd Balance Template Lookups	When checked, CPS is enabled to lookup CRD defined balance templates. If the CRD tables are not defined, this feature is disabled. **Note** Even if the CRD tables are not defined as required, and this feature is disabled, the **Dynamic Reference Data Key** field is still enabled but only for Policy Builder defined Account Balance Templates. For more information, see Dynamic Reference Data Key.
Remote Database	
Name	String - Name of the remote database.
Key Prefix	Key prefix to be match for the remote database to be selected for lookup.
Connections Per Host	Number of connections that can be created per host. Default value is 5.
Db Read Preference	Read preference describes how sessionmgr clients route read operations to members of a replica set. You can select from the following drop-down list: • Primary • PrimaryPreferred • Secondary • SecondaryPreferred For more information, see http://docs.mongodb.org/manual/core/read-preference/.
Primary Database Host/IP address	IP address or a host name of the sessionmgr database.
Secondary Database Host/IP address	Optional, this field is the IP address or a host name of a secondary, backup, or failover sessionmgr database.
Port	Port number of the remote sessionmgr database. It must be the same for both the primary and secondary databases.
Backup Db Host On Local Site	String - The host name of backup database for remote balance for current site. Default value is sessionmgr01.
Backup Db Port on Local Site	The port number of backup database for remote balance for current site. Default value is 27719.

If you have a Geo-Redundancy setup, click **Backup Db Configuration**. It stores back up of entire balance records. If the primary balance database goes down, CPS will check the balance record on both secondary and backup databases, and take the latest version for processing.

Figure 5: Backup Db Configuration



Backup Db Configuration

Backup Db Host: sessionMgr01

Backup Db Port: 27719

Backup Db Monitor Interval In Sec: 3

*Rate Limit: 100

The following parameters can be configured under **Backup Db Configuration**:

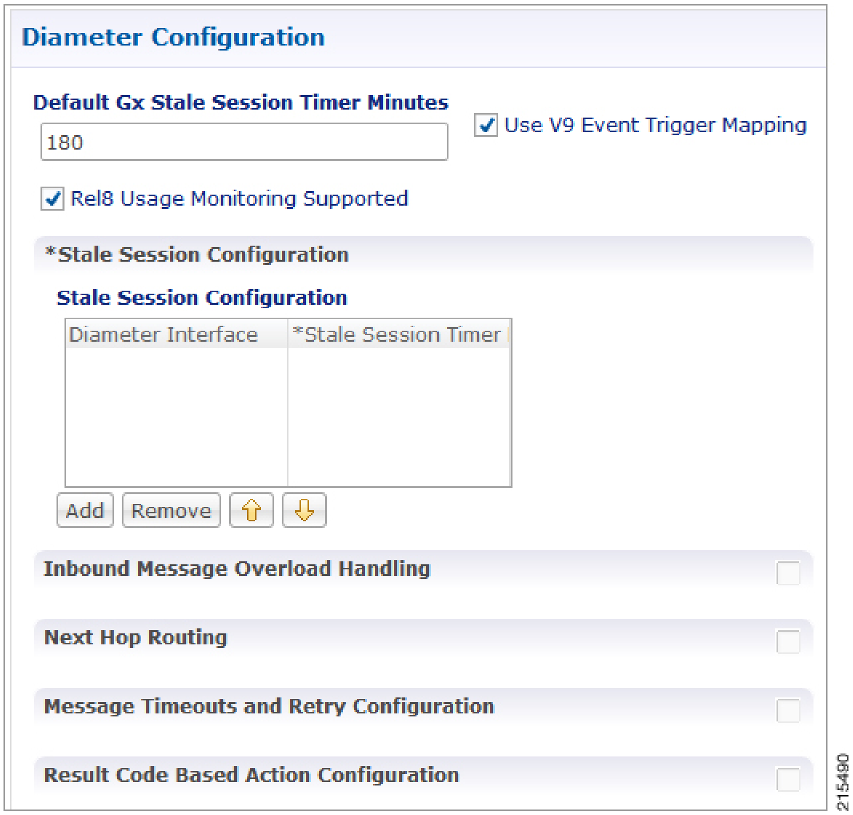
Table 5: Backup Db Configuration Parameters

Parameter	Description
Backup Db Host	Default value is sessionmgr01.
Backup Db Port	Default value is 27719.
Backup Db Monitor Interval In Sec	Used in thread which updates the primary balance DB (when primary balanceDB is available after fail over) with 'BackupBalance' db records. Default value is 3 seconds.
Rate Limit	Used to control the TPS (with how much TPS reconciliation should happen once primary balance db is up).

Diameter Configuration

Click **Diameter Configuration** in the right pane to add the configuration in the system.

Figure 6: Diameter Configuration



Diameter Configuration

Default Gx Stale Session Timer Minutes

180

☑ Use V9 Event Trigger Mapping

☑ Rel8 Usage Monitoring Supported

*Stale Session Configuration

Stale Session Configuration

Diameter Interface	*Stale Session Timer

Inbound Message Overload Handling □

Next Hop Routing □

Message Timeouts and Retry Configuration □

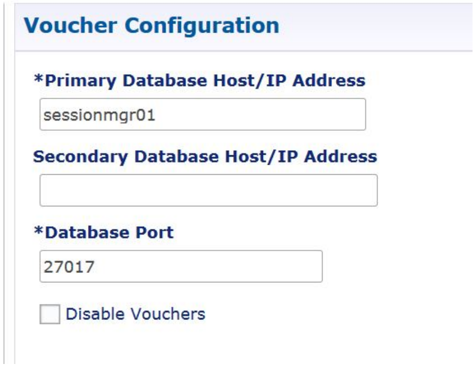
Result Code Based Action Configuration □

For more information on the parameters under this plug-in, see Diameter Configuration.

Voucher Configuration

Click **Voucher Configuration** in the right pane to add the configuration in the system.

