



## Plug-in Configuration

---

- [Overview, on page 1](#)
- [Threading Configuration, on page 2](#)
- [Portal Configuration, on page 3](#)
- [Async Threading Configuration, on page 4](#)
- [Custom Reference Data Configuration, on page 6](#)
- [Balance Configuration, on page 7](#)
- [Diameter Configuration, on page 11](#)
- [Voucher Configuration, on page 12](#)
- [Unified API Configuration, on page 13](#)
- [Notification Configuration, on page 14](#)
- [Audit Configuration, on page 15](#)
- [USuM Configuration, on page 16](#)
- [Scheduled Events, on page 22](#)
- [LDAP/Ud Configuration, on page 27](#)
- [Subscriber Lookup Server Configuration, on page 30](#)

## 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.

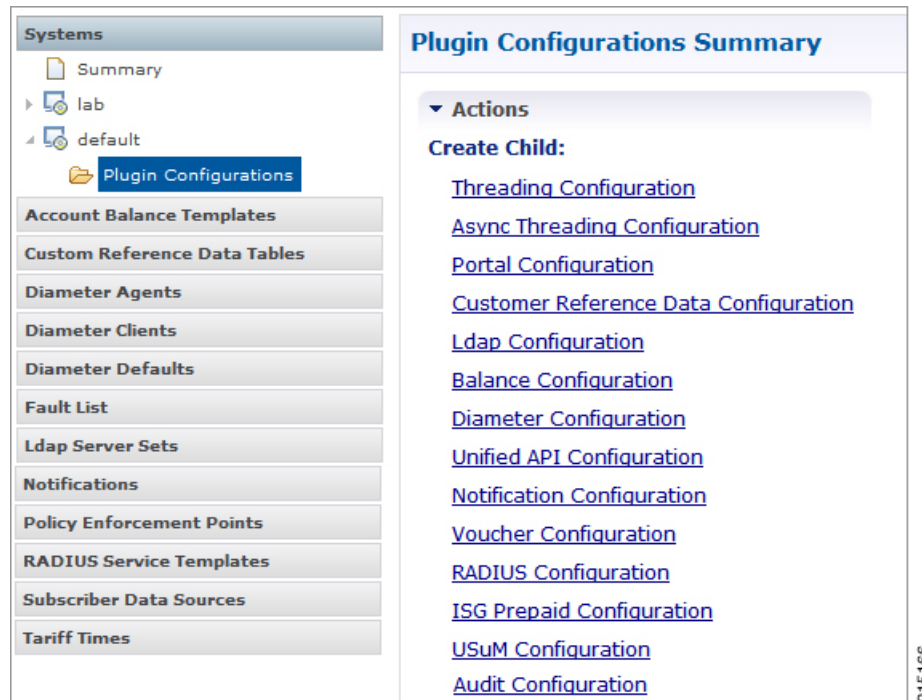
Cisco Policy Builder provides core plug-ins for customizing and optimizing your installation.

- 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**



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. If you are planning to run the system with higher TPS, then you need to configure Threading Configuration. For further information, contact your Cisco Technical 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 that are executing at any given time. The default value is 50.

Cisco recommends not to configure the value below 50, but it can be set higher to help increase performance in certain situations.

A configuration example is shown below:

**Figure 2: Thread Pool Configuration**

The screenshot shows a web-based configuration interface titled "Threading Configuration". Inside, there is a section "Thread Pool Configuration" containing a table. The table has four columns: "\*Thread Pool Name", "\*Threads", "\*Queue Size", and "\*Scale By Cpu Core". There is one row with the name "rules", 50 threads, a queue size of 0, and an unchecked checkbox for scaling by CPU core. Below the table are buttons for "Add", "Remove", and two arrows (up and down). A vertical label "215173" is on the right side of the interface.

*Thread Pool Name	*Threads	*Queue Size	*Scale By Cpu Core
rules	50	0	<input type="checkbox"/>

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.
Threads	Threads to set in the thread pool. You can set Rules Thread to 50/100 depending on call flow (based on number of lookup and per transaction round trip time). <ul style="list-style-type: none"> <li>rules = 50; Queue Size = 0; Scale By Cpu Core = unchecked</li> <li>rules = 100; Queue Size = 0 (If TPS is &gt; 2000 per Policy Server (QNS) depending on call model used; for example, if LDAP is enabled); Scale By Cpu core = unchecked</li> </ul>
Queue Size	Size of the queue before they are rejected.
Scale By Cpu Core	Select this check box to scale the maximum number of threads by the processor cores.