Figure 7: Voucher Configuration



Voucher Configuration

*Primary Database Host/IP Address

sessionmgr01

Secondary Database Host/IP Address

*Database Port

27017

□ Disable Vouchers

The voucher plug-in uses the following defaults:

- HA example:

- Primary: sessionmgr01
- Secondary: sessionmgr02
- Port: 27718

The following parameters can be configured under Voucher Configuration:

Table 6: Voucher Configuration Parameters

Parameter	Description
Primary Database Host/IP Address	The IP address or a host name of the Session Manager database that holds voucher information for Cisco Policy Builder and Cisco Policy Server.
Secondary Database Host/IP Address	The IP address or a host name of the database that provides fail over support for the primary database. This is the mirror of the database specified in the Primary Database IP Address field.
Database Port	Port number of the sessionmgr. It must be the same for both the primary and secondary databases.
Disable Vouchers	Select the check box to disable voucher configuration.

Unified API Configuration

Click **Unified API Configuration** in right pane to add the configuration in the system.

The following parameters can be configured under Unified API Configuration:

Table 7: Unified API Configuration Parameters

Parameter	Description
Fields To Wrap With Cdata Tags	This is a CSV separated string. The Unified API can handle CDATA fields. Use the Plug-in configuration in Policy Builder to set CDATA fields for the main Unified API. The property `ua.cdata.fields` is used to set the fields that must be wrapped in CDATA tags for the client CommFactory to properly send and receive API requests. `-Dua.cdata.fields=networkId,password,data,oldNetworkId,oldPassword,newPassword` is the default.
Session Route Key	Session route key that vDRA uses to look up the peer group and route the Rx AAR message to the correct PCRF. When vDRA makes REST API requests to multiple PCRFs for session query using the Framed-IPv6-Prefix received in the Rx AAR message, one of the PCRF that has the corresponding Gx session sends this session route key in the response. vDRA then uses this key to look up the peer group and route the Rx AAR message to the correct PCRF.

Parameter	Description
Max API TPS Threshold	This value defines maximum API TPS supported per Policy Server (qns) process. Default value is 0. For API rate limiting at HAProxy, refer to Note [1].
HTTP Error Code on Threshold Reached	HTTP response code to send when API request is throttled (rate limiter acquire fails). Default value is 500 (Internal Server Error).
Submit Requests To Audit Log	Select the check box to log requests to API in audit log. Default value is True (checked).
Submit Read Requests To Audit Log	Select this check box to log read requests in audit log. Default value is False (unchecked).

[1] HAProxy has `maxconn <conns>` configuration which manages the total number of connections that haproxy, as a service, queues or processes at a single point of time.

Notification Configuration

Notification in Cisco Policy Builder relates to pushing messages from Cisco Policy Builder to subscribers. The messages are used to alert the subscriber of issues as well as opportunities on their network. Not only can you alert subscribers, but you can also send messages to any address, for example, system monitoring addresses.

Currently, Cisco Policy Builder offers following notification types for Mobile:

- Apple iOS devices/iPhone® push (iOS devices)
- Email (IMAP only)
- SMS notification (SMPP v 3.4)
- Realtime Notification

The following parameters can be configured under **Notification Configuration**. For more information about these parameters, see the Notification Services chapter.

Table 8: Notification Configuration Parameters

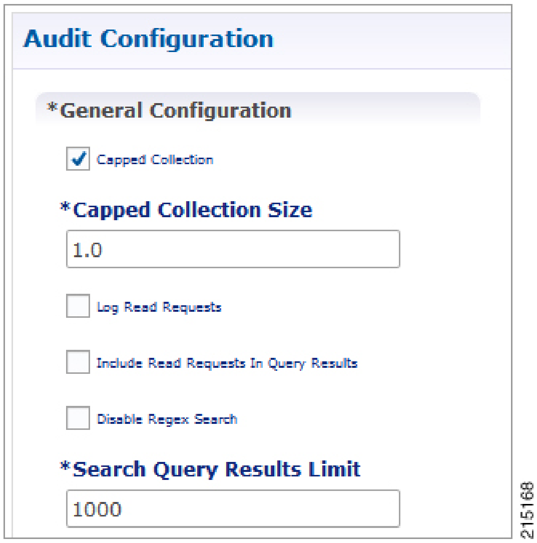
Parameter	Description
Apple Push Notification Configuration	Select this check box to configure the connection for a push to an Apple iOS device or iPhone.
Email Notification Configuration	Select this check box to configure the connection for an email notification.
SMS Notification Configuration	Select this check box to configure the connection for a SMS notification.

Parameter	Description
Realtime Notification Configuration	Select this check box to configure the connection for a realtime notification.

Audit Configuration

Click **Audit Configuration** in the right pane to add the configuration in the system.

Figure 8: Audit Configuration



Audit Configuration

*General Configuration

☑ Capped Collection

*Capped Collection Size

1.0

□ Log Read Requests

□ Include Read Requests In Query Results

□ Disable Regex Search

*Search Query Results Limit

1000

The following parameters can be configured in the **General Configuration** pane under Audit Configuration:

Table 9: Audit Configuration Parameters

Parameter	Description
Capped Collection check box	Select this check box to activate capped collection function.
Capped Collection Size	By default, the Audit History uses a 1 GB capped collection in MongoDB. The capped collection automatically removes documents when the size restriction threshold is hit. Configuration in Policy Builder is done in GB increments. It is possible to enter decimals, for example, 9.5 will set the capped collection to 9.5 GB.
Log Read Requests check box	Select this check box if you want read requests to be logged.
Include Read Requests In Query Results check box	Select this check box only if you want to include read requests to be displayed in query results.
Disable Regex Search check box	If you select this check box, the use of regular expressions for queries is turned off in the Policy Builder configuration.

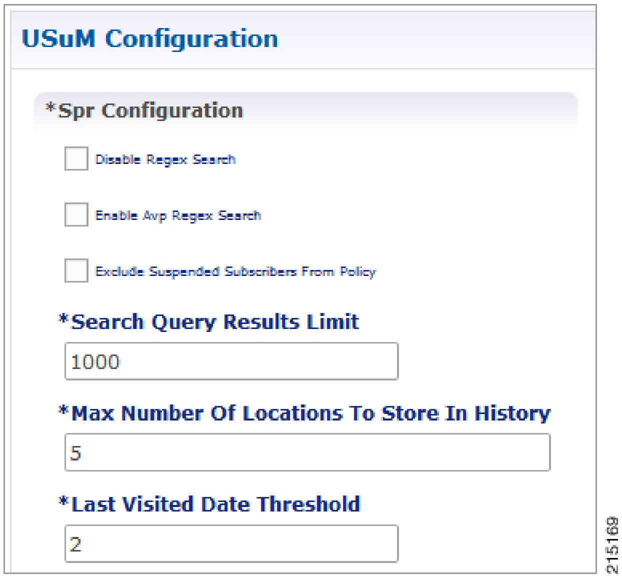
Parameter	Description
Search Query Results Limit	This parameter limits the search results.

For more information related to other parameters like Queue Submission Configuration, Database Configuration, Shard Configuration under Audit Configuration, refer to the *CPS Operations Guide* for this release.

USuM Configuration

Click **USuM Configuration** from right pane to add the configuration in the system.

Figure 9: USuM Configuration



USuM Configuration

*Spr Configuration

□ Disable Regex Search

□ Enable Avp Regex Search

□ Exclude Suspended Subscribers From Policy

*Search Query Results Limit: 1000

*Max Number Of Locations To Store In History: 5

*Last Visited Date Threshold: 2

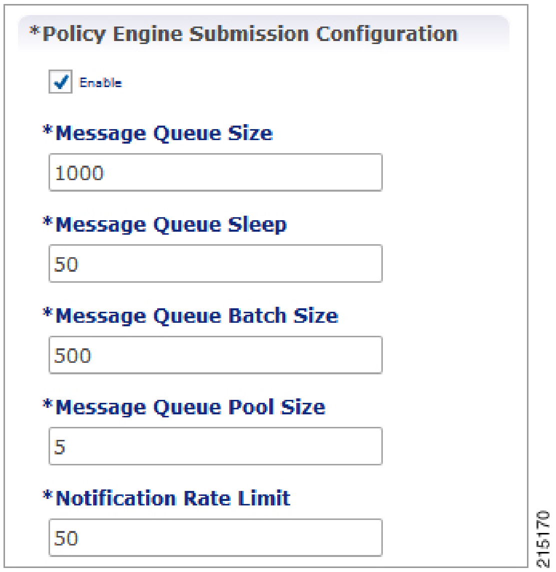
The following parameters can be configured in the **Spr Configuration** pane under USuM Configuration:

Table 10: USuM Configuration Parameters - 1

Parameter	Description
Spr Configuration	
Disable Regex Search	For SP Wi-Fi, you can use email ID which has realm, username, and so on, as key of SPR. So, part of the string needs to match for regex support. **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.
Enable Avp Regex Search	For regex search on values for AVP for SPR.
Exclude Suspended Subscribers From Policy	If the subscriber state is Suspended, SPR does not validate IMSI.

Parameter	Description
Search Query Results Limit	Used to limit search if you are not passing any IMSI/MSISDN (NetworkID) in control center to list subscriber. Default value is 1000.
Max Number Of Locations To Store In History	It is used to track subscriber last location to maintain history. Maximum "n" last locations are stored as location history.
Last Visited Date Threshold	This parameter is used to identify if the subscriber is visiting same location again (based on the location history). If the subscriber is vising the same location, then it will change the last visited date if current visited date is more than last visited date + "n" days defined here.

Figure 10: Policy Engine Submission Configuration



*Policy Engine Submission Configuration

☑ Enable

*Message Queue Size

1000

*Message Queue Sleep

50

*Message Queue Batch Size

500

*Message Queue Pool Size

5

*Notification Rate Limit

50

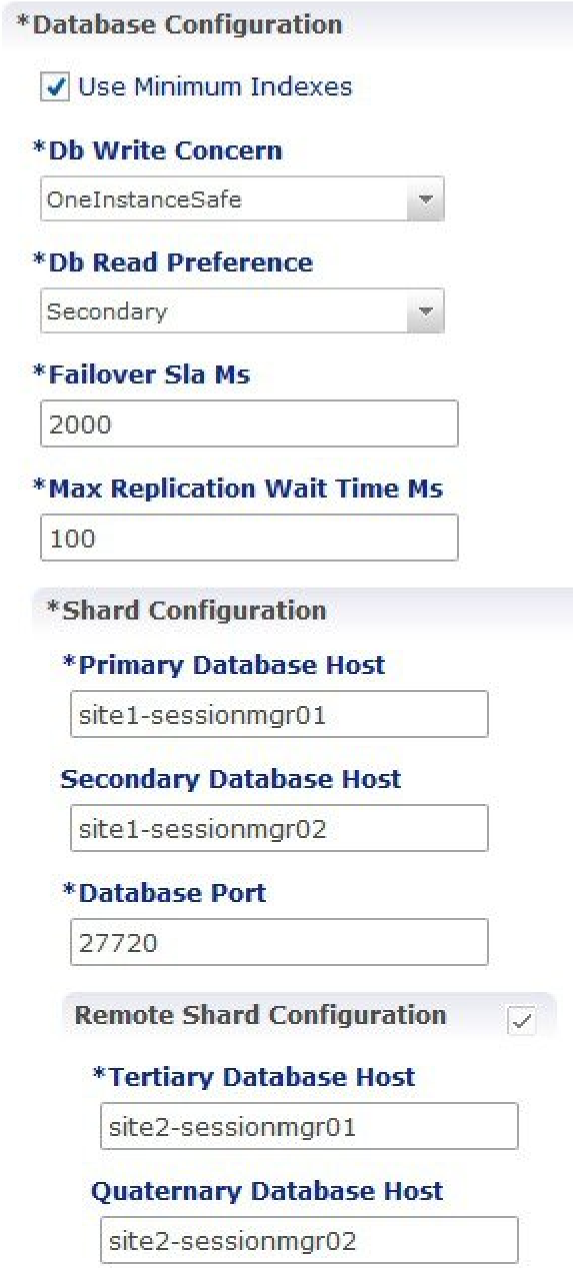
The following parameters can be configured in the **Policy Engine Submission Configuration** pane under USuM Configuration:

Table 11: USuM Configuration Parameters - 2

Parameter	Description
Enable check box	Keep it default.
Message Queue Size	Queue to hold data to generate internal SPR Refresh events for policy engine during Create, Update, Delete of subscriber.
Message Queue Sleep	Sleep before popping next batch for generating SPR Refresh events for policy engine for RAR processing.
Message Queue Batch Size	Batch size for fetching number of subscriberIds in one go for generating SPR Refresh events for policy engine for RAR processing.

Parameter	Description
Message Queue Pool Size	Message queue pool size to consume the data from queue and generate SPR Refresh events.
Notification Rate Limit	Rate limiting for generating SPR Refresh events. SPR Refresh events is used to generate RAR for active session where subscriber data has been change.

Figure 11: Database Configuration



*Database Configuration

☑ Use Minimum Indexes

*Db Write Concern: OneInstanceSafe

*Db Read Preference: Secondary

*Failover Sla Ms: 2000

*Max Replication Wait Time Ms: 100

*Shard Configuration

*Primary Database Host: site1-sessionmgr01

Secondary Database Host: site1-sessionmgr02

*Database Port: 27720

Remote Shard Configuration ☑

*Tertiary Database Host: site2-sessionmgr01

Quaternary Database Host: site2-sessionmgr02

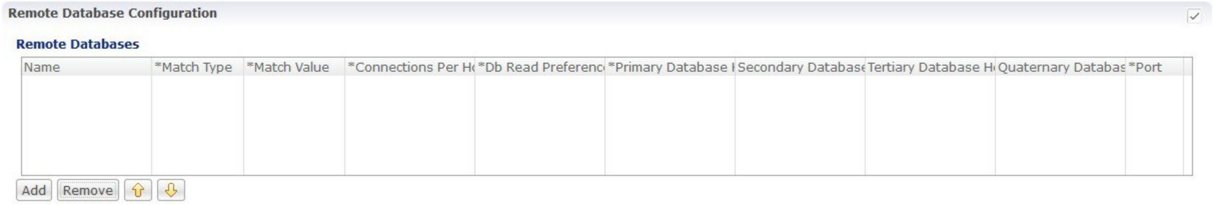
The following parameters can be configured in **Database Configuration** pane under USuM Configuration:

Table 12: USuM Configuration Parameters - 3

Parameter	Description
Database Configuration	
Use Minimum Indexes	It is used to decide what all indexes need to be created on SPR collection by default. You need all the indexes to be created (You can select this check box when number of subscribers are low, for example, less than 50K). Default value is unchecked.
Db Write Concern	Controls the write behavior of Session Manager and for what errors exceptions are raised. Db Write Concern defined in Cluster page applies only to Admin, Trace and Endpoint databases. Select one of the following options from drop-down list: • OneInstanceSafe: This means the system waits for confirmation of writing in primary member. • TwoInstanceSafe: This means the system waits for confirmation in primary and one secondary member. Default value is OneInstanceSafe. For more information, see MongoDB documentation.
Db Read Preference	Read preference describes how sessionmgr clients route read operations to members of a replica set. You can select from the following drop-down list: • Primary • PrimaryPreferred • Secondary • SecondaryPreferred For more information, refer to http://docs.mongodb.org/manual/core/read-preference/. **Important** For consistent profile updates across multiple sessions for same subscriber, Cisco recommends to set the **Db Read Preference** as *PrimaryPreferred*.
Failover Sla Ms	This parameter is used to enter the amount of time to wait before starting failover database handling. The time is in milliseconds.

Parameter	Description
Max Replication Wait Time Ms	This option specifies a time limit, in milliseconds, for the write concern. This parameter is applicable only if you select TwoInstanceSafe in Db Write Concern. This parameter causes write operations to return with an error after the specified limit, even if the required write concern eventually succeeds. When these write operations return, MongoDB does not undo successful data modifications performed before the write concern exceeded the replication wait time limit. This time is in milliseconds.
Shard Configuration **Important** The host names must exactly be the same host name used when the corresponding replica-set is created in Mongo. Only the data holding members need to be configured (and not the arbiters).	
Primary Database Host	String - Primary Host Address.
Secondary Database Host	String - Secondary Host Address.
Database Port	Default value is 27720.
Remote Shard Configuration **Important** Remote shard configuration is used only for GR deployments. The host names must exactly be the same host name used when the corresponding replica-set is created in Mongo. Only the data holding members need to be configured (and not the arbiters).	
Tertiary Database Host	String - Tertiary Host Address.
Quaternary Database Host	String - Quaternary Host Address.

Figure 12: Remote Database Configuration



Remote Database Configuration

Remote Databases

Name	*Match Type	*Match Value	*Connections Per H	*Db Read Preferenc	*Primary Database I	Secondary Databas	Tertiary Database H	Quaternary Databas	*Port

Click **Add** to add a new row in the **Remote Database Configuration** pane. The following parameters can be configured in the **Remote Database Configuration** pane under **USuM Configuration**:

Note To enable CPS to route the Sh data based on Gx CCR-I origin-host pattern, you need to enable **Remote Database Configuration**. For more information, see External Profile Cache.

Important Remote database configuration is used only for GR deployments. The host names must exactly be the same host name used when the corresponding replica-set is created in Mongo. Only the data holding members need to be configured (and not the arbiters).