## 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**

**Secondary Database Host/IP Address**

**\*Database Port**

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.

## Async Threading Configuration

Click **Async Threading 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.



### 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:

\*Default Action Priority:

\*Default Action Threads:

\*Default Action Queue Size:

☒ Default Action Drop Oldest When Full

**Action Configurations**

*Action Name	*Action Priority	*Action Threads	*Action Queue Size	*Action Drop Oldest When Full

Add Remove ↑ ↓

The following parameters can be configured under Async Threading Configuration.

Table 2: Async Threading Configuration

Parameter	Description
Default Processing Threads	The number of threads that are allocated to process actions based on priority.
Default Action Priority	The priority assigned to an action if it is not specified in the Action Configurations table.
Default Action Threads	The number of threads assigned to process the action if it is not specified in the Action Configurations table.
Default Action Queue Size	The number of actions that can be queued up for an action if it is not specified in the Action Configurations table.
Default Action Drop Oldest When Full	When checked, the oldest queued action is dropped from the queue when a new action is added to a full queue. Otherwise, the new action to add is ignored.  This check box applies to all the threads specified. To drop a specific thread, leave this unchecked and use the Action Configurations table.
<b>Action Configurations Table</b>	
Action Name	The name of the action. This must match the implementation class name.
Action Priority	The priority of the action. Used by the default processing threads to determine which action to execute first.
Action Threads	The number of threads dedicated to processing this specific action.

Parameter	Description
Action Queue Size	The number of actions that can be queued up.
Action Drop Oldest When Full	For the specified action only:  When checked, the oldest queued action is dropped from the queue when a new action is added to a full queue. Otherwise, the new action to add is ignored.

## Custom Reference Data Configuration

Before you can create a custom reference data table, configure your system to use the Custom Reference Data Table plug-in configuration.

You only have to do this one time for each system, cluster, or instance. Then you can create as many tables as needed.

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

Here is an example for HA and AIO setups:

- HA example:
  - Primary Database Host/IP Address: sessionmgr01
  - Secondary Database Host/IP Address: sessionmgr02
  - Database Port: 27717
- AIO example:
  - Primary Database Host/IP Address: localhost or 127.0.0.1
  - Secondary Database Host/IP Address: NA (leave blank)
  - Database Port: 27017

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.
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	Port number of the sessionmgr. It should be the same for both the primary and secondary databases.

Parameter	Description
Db Read Preference	<p>Read preference describes how sessionmgr clients route read operations to members of a replica set. You can select from the following drop-down list:</p> <ul style="list-style-type: none"> <li>• Primary: Default mode. All operations read from the current replica set primary.</li> <li>• PrimaryPreferred: In most situations, operations read from the primary but if it is unavailable, operations read from secondary members.</li> <li>• Secondary: All operations read from the secondary members of the replica set.</li> <li>• SecondaryPreferred: In most situations, operations read from secondary members but if no secondary members are available, operations read from the primary</li> </ul> <p>For more information, refer to <a href="http://docs.mongodb.org/manual/core/read-preference/">http://docs.mongodb.org/manual/core/read-preference/</a>.</p>
Connection Per Host	<p>Number of connections that are allowed per DB Host.</p> <p>Default value is 100.</p>
Avp Persists	<p>This table provides CPS with the ability to configure certain AVPs that need to be stored in the session database. AVPs that are not configured as part of this table, are not persisted.</p> <ul style="list-style-type: none"> <li>• Name: The name with which the AVP value needs to be stored in the session.</li> <li>• Avp Name: The logical name of the CRD/policy derived AVP.</li> </ul> <p>To retrieve these stored AVPs from the session, Customer Reference Data Debug AVPs retriever can be used. This retriever is used in the <b>PolicyState/Session data to Custom AVP Mapping</b> under Custom AVP Profiles, to send the stored AVPs in any diameter message.</p> <p><b>Restriction</b> When configuring the AVP Persists table in the Policy Builder, for each AVP, its corresponding AVP Name and Name is expected to be configured. If either is found to be empty, then the particular AVP is not added to the Gx session. Thus the concerned AVP is not available to send in any custom AVP as well.</p>