Table 13: USuM Configuration Parameters - 4

Parameter	Description
Name	String - Name of the remote database.
Match Type	Select any one of the following values from the drop down: • StartsWith • Regex • EndsWith • Equals
Match Value	A string value which matches the MatchType specified. In case of Regex, you need to specify valid java regex pattern. This is used to lookup the remoteDB specified for a subscriber match for read/write operations on the SPR database.
Connections Per Host	This parameter is not used in USuM Configuration.
Db Read Preference	Read preference describes how sessionmgr clients route read operations to members of a replica set. You can select from the following drop-down list: • Primary • PrimaryPreferred • Secondary • SecondaryPreferred For more information, refer to http://docs.mongodb.org/manual/core/read-preference/.
Primary Database Host	Host name of the remote sessionmgr database.
Secondary Database Host	(Optional) Host name of a secondary, backup, or failover sessionmgr database.
Tertiary Database Host	Host name of the tertiary database.
Quaternary Database Host	Host name of the quaternary database.
Port	Port number of the remote sessionmgr database. It must be the same for both the primary and secondary databases. Default value is 27720.

Scheduled Events

The Scheduled Events plug-in is configured in the Policy Builder to implement offline notifications and SPR cleanup. Offline notifications send an SMS notification to an off-line subscriber indicating that their quota is about to expire. SPR cleanup allows you to delete subscriber data that is no longer needed or valid. For example, a subscriber account no longer has any services assigned to it, and therefore should be deleted from the database.

Enable Scheduled Events

To enable the scheduled events framework, this feature has to be enabled in the feature set of Policy Server and Policy Builder. The following packages, when added to the respective servers, deploy the functionality of scheduledEvents during a session:

- In the Policy Builder – com.broadhop.client.feature.scheduledevents package is added.
- In the Policy Server – com.broadhop.scheduledevents.service.feature package is added.

To add **Scheduled Events Configuration**, perform the following steps:

Step 1 If this is HA environment, edit the corresponding features files in Cluster Manager VM:

In the `/var/qps/current_config/etc/broadhop/pb/features` file, add the following line:

```
com.broadhop.client.feature.scheduledevents
```

In the `/var/qps/current_config/etc/broadhop/pcrf/features` file, add the following line:

```
com.broadhop.scheduledevents.service.feature
```

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

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

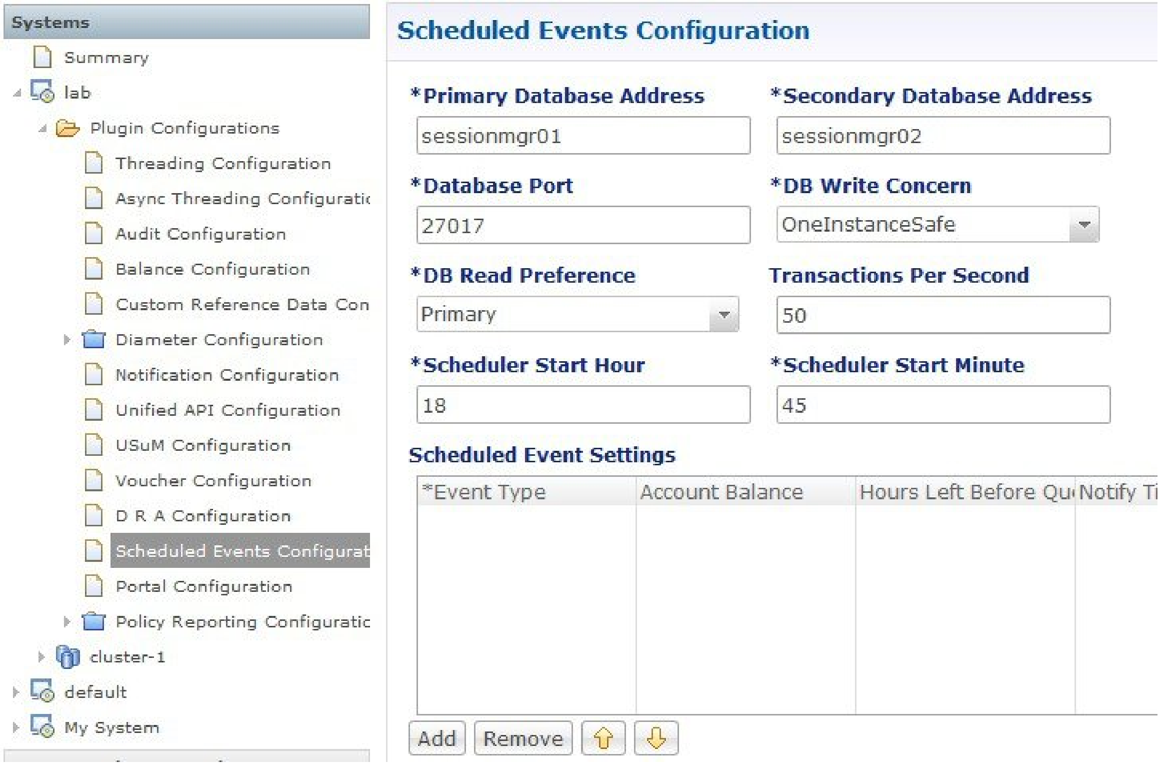
```
/var/qps/install/current/scripts/upgrade/reinit.sh
```

Scheduled Events Configuration

Step 1 Click **Scheduled Events Configuration** in the right pane.

Step 2 In the **Scheduled Event Configuration** pane and enter the values for the fields provided.

Figure 13: Scheduled Events Configuration



Scheduled Events Configuration

*Primary Database Address: sessionmgr01

*Secondary Database Address: sessionmgr02

*Database Port: 27017

*DB Write Concern: OneInstanceSafe

*DB Read Preference: Primary

Transactions Per Second: 50

*Scheduler Start Hour: 18

*Scheduler Start Minute: 45

Scheduled Event Settings

*Event Type	Account Balance	Hours Left Before Qu	Notify Ti

The following table describes the parameters that can be configured under **Scheduled Events Configuration**.

Table 14: Scheduled Events Configuration Parameters

Parameter	Description
Primary Database Address	The IP address of the sessionmgr database.
Secondary Database Address	The IP address of a secondary, backup, or failover sessionmgr database.
Database Port	The port used by the database; this is the sessionmgr port.
DB Write Concern	Controls the write behavior of Session Manager and for what errors exceptions are raised. Db Write Concern defined in Cluster page applies only to Admin, Trace and Endpoint databases. Select one of the following options from drop-down list: • OneInstanceSafe: This means the system waits for confirmation of writing in primary member. • TwoInstanceSafe: This means the system waits for confirmation in primary and one secondary member. Default value is OneInstanceSafe. For more information, see MongoDB documentation.

Parameter	**Description**
DB Read Preference	Describes how sessionmgr clients route read operations to members of a replica set. You can select from the following drop-down list: • Primary – Default mode. All operations read from the current replica set primary. • PrimaryPreferred – In most situations, operations read from the primary but if it is unavailable, operations read from secondary members. • Secondary – All operations read from the secondary members of the replica set. • SecondaryPreferred – In most situations, operations read from secondary members but if no secondary members are available, operations read from the primary. For more information, refer to http://docs.mongodb.org/manual/core/read-preference/.
Transactions Per Second	Controls the maximum number of internally generated transactions per second that the system will produce.
Scheduled Start Hour	The hour at which the event is triggered. The value specified should be in the range of 0 to 23 (24-hour format).
Scheduled Start Minute	The minute at which the event is triggered. The value specified should be in the range 0 to 59.
Event Type	The type of event that will be triggered. You can select either of the following: **QuotaExpiration** – The scheduled event will be triggered when the system detects that a subscriber's quota is going to expire within the number of hours specified in the **Hours Left Before Quota Exhausts** parameter. **SubscriberInactivity** – The scheduled event will be triggered when the system detects that a subscriber is inactive. If you select this event type, the **Hours Left Before Quota Exhausts** and **Notify Time in Hours** parameters are ignored.
Account Balance	Processes only those subscribers whose account balance is specified in the configuration. Other subscribers are ignored. The **Account Balance** and **Service** parameters filter for subscribers having the configured balance and service. If these columns are not specified, the event processes all subscribers.

Parameter	Description
Hours Left Before Quota Exhausts	Used only with the QuotaExpiration event type. This parameter specifies the number of hours before the subscriber's quota expires. The system checks this field in the scheduled events loop and looks for quotas that are about to expire within the number of hours specified. If the number of hours before expiration is less than the value in this column, then subscribers with that quota will be added to the eventsCollection in the ScheduleEvents mongo database. For example, if this value is 8, when the scheduled events task runs, any subscribes who have the service specified and whose quota will expire in less than 8 hours will be added to the eventsCollection. Once in eventsCollection, new actions are taken for that subscriber depending on scheduled event configuration.
Notify Time in Hours	Used only with the QuotaExpiration event type. This parameter specifies the number of hours before a notification is sent to the subscriber. This parameter is used in conjunction with the **Hours Left Before Quota Exhausts** parameter. When this number is reached, CPS submits a QuotaExpiredEvent to the policy engine with the subscriber's balance information. When this occurs, the state of the entry in the eventsCollection changes to "notified." For example, if **Hours Left Before Quota Exhausts** = 8 and **Notify Time in Hours** = 4, an entry is created with the subscriber's balance information in the eventCollections 8 hours prior to quota expiration, and a QuotaExpiration event is submitted to the policy engine 4 hours before expiration. You can set up polices to send out notifications when this event occurs; for example, you might set up scheduled events to send out notifications 8 hours, 6 hours, 4, hours, and 2 hours before a subscriber's quota expires, reminding the subscriber to "top up."
Service	Processes only those subscribers who have the configured service associated. Other subscribers are ignored. The **Account Balance** and **Service** parameters filter for subscribers having the configured balance and service. If these columns are not specified, the event processes all subscribers.
Max Number of Days	Used only with the SubscriberInactivity event type. This parameter specifies the duration in days to retain the subscriber in the inactive state. If the status of a subscriber remains inactive for longer than the configured maximum number of days, the subscriber is automatically deleted from the database.

Parameter	Description
Command	A string value that is used to provide additional information about the event that is being submitted. This string can be used in the polices that look for events submitted to the policy engine. For example, when used with a QuotaExpiration event type, the command could be set to "8 hours" or "6 hours," or to any other string. A policy can use this string in its condition parameters to send one notification as opposed to another, or to take one action as opposed to another.

LDAP/Ud Configuration

CPS has capability to access subscriber profile data either from internal or external database. LDAP/Ud feature fetches subscriber profile data from the external database.

In this section, LDAP plug-in configuration is used an example.

LDAP plugin queries the LDAP server to fetch attributes depending on the configuration. This feature has capability to refresh the profile and fetch the latest updated attribute from the LDAP server. CPS connects to multiple LDAP severs and queries them depending on the LDAP server priority.

Note Refer to *CPS Installation Guide for VMware* to configure this plugin.

Click **LDAP Configuration** from the right pane to add the configuration in the system.

Click **Ldap Server Configuration**.