For more information on Custom Reference Data API Usage, refer to 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 sessionmgr and for what errors exceptions are raised. Default option is OneInstanceSafe.
Db Read Preference	<p>Read preference describes how sessionmgr clients route read operations to members of a replica set. You can select from the following drop-down list:</p> <ul style="list-style-type: none"> <li>• Primary</li> <li>• PrimaryPreferred</li> <li>• Secondary</li> <li>• SecondaryPreferred</li> </ul> <p>For more information, refer to <a href="http://docs.mongodb.org/manual/core/read-preference/">http://docs.mongodb.org/manual/core/read-preference/</a>.</p>
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.
Max Replication Wait Time Ms	<p>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.</p> <p>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.</p>
Default Minimum Dosage Time Based	<p>This field is optional but recommended.</p> <p>This is the minimum amount of time that is granted for a reservation, assuming quota is not exhausted.</p> <p>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.</p> <p>Minimum value is 2 seconds.</p>



Parameter	Description				
Default Minimum Dosage Volume Based	<p>This field is optional but recommended.</p> <p>This is the minimum amount of volume that is granted for a reservation, assuming quota is not exhausted.</p> <p>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.</p>				
Expired Reservations Purge Time (minutes)	<p>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.</p> <p>Default value is 0.</p>				
Recurring Refresh Max Delay (minutes)	<p>The amount of time refreshing of recurring quotas are staggered across randomly, for sessions that are not actively using quota but are still established.</p> <p>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.</p> <p>Default value is 0.</p> <p>To calculate the Recurring Refresh Max Delay, use the following:</p> $\text{Recurring Refresh Max Delay} = (\text{Number of sessions} / \text{Max Timer TPS}) * 2$ <p>For example:</p> <p>If 30 million sessions are present on the system, and Max Timer TPS is configured to 2000, then</p> <table border="1"> <tr> <td>Recurring Refresh Max Delay</td><td><math>= (30,000,000 / 2000) * 2</math></td></tr> <tr> <td></td><td><math>= 500 \text{ minutes} \sim 8.33 \text{ hours}</math></td></tr> </table> <p>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.</p> <p><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 <a href="#">Adding an HA Cluster</a>.</p>	Recurring Refresh Max Delay	$= (30,000,000 / 2000) * 2$		$= 500 \text{ minutes} \sim 8.33 \text{ hours}$
Recurring Refresh Max Delay	$= (30,000,000 / 2000) * 2$				
	$= 500 \text{ minutes} \sim 8.33 \text{ hours}$				
Remote Database Lookup Filter Type	<p>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.</p> <p>By default, NetworkId is selected.</p> <p><b>Note</b> Filter type must be same in API Router Configuration and Balance Configuration in Policy Builder.</p>				

Parameter	Description
Reduce Dosage on Threshold	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.
Submit Balance Events To Reporting	Submits balance transaction to the policy engine, and these can be reflected in reporting.
Enable Crd Balance Template Lookups	<p>When checked, CPS is enabled to lookup CRD defined balance templates. If the CRD tables are not defined, this feature is disabled.</p> <p><b>Note</b> Even if the CRD tables are not defined as required, and this feature is disabled, the <b>Dynamic Reference Data Key</b> field is still enabled but only for Policy Builder defined Account Balance Templates. For more information, see <a href="#">Dynamic Reference Data Key</a>.</p>
<b>Remote Database</b>	
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	<p>Number of connections that can be created per host.</p> <p>Default value is 5.</p>
Db Read Preference	<p>Read preference describes how sessionmgr clients route read operations to members of a replica set. You can select from the following drop-down list:</p> <ul style="list-style-type: none"> <li>• Primary</li> <li>• PrimaryPreferred</li> <li>• Secondary</li> <li>• SecondaryPreferred</li> </ul> <p>For more information, refer to <a href="http://docs.mongodb.org/manual/core/read-preference/">http://docs.mongodb.org/manual/core/read-preference/</a>.</p>
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.

Parameter	Description
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**

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**  
 ☒ 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** ☐

215490

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**

**Secondary Database Host/IP Address**

**\*Database Port**

☐ Disable Vouchers

The voucher plug-in uses the following defaults:

- HA example:

- Primary: sessionmgr01
- Secondary: sessionmgr02
- Port: 27718
- AIO example:
  - Primary: localhost or 127.0.0.1
  - Secondary: NA (leave blank)
  - Port: 27017

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.

**Figure 8: Unified API Configuration**

Unified API Configuration

\*Fields To Wrap With Cdata Tags  
networkId,password,data,oldNetw

Session Route Key  
cluster1.dc1

☒ Submit Requests To Audit Log

☐ Submit Read Requests To Audit Log

The following parameters can be configured under Unified API Configuration:

Table 7: Unified API Configuration Parameters

Parameter	Description
Fields To Wrap With Cdata Tags	<p>This is a CSV separated string.</p> <p>The Unified API can handle CDATA fields. Use the Plug-in configuration in Policy Builder to set CDATA fields for the main Unified API.</p> <p>The property <code>ua.cdata.fields</code> is used to set the fields that must be wrapped in CDATA tags for the client CommFactory to properly send and receive API requests.</p> <p><code>-Dua.cdata.fields=networkId,password,data,oldNetworkId,oldPassword,newPassword</code> is the default.</p>
Session Route Key	<p>Session route key that vDRA uses to look up the peer group and route the Rx AAR message to the correct PCRF.</p> <p>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.</p>
Submit Requests To Audit Log	<p>Select the check box to log requests to API in audit log.</p> <p>Default value is True (checked).</p>
Submit Read Requests To Audit Log	<p>Select this check box to log read requests in audit log.</p> <p>Default value is False (unchecked).</p>

## 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.
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 9: Audit Configuration

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.

Parameter	Description
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.
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 10: USuM Configuration**

The screenshot shows the 'USuM Configuration' window. Inside, there is a section titled '\*Spr Configuration' with three unchecked checkboxes: 'Disable Regex Search', 'Enable Avp Regex Search', and 'Exclude Suspended Subscribers From Policy'. Below this is a section titled '\*Search Query Results Limit' with a text input field containing '1000'. The next section is '\*Max Number Of Locations To Store In History' with a text input field containing '5'. The final section is '\*Last Visited Date Threshold' with a text input field containing '2'. A vertical text '215169' is visible on the right side of the configuration pane.

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



Table 10: USuM Configuration Parameters - 1

Parameter	Description
<b>Spr Configuration</b>	
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.  <b>Note</b> 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.
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 visting 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 11: Policy Engine Submission Configuration

**\*Policy Engine Submission Configuration**

☒ Enable

**\*Message Queue Size**

**\*Message Queue Sleep**

**\*Message Queue Batch Size**

**\*Message Queue Pool Size**

**\*Notification Rate Limit**

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.
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 12: 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	

Parameter	Description
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 sessionmgr and for what errors exceptions are raised. Default option is OneInstanceSafe.
Db Read Preference	<p>Read preference describes how sessionmgr clients route read operations to members of a replica set. You can select from the following drop-down list:</p> <ul style="list-style-type: none"> <li>• Primary</li> <li>• PrimaryPreferred</li> <li>• Secondary</li> <li>• SecondaryPreferred</li> </ul> <p>For more information, refer to <a href="http://docs.mongodb.org/manual/core/read-preference/">http://docs.mongodb.org/manual/core/read-preference/</a>.</p> <p><b>Important</b> For consistent profile updates across multiple sessions for same subscriber, Cisco recommends to set the <b>Db Read Preference</b> as <i>PrimaryPreferred</i>.</p>
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.
Max Replication Wait Time Ms	<p>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.</p> <p>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.</p>
<b>Shard Configuration</b>	
<b>Important</b> 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.

Parameter	Description
<b>Remote Shard Configuration</b> <b>Important</b> 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 13: Remote Database Configuration

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: <ul style="list-style-type: none"> <li>• StartsWith</li> <li>• Regex</li> <li>• EndsWith</li> <li>• Equals</li> </ul>