Figure 14: LDAP Configuration

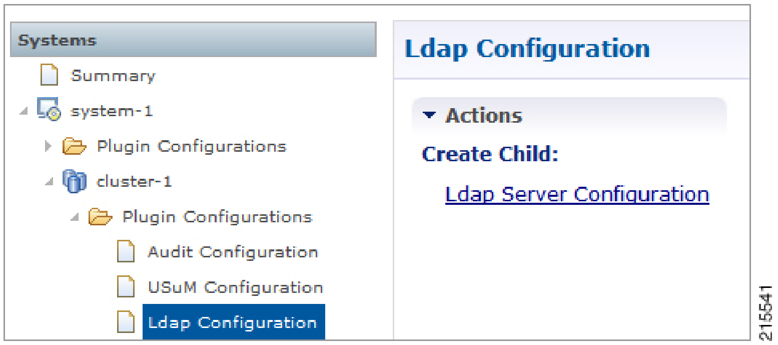
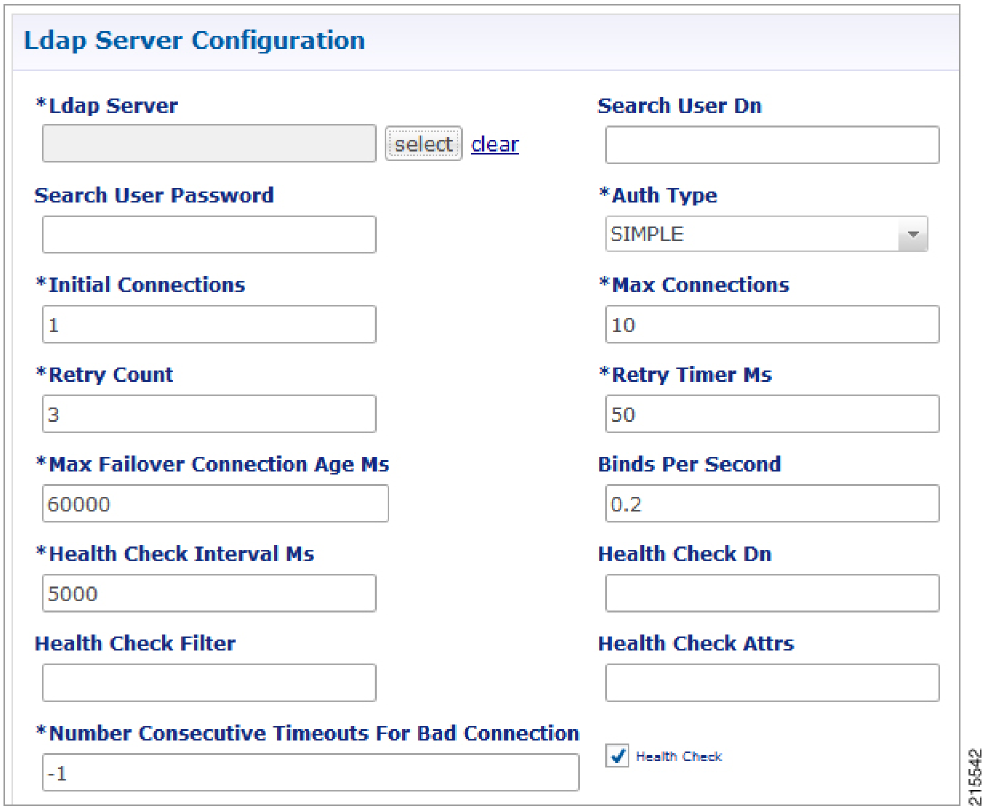


Figure 15: LDAP Server Configuration



Ldap Server Configuration

*Ldap Server: [ ] select clear

Search User Dn: [ ]

Search User Password: [ ]

*Auth Type: SIMPLE

*Initial Connections: 1

*Max Connections: 10

*Retry Count: 3

*Retry Timer Ms: 50

*Max Failover Connection Age Ms: 60000

Binds Per Second: 0.2

*Health Check Interval Ms: 5000

Health Check Dn: [ ]

Health Check Filter: [ ]

Health Check Attrs: [ ]

*Number Consecutive Timeouts For Bad Connection: -1

☑ Health Check

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

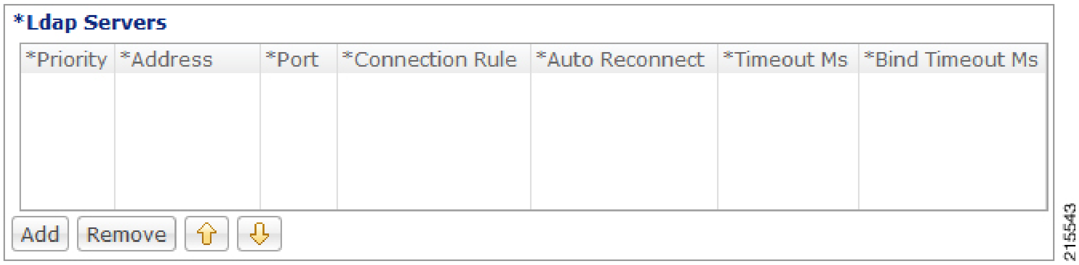
Table 15: LDAP Server Configuration Parameters – 1

Parameter	**Description**
Ldap Server	Assign this to the LDAP Server Set.
Search User Dn	The user DN for connecting to the LDAP server; for example, `cn=managerou=accountso=profile`.
Search User Password	The password for connecting to the LDAP server. **Note** The same password must apply to all servers defined in this configuration.
Auth Type	The LDAP authorization type required by the LDAP server. Default: SIMPLE
Initial Connections	Set the initial connections to “50.” This represents the number of connections from a Policy Director (load balancer) to the LDAP server(s).
Retry Count	The total number of tries the system executes for a given LDAP query. For example, a value of 2 indicates one try and then one more attempt when the query times out.

Parameter	Description
Retry Time Ms	The time period when the policy engine retries to a second Policy Director (load balancer) to send the request. **Note** Setting this value too low results in a large number of additional requests. This value should be set to a value close to the SLA provided by the LDAP server in servicing requests.
Max Failover Connection Age Ms	The time in milliseconds a secondary connection is used before checking to determine if the original primary server is available. This is the time to fall back from a failover connection. CPS returns the connection to the LDAP connection pool and gets another connection. Default: 60000 milliseconds (1 minute)
Binds Per Second	The maximum rate at which to connect to the LDAP server. Setting this to a high value may result in extra load on the peer LDAP server.
Health Check Interval Ms	The time in milliseconds to generate a health check message; for example, 5000 milliseconds (5 seconds).
Health Check Dn	The health check DN that is sent on the health check LDAP query.
Health Check Filter	The filter that is sent on the health check LDAP query.
Health Check Attrs	A comma-delimited list of attributes to retrieve in the LDAP health check query.
Health Check	Select this check box to enable the health check.
Number Consecutive Timeouts For Bad Connection	The number of timeouts that trigger a bad connection and force a reconnection. A value of -1 disables this function, preventing CPS from marking any connection bad. Default: -1

Add entries to the LDAP Servers to represent the primary and secondary connections from the CPS system to the LDAP servers.

Figure 16: LDAP Servers



You can configure the following parameters under **LDAP Servers**:

Table 16: LDAP Server Configuration Parameters – 2

Parameter	Description
Priority	The priority of the server when sending requests. Higher number is equal to higher priority.
Address	The IP address of the server to send requests.
Port	The port address of the LDAP Server.
Connection Rule	This setting is not currently used.
Auto Reconnect	This setting is not currently used.
Timeout Ms	The SLA for queries for the LDAP server. Cisco recommends a value of 5000 milliseconds.
Bind Timeout Ms	The SLA for binds to the LDAP server.

Subscriber Lookup Server Configuration

Note Refer to the section *Subscriber Lookup Feature Installation* in *CPS Installation Guide for VMware* to configure this plugin.

You can configure CPS to act as an LDAP server to support LDAP search queries that use framedIp/msisdn/imsi/framedIpv6Prefix key to get subscriber details.

In case multiple sessions are found for matching the same LDAP query, CPS responds with details of all the sessions to LDAP client.

The search query can come to any clusters in the deployment. For configuring cluster peer, refer to Cluster Peer Configuration, on page 34. The cluster that receives the request forwards the request to all other clusters based on Cluster Peer Configuration.

In Policy Builder, click **Subscriber Lookup Server Configuration** from the right pane to add the configuration in the system.

The following parameters can be configured under **Subscriber Lookup Server Configuration**:

Table 17: Subscriber Lookup Server Configuration Parameters

Parameter	Description
Bind DN/Bind DN (Admin) Password	Used to authenticate the LDAP search request before getting processed. Default: admin/password
Ldap Server Port	Used to configure the port where you want to start the LDAP server. Default: 1399

Parameter	Description
Request Timeout (ms.)	Used to configure the time LDAP server waits to get response. Default: 5 millisec
Health check Filter Name	Used to add the attribute name to identify a health-check request.
Health check Filter Value	Used to add the filter value to identify a health-check request.
Session update Time in ms.	If checked, returns the session update time in milliseconds in the query response. If unchecked, session update time is returned in seconds. Default: unchecked
Input Mapping	Used to map Filter Id received from LDAP client to one of the internal CPS lookup keys. Is Unique Key: Indicates the key is unique for the sessions and only one session would exist for the key. If selected for non unique key, only single active session is returned for the query. Default: unchecked
Output Mapping	Used to define the response attributes for the client. Response attribute name can be mapped to internal CPS session attributes for added flexibility.
Ldap Clients	Used to configure CPS to support multiple client authentication parameters.
Health Check Attributes	Used to define the response attributes and values to be returned to LDAP client for Health-check requests.

Cluster Peer Configuration

Configuration in qns.conf

Note "-" is not allowed in the cluster name (both local and peer).

- Local cluster must be specified with `local.cluster.peer` parameter in `/etc/broadhop/qns.conf` file. This parameter is used to find out the local cluster name and is used to create local cluster queue.

  Example: `-Dlocal.cluster.peer=Cluster1`

- All cluster peers must be specified with `broadcast.cluster.peers` parameter in `/etc/broadhop/qns.conf` file. This parameter is used to find out all other clusters and to create redisQ between local cluster and other clusters. Each cluster name must be separated with semicolon. Add all the clusters including local cluster name.

  Example: `-Dbroadcast.cluster.peers=Cluster1;Cluster2;Cluster3`

Configuration for RedisQ Servers

- Redis server peers must be configured in `/etc/broadhop/broadcast-cluster.conf` file:

  This file has information about the redisQ servers. You need to provide Policy Directory (lb) VIP address if this is a HA setup. Each cluster specified in `broadcast.cluster.peers` must have one entry in this file to represent redis server related to that cluster.

  Syntax: *<ClusterName>*`-clusterBroadcastQ.redis.qserver=`*`<lbvipIPadress>`*

  where, *<lbvipIPadress>* is the IP address of Policy Director (LB) VIP.

  ClusterName is the local cluster peer (configured for `local.cluster.peer` parameter in `qns.conf` file) of every cluster.

  Example:

```
[root@lb02 broadhop]# cat /etc/broadhop/broadcast-cluster.conf
Cluster1-clusterBroadcastQ.redis.qserver=IPaddress1
Cluster2-clusterBroadcastQ.redis.qserver=IPaddress2
Cluster3-clusterBroadcastQ.redis.qserver=IPaddress3
```

Note

- During replica-set failover, some of the LDAP search requests coming from LDAP clients to a CPS site fail to respond back with session details. This is because CPS reads the session details from the nearest secondary replica-set member, and with two replica-set members present on a site when the Primary member goes down the only remaining secondary member transitions to Primary state. During this transition, there is no Secondary member available in the nearest location (or local site) and therefore Mongo is not able to read the session information. As a result, the CPS application responds back to the LDAP request without any session information. However, since the failover transition period is less than 30 seconds, so a retry from the LDAP client after this period results in an LDAP response with session information.
- If local session affinity is enabled in CPS, then during migration of sessions to replica-set of a remote CPS site, some of the LDAP search requests coming from LDAP clients to the local CPS site fail to respond back with session details. This is because CPS reads the session details from the nearest secondary replica-set member, and with migration in progress the nearest secondary members of the remote site replica-set present on the local CPS site is not in sync with the corresponding Primary member present on the remote site. This can happen due to latency between the two CPS sites. As a result, the CPS application responds back to the LDAP request without any session information. However, depending upon the delay in sync between the two site replica-set members, a retry of the LDAP client request results in an LDAP response with session information.