Parameter	Description
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: <ul style="list-style-type: none"> <li>• Primary</li> <li>• PrimaryPreferred</li> <li>• Secondary</li> <li>• SecondaryPreferred</li> </ul> For more information, refer to <a href="http://docs.mongodb.org/manual/core/read-preference/">http://docs.mongodb.org/manual/core/read-preference/</a> .
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** If this is AIO environment, edit the features files in Cluster Manager VM:
- In the `/var/qps/current_config/etc_aio/broadhop/pb/features` file, add the following line:
- ```
com.broadhop.client.feature.scheduledevents
```
- In the `/var/qps/current_config/etc_aio/broadhop/pcrf/features` file, add the following line:
- ```
com.broadhop.scheduledevents.service.feature
```
- Step 3** 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
```
- Note** `reinit.sh` executes puppet on AIO and also checks if it is executed successfully.
- 

## 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 14: 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

Add Remove ↑ ↓

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 sessionmgr and for what errors exceptions are raised. Default: OneInstanceSafe



Parameter	Description
DB Read Preference	<p>Describes how sessionmgr clients route read operations to members of a replica set. You can select from the following drop-down list:</p> <ul style="list-style-type: none"> <li>• <b>Primary</b> – Default mode. All operations read from the current replica set primary.</li> <li>• <b>PrimaryPreferred</b> – In most situations, operations read from the primary but if it is unavailable, operations read from secondary members.</li> <li>• <b>Secondary</b> – All operations read from the secondary members of the replica set.</li> <li>• <b>SecondaryPreferred</b> – In most situations, operations read from secondary members but if no secondary members are available, operations read from the primary.</li> </ul> <p>For more information, refer to <a href="http://docs.mongodb.org/manual/core/read-preference/">http://docs.mongodb.org/manual/core/read-preference/</a>.</p>
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	<p>The type of event that will be triggered. You can select either of the following:</p> <p><b>QuotaExpiration</b> – 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 <b>Hours Left Before Quota Exhausts</b> parameter.</p> <p><b>SubscriberInactivity</b> – The scheduled event will be triggered when the system detects that a subscriber is inactive. If you select this event type, the <b>Hours Left Before Quota Exhausts</b> and <b>Notify Time in Hours</b> parameters are ignored.</p>
Account Balance	<p>Processes only those subscribers whose account balance is specified in the configuration. Other subscribers are ignored.</p> <p>The <b>Account Balance</b> and <b>Service</b> parameters filter for subscribers having the configured balance and service. If these columns are not specified, the event processes all subscribers.</p>

Parameter	Description
Hours Left Before Quota Exhausts	<p>Used only with the QuotaExpiration event type. This parameter specifies the number of hours before the subscriber's quota expires.</p> <p>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.</p> <p>For example, if this value is 8, when the scheduled events task runs, any subscribers 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.</p>
Notify Time in Hours	<p>Used only with the QuotaExpiration event type. This parameter specifies the number of hours before a notification is sent to the subscriber.</p> <p>This parameter is used in conjunction with the <b>Hours Left Before Quota Exhausts</b> 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."</p> <p>For example, if <b>Hours Left Before Quota Exhausts</b> = 8 and <b>Notify Time in Hours</b> = 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.</p> <p>You can set up policies 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."</p>
Service	<p>Processes only those subscribers who have the configured service associated. Other subscribers are ignored.</p> <p>The <b>Account Balance</b> and <b>Service</b> parameters filter for subscribers having the configured balance and service. If these columns are not specified, the event processes all subscribers.</p>
Max Number of Days	<p>Used only with the SubscriberInactivity event type.</p> <p>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.</p>

Parameter	Description
Command	<p>A string value that is used to provide additional information about the event that is being submitted. This string can be used in the policies that look for events submitted to the policy engine.</p> <p>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.</p>

## 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 as 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 servers 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 15: LDAP Configuration**



Figure 16: LDAP Server Configuration

**Ldap Server Configuration**

\*Ldap Server  [select](#) [clear](#)

Search User Password

\*Initial Connections

\*Retry Count

\*Max Failover Connection Age Ms

\*Health Check Interval Ms

Health Check Filter

\*Number Consecutive Timeouts For Bad Connection

Search User Dn

\*Auth Type

\*Max Connections

\*Retry Timer Ms

Binds Per Second

Health Check Dn

Health Check Attrs

☒ Health Check

215542

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, <code>cn=managerou=accountso=profile</code> .
Search User Password	The password for connecting to the LDAP server. <b>Note</b> 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.  <b>Note</b> 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 17: LDAP Servers**

**\*Ldap Servers**

*Priority	*Address	*Port	*Connection Rule	*Auto Reconnect	*Timeout Ms	*Bind Timeout Ms

Add
Remove
↑
↓

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 31](#). 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 millisecc
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=<lbvipIPaddress>`

where, `<lbvipIPaddress>` 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